Technische Hochschule
Brandenburg
University of
Applied Sciences

IT-Sicherheit im Kontext der fortschreitenden Digitalisierung von klinischen Infrastrukturen

Masterarbeit
zur Erlangung des Grades Master of Science (M. Sc.)
des Fachbereichs Wirtschaft der
Technischen Hochschule Brandenburg

vorgelegt von:
Torsten Otto
geb. am 26. August 1974 in Frankenberg
7. Semester

Betreuer: Prof. Dr. Ivo Keller
Zweitgutachter: Prof. Dr. Michael Pilgermann

Otto, Torsten Master Security Management 7. Fachsemester (Tz)	Dallgower Straße 90 14612 Falkensee ottot@th-brandenburg.de Matr.-Nr. 20205824

Brandenburg an der Havel, den 18. Oktober 2021

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Beschreibung
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AG	Arbeitgeber
ARP	Address Resolution Protocol
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BVDW	Bundesverband Digitale Wirtschaft e.V.
CA	certificate authority
CIS	Center for Internet Security
CT	Computertomographie
CTG	Cardiotokografie
CVC	Card Verifiable Certificate
DEMIS	Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz
DICOM	Digital Imaging and Communications in Medicine
DiGA	Digitale Gesundheitsanwendungen
DiGAV	Digitale Gesundheitsanwendungen-Verordnung
DKG	Deutsche Krankenhausgesellschaft e.V.
DNS	Domain Name System
DSGVO	Datenschutzgrundverordnung
DVG	Digitale-Versorgung-Gesetz
DVPMG	Digitale-Versorgungs- und Pflege-Modernisierungs-Gesetz
EAL	Evaluation Assurance Level
eAU	elektronische Arbeitsunfähigkeitsbescheinigung
EDR	Endpoint Detection and Response
eGK	elektronische Gesundheitskarte
eID	elektronische Identität
eMP	elektronischer Medikationsplan
EMRAM	Electronic Medical Records Adoption Model
ePA	elektronische Patientenakte
EU	Europäischen Union
EuGH	Gerichtshof der Europäischen Union
FAQ	Frequently Asked Questions
GKV	Gesetzliche Krankenversicherung

Abkürzung	Beschreibung
GLT	Gebäudeleittechnik
GmbH	Gesellschaft mit beschränkter Haftung
HIMSS	Healthcare Information and Management Systems Society
HSM-Proxy	Hardware Security Module Proxy
IDS	Intrusion Detection Systeme
IP	Internet Protokoll
ISDN	Integrated Services Digital Network
ISMS	Informationssicherheitsmanagementsystem
IoT	Internet of Things
IT	Informationstechnik
ITSiG	IT-Sicherheitsgesetz
IVDR	In-Vitro-Diagnostika
KBV	Kassenärztliche Bundesvereinigung
kDL	kritische Dienstleistung
KHG	Krankenhausfinanzierungsgesetz
KHZG	Krankenhauszukunftsgesetz
KI	Künstliche Intelligenz
KIM	Kommunikation im Medizinwesen
KIS	Krankenhausinformationssystem
KOM-LE	Kommunikation zwischen Leistungserbringern
KTR-AdV	Kostenträger-Anwendungen des Versicherten
KTR-Consumer	Kostenträger-Consumer
LAN	Local Area Network
MDR	Medical Device Regulation
MV	Mecklenburg-Vorpommern
MVZ	Medizinische Versorgungszentren
NFD	Notfalldatensatz
OCSP	Online Certificate Status Protocol
OID	Object Identifie
OWASP	Open Web Application Security Project
PACS	Picture Archiving and Communication System
P-A-P	Paketfilter – Application-Level-Gateway – Paketfilter
PDAC	Plan-Do-Check-Act
PDSG	Patientendaten-Schutz-Gesetz
PIN	Personal Identification Number
PTV	Produkttypversionen
PUK	Personal Unblocking Key
PVS	Praxisverwaltungssystem
SD-WAN	Software-Defined Networking in einem Wide Area Network
SGB	Sozialgesetzbuch
SIEM	Security Information and Event Management
SMC	Security Module Card
SZZPs	Sicherer Zentraler Zugangspunkt
TI	Telematikinfrastruktur
TSVG	Terminservice- und Versorgungsgesetz

Abkürzung	Beschreibung
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
VSDM	Versichertenstammdatenmanagement
WAN	Wide Area Network
XDR	Extended Detection and Response

1 Ausgangssituation

Die Bedeutung von klinischen Infrastrukturen für die Bevölkerung und die Wirtschaft wird im Rahmen der Covid-19-Pandemie sehr deutlich aufgezeigt. Dessen Verfügbarkeit ist für jeden Einzelnen, nicht nur in Ausnahmesituation, sondern jederzeit von besonderer Wichtigkeit und gehört zur existentiellen Grundversorgung. Aus diesem Grund wurde das Gesundheitswesen, als eine der neun Sektoren, bereits im ersten IT-Sicherheitsgesetzt als kritische Infrastruktur eingestuft. Mit der fortschreitenden Digitalisierung und der damit einhergehenden zunehmenden Vernetzung der klinischen Infrastrukturen nimmt die Bedeutung der IT-Sicherheit weiter zu. Neue Bedrohungen und Risiken ergeben sich insbesondere durch die Einbindung neuer IT-Anwendungen und deren Schnittstellen sowie die Nutzung der Infrastrukturen von weiteren Akteuren in einem nicht unerheblichen zusätzlichen Umfang. Dabei entsteht ein Spannungsfeld zwischen dem Wunsch nach Vernetzung und Prozessoptimierung und dem Schutz der Patienten und deren Daten.

Welchen Beitrag die überarbeitete und am 07. Mai 2021 vom Bundesrat gebilligte zweiten Fassung des IT-Sicherheitsgesetzes (ITSiG) und weitere relevante Gesetze im Gesundheitsumfeld für die IT-Sicherheit leisten können, ist bei einer hierfür nicht hinreichend erscheinenden finanziellen und personellen Ausstattung der Akteure im Gesundheitswesen zu bewerten. Dabei soll mit dieser Arbeit sowohl auf den Stand der Digitalisierung als auch die neuen Anforderungen in Bezug auf ihre Bedeutung, Wichtigkeit und Einflussnahme auf die IT-Sicherheit, die sich hieraus an diese kritische Infrastruktur und deren Betreiber ergeben, eingegangen werden. Es wird nicht nur ausschließlich auf den Umsetzungsstand und das Bewusstsein für IT-Sicherheit in klinische Infrastrukturen eingegangen, die nach den aktuellen Schwellenwerten der BSI-KritisV als kritische Infrastruktur eingestuft sind, sondern auch darüber hinaus.

Mit dem am 23.10.2020 verabschiedeten Krankenhauszukunftsgesetz wurden finanzielle Mittel zur Überwindung der strukturellen Mängel und der Weiterentwicklung der Digitalisierung und Vernetzung des Gesundheitswesens durch Förderung entsprechender Projekte freigegeben. Dessen Beitrag zu einer signifikanten und nachhaltigen Veränderung soll vor dem Hintergrund des bestehenden Finanzierungsmodels hinterfragt werden.

2 Gesundheitswesen in Deutschland

Das Gesundheitssystem wird aufgeteilt in Leistungserbringung, Leistungsempfänger, Finanzierung und Kontrollinstanzen. Das Gesundheitswesen als Versorgungssystem kann in die drei wesentlichen Versorgungsbereiche Primärversorgung, Akutversorgung und Rehabilitation unterteilt werden. Es umfasst weit mehr als einzelne Versorgungseinrichtungen, wie Krankenhäuser, Therapie- und Pflegeeinrichtungen oder einzelne Arztpraxen. In einem gesamtheitlichen Ansatz müssen darüber hinaus weitere Akteure wie Krankenkassen, Labore, die gematik GmbH als Betreiber der Telematikinfrastruktur sowie weitere Dienstleister betrachtet werden. Daher soll im Folgenden auf die wichtigsten Akteure eingegangen und deren Bedeutung für das gesamte Ökosystem des Gesundheitswesens herausgestellt werden. Beteiligt ist in allen Bereichen, neben dem Einsatz von IT-Systemen zur Unterstützung, immer auch der Mensch.

2.1 Akteure im Gesundheitswesen

2.1.1 Krankenhäuser

In Deutschland gab es 2019 insgesamt 1.914 Krankenhäuser im Sinne des §2 Nr. 1 des Krankenhausfinanzierungsgesetzes (KHG) einschließlich der in den §§ 3, 5 des KHG genannten Krankenhäuser, soweit sie zu den Krankenhäusern nach § 107 Abs. 1 des Fünften Buches Sozialgesetzbuch gehören.[1] Hierbei können Krankenhäuser nach verschiedenen Merkmalen, z.B. in Trägerschaften, Rechtsformen, Größe und fachliche Ausrichtung, klassifiziert werden.
Eine weitere Möglichkeit ist eine Einteilung der Krankenhäuser in vier Versorgungsstufen, Grundversorgung, Regelversorgung, Schwerpunktversorgung und Maximalversorgung vorzunehmen. Von einem Krankenhaus der Grundversorgung spricht man, wenn es mindestens ein der Fachrichtung Innere Medizin oder Chirurgie vorhält. In der Regelversorgung muss zusätzlich zu diesen beiden

1 Vgl. Statistisches Bundesamt (April 2021).

Fachrichtungen bei Bedarf auch die Fachrichtungen Gynäkologie und Geburtshilfe, Hals-, Nasen- und Ohrenheilkunde sowie Augenheilkunde vorgehalten werden, so dass in den meisten Fällen Grund- und Regelversorgung zusammengefasst werden. Bei der Schwerpunkversorgung erweitert sich das Spektrum der vorgehaltenen Fachrichtung des Krankenhauses um Pädiatrie, Neurologie sowie Mund-, Kiefer- und Gesichtschirurgie. Krankenhäuser der Maximalversorgung bieten Gesundheitsleistungen in noch darüberhinausgehend weiteren Fachrichtungen an und halten auch die dafür erforderlichen Einrichtungen und Großgeräte vor.
Aus dem Versorgungstyp können in der Regel Rückschlüsse auf die Größe des Krankenhauses gezogen werden. Auch wenn die Spezifizierung nicht bundeseinheitlich geregelt ist, so kann grob folgende Einteilung vorgenommen werden[2]

- Grundversorgung (bis 200 Betten)
- Grund- und Regelversorgung (200 bis 350 Betten)
- Schwerpunkt- bzw. Zentralversorgung (350 bis 1.000 Betten)
- Maximalversorgung (über 1.000 Betten)

Die Einrichtungen der Grund- und Regelversorgung stellen mit ca. dreiviertel aller Häuser den überwiegenden Anteil. Auf Grund des auf Fallpauschalen basierenden Finanzierungkonzeptes agieren diese Häuser häufig am Existenzminimum, was sich auch auf die Ausstattung der IT und somit auf deren Sicherheit auswirkt. Dabei sichern gerade diese Einrichtungen die Versorgung der Bevölkerung insbesondere im ländlichen Raum.

2.1.2 Klinikverbünde

Aus betriebswirtschaftlicher Sicht sind Krankenhäuser als eigenständige Häuser oder in Klinikverbünden organisiert. Ob eine betriebswirtschaftliche Zusammenarbeit zwischen verschieden Häusern vorliegt und damit von gemeinsamen Optimierungsinteressen im Rahmen von Prozess-Digitalisierung vorliegt, ist nicht immer so offensichtlich wie bei dem Unternehmen Helios, welches 89 Kliniken und 120 Medizinische Versorgungszentren in einem Unternehmen vereint.[3] Über Recherchen im Krankenhausverzeichnis[4] der Deutsche Krankenhausgesellschaft konnten mehr als 90 Klinikverbünde ermittelt werden.[5]
In Bezug auf die weitere Betrachtung wird die Organisationsform im Kontext der KRITIS-Relevanz und der IT-Sicherheit von Klinikverbünden noch von Relevanz

2 Vgl. Nürnberg/Schneider (2014).
3 Vgl. https://www.helios-gesundheit.de/ (15.06.2021).
4 Vgl. Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (19.09.2021).
5 Vgl. Die Aufstellung der Klinikverbünde und eine Zuordnung der Einrichtungen kann den Anhängen A und B entnommen werden.

sein, insbesondere da im Rahmen der Digitalisierung von einer stärkeren Vernetzung und Konsolidierung/Zentralisierung von IT-Infrastrukturen und Systemen innerhalb dieser Verbünde ausgegangen werden kann. Deutlich wird dies an den beiden Beispielen aus dem Umfeld der Helios-Kliniken-Gruppe, wo die General Electric Healthcare GmbH die deutschlandweite Vernetzung bereitstellt und betreibt und dem Pilotprojekt zur Vernetzung des Helios Klinikums München West mit 52 Einzelpraxen und medizinischen Versorgungszentren im Münchner Umfeld zum übergreifenden Austausch von Patientendaten.[6]

2.1.3 Vorsorge- oder Rehabilitationseinrichtungen

Stationäre Heilbehandlungen werden neben klassischen Krankenhäusern zu einem Großenteil in entsprechenden Vorsorge- oder Rehabilitationseinrichtungen erbracht. Diese sind teilweise Bestanteil der Klinikverbünde, werden aber auch von anderen unabhängigen Trägern als Einzeleinrichtungen oder als Gruppe betrieben. Insgesamt werden im Krankenhausverzeichnis durch das Statistische Bundesamt 1.074 Einrichtungen dieses Typs mit einer Gesamtkapazität von etwas mehr als 158.500 Betten ausgewiesen.[7]
Diese Einrichtungen müssen zur Übermittlung von Gesundheitsdaten ebenfalls Teilnehmer der Telematikinfrastruktur sein. Darüber hinaus bedarf es einer Vielzahl weiterer externer und interner Kommunikationsbeziehungen zum Betrieb und zur Nutzung der Einrichtungen. Da die Versorger öffentliche Bereiche darstellen, in denen Patienten und deren Angehörige mehr wie ein Publikum verkehren, ist die Absicherung der inneren Bereiche und deren Infrastruktur nicht zu vernachlässigen.

2.1.4 Medizinische Versorgungszentren

Ein weiter Teil der medizinischen Versorgung wird durch Medizinische Versorgungszentren erbracht. Bei diesen Zentren erfolgen der Betrieb und die medizinische Versorgung durch unterschiedliche Parteien. Betreiber von Medizinischen Versorgungszentren (MVZ) können Krankenhausketten, kommunale Träger oder andere Leistungserbringer der Gesetzlichen Krankenversicherung sein. Ziel der mit dem GKV-Modernisierungsgesetz eingeführten MVZ war die Bereitstellung von fachübergreifenden medizinischen Dienstleistungen unter einem Dach durch angestellte Ärzte. Damit stellt der Betreiber des MVZ die IT-Infrastruktur für die

6 Vgl. https://www.helios-gesundheit.de/ (12.04.2019).
7 Vgl. Statistisches Bundesamt (April 2021).

einzelnen Praxen zur Verfügung und ist für deren Sicherheit und Aktualität verantwortlich. Das umfasst auch die durchgängige Einhaltung des Datenschutzes, was bei gemeinsam genutzten Infrastrukturen eine zusätzliche Herausforderung darstellt.

2.1.5 Niedergelassene Ärzte

Niedergelassene Ärzte betreiben in alleiniger Verantwortung oder in Gemeinschaftspraxen Einrichtung zur medizinischen Versorgung der Bevölkerung in spezifischen Fachrichtungen. In Deutschland gibt es ca. 115.000 niedergelassene Ärzte, wobei es deutliche regionale Unterschiede in der Ärztedichte gibt. Diese variiert zwischen 133 Einwohnern je berufstätigem Arzt in Hamburg und 248 Einwohnern je praktizierendem Arzt in Brandenburg.[8]
Als erste Anlaufstelle für medizinische Fragen nehmen niedergelassene Ärzte neben den angestellten Ärzten in den MVZ eine zentrale Rolle in der Gesundheitsversorgung ein. Als Praxisbetreiber ist diese Berufsgruppe neben der Gesundheitsversorgung auch für IT-Infrastruktur inkl. der Anbindung an TI zum Austausch von medizinischen und Abrechnungsdaten verantwortlich. Anforderungen an die Praxen zur Gewährleistung der IT-Sicherheit ergeben sich aus der IT-Sicherheitsrichtlinie nach §75b Absatz 5 des SGB V und müssen durch diese eigenverantwortlich umgesetzt werden. Ohne entsprechende Unterstützung in Form von finanzieller Unterstützung und technischen Support werden sie dieser Anforderung mit großer Wahrscheinlichkeit nicht gerecht werden können. Die Definition von Maßnahmen in Abhängigkeit der Einrichtungsgröße, wie dies in der IT-Richtlinien der Deutschen Krankenhaus Gesellschaft erfolgt, ist nicht zielführend. Das von Teilnehmern der TI ausgehende Risiko auf die klinische Infrastruktur bestimmt sich nicht aus deren Größe. Die Maßnahmen müssen sich vielmehr auf die genutzten Systeme und deren Schnittstellen beziehen.

2.1.6 Labore

Circa 1730[9] Labore erbringen in Deutschland für Krankenhäuser, Gesundheitszentren und niedergelassene Ärzte labordiagnostische Leistung und Untersuchung oder bestätigen diese. Damit tragen sie ein erhebliches Maß zur Gesundheitsversorgung der Bevölkerung bei und bilden hierbei eine Kommunikationsdrehscheibe innerhalb der klinischen Infrastruktur. Eine Digitalisierung der Prozesse in diesem Umfeld verspricht ein erhebliches Optimierungspotential, was

8 Vgl. Bundesärztekammer (31.12.2020).
9 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020a).

bei der aktuellen finanziellen Ausstattung der Labore mit ca. 3% der Ausgaben der GKV-Gesamtausgaben als unausweichlich erscheint. Hierbei basieren nahezu zwei Drittel aller klinischen Diagnosen auf Laboruntersuchungen.[10]

2.1.7 Krankenkassen

Derzeit gibt es in Deutschland 103 gesetzliche Krankenkassen[11] und 42 private Anbieter von Krankenversicherungen.[12] Das Sozialgesetzbuch weist den gesetzlichen Krankenkassen Aufgaben und Leistungen zu. Krankenkassen stellen innerhalb der klinischen Infrastruktur eine weitere Informationsdrehscheibe zwischen den Akteuren im Gesundheitswesen und der Bevölkerung dar. Zusätzlich sind die Krankenkassen und deren Verbände, nicht nur als Gesellschafter der gematik GmbH und Herausgeber der elektronischen Versichertenakte und Anbieter der elektronischen Patientenakte, bereits stark in Digitalisierungsprozesse eingebunden. Hierdurch sind Krankenkassen ein zentraler Akteur der Digitalisierung und tragen ein hohes Maß an Verantwortung für die Sicherheit der Infrastruktur und deren Nutzer.

2.1.8 Apotheken

In 2020 hatten die 18.753 öffentlichen Apotheken in Deutschland mehr als eine Milliarde Patientenkontakte.[13] Dabei sinkt die Anzahl der Einzelapotheken seit dem Inkrafttreten des GKV-Modernisierungsgesetzes im Jahr 2004 kontinuierlich. Der Trend geht klar weg von eigenständigen Filialapotheken hin zu Hauptapotheken mit zugehörigen Filialapotheken und Versandapotheken. Letztere Rubik konnte in 2020 ein Umsatzplus von 13,5% gegenüber dem Vorjahr verzeichnen, was teilweise auch auf den Pandemieeffekt zurückgeführt werden kann. [14]
Laut der Bundesvereinigung Deutscher Apothekerverbände wurde mit der Digitalisierung früher als in anderen Bereichen begonnen, zumindest was die interne Logistik und Ausgabeverfahren betrifft. Ein Beispiel sind die mehr als 34 Mio. Scann-Vorgängen von Arzneimitteln in Deutschland im Jahr.[15] In der Vernetzung mit Leistungserbringern hängt das System aber noch im internationalen Vergleich hinterher. Lösungen sind vorhanden, entwickeln sich aber nicht weiter, da der finanzielle Rahmen hierfür nicht gegeben ist.

10 Vgl. Verband der Diagnostica-Industrie (2018).
11 Vgl. GKV-Spitzenverband (22.06.2021).
12 Vgl. PKV (22.06.2021).
13 Vgl. ABDA – Bundesvereinigung Deutscher Apothekerverbände e. V. (Juni 2021).
14 Vgl. ABDA – Bundesvereinigung Deutscher Apothekerverbände e. V. (Juni 2021).
15 Vgl. ABDA – Bundesvereinigung Deutscher Apothekerverbände e. V. (Juni 2021).

2.1.9 Betreiber Telematikinfrastruktur

Die gematik GmbH hat den Auftrag, den Betrieb der Telematikinfrastrukur (TI) in der erforderlichen Qualität und unter Einhaltung der definierten Sicherheitsanforderungen sicherzustellen.[16] Zukünftig sieht sich die gematik GmbH auch als Gestalter des Regelwerks zur Zulassung und Auditierung von Teilnehmern an der TI auf Basis der durch sie definierten Sicherheitsanforderungen und Betriebsregeln.[17] Dieses Rollenverständnis birgt Konfliktpotential auf Grund von Kompetenzüberschneidungen mit dem Bundesamt für Informationssicherheit (BSI), was unter anderem zu

- einer Hemmung des Digitalisierungsprozesses
- unterschiedlichen Vorgaben für Sicherheitsstandards
- höheren Kosten

führen kann. Insbesondere im Bereich der Kritischen Infrastrukturen ist daher eine klare Rollenverteilung zwischen der gematik GmbH und dem BSI erforderlich. Daraufhin wirken und entsprechend Einfluss nehmen sollten das Bundesministerium für Gesundheit, welches 51% der Gesellschafteranteile an der gematik GmbH hält, und das Bundesministerium des Innern, für Bau und Heimat (BMI) zu dem das BSI als eine von 20 Behörden zugeordnet ist.[18]

2.1.10 Weitere Dienstleister

Neben den einzelnen benannten Akteuren gibt es noch eine große Anzahl von Teilnehmern, die in bzw. an klinische IT-Infrastrukturen angebunden sind oder mit Patienteninformationen arbeiten. Mit zunehmender Digitalisierung kann von einem weiteren Anstieg in diesem Umfeld ausgegangen werden. Insbesondere da ein Großteil der krankenhausnahen Dienstleistungen, wie Bettenmanagement, Essensversorgung oder Krankentransporte, an externe Unternehmen ausgelagert sind. Aber auch im Bereich von infrastrukturellen Dienstleistungen, wie Heizungs-, Sanitär- und Klimatechnik oder Abfallentsorgung, steigt die Nutzung von IT-Komponenten und Nutzung von Remote Überwachung und Serviceerbringung. Gerade im zuletzt genannten Umfeld der Heizungs-, Sanitär- und Klimatechnik sind oftmals Industriekomponenten im Einsatz, welche Schnittstellen und Protokolle nutzen, die oft ungenügende oder veraltete Sicherheitstechniken benutzen.

16 Vgl. gematik GmbH (26.06.2021).
17 Vgl. gematik GmbH (Dezember 2020).
18 Vgl. (25.09.2017).

Weitere Dienstleistungen im klinischen Umfeld sind gerade erst im Entstehen und drängen in den Markt. Wie hoch die Anforderungen an die Informationssicherheit und Teil eines entsprechenden Zulassungsverfahrens sein sollten, zeigt das aktuelle Beispiel am Unternehmen Doctolib GmbH, welches Patienteninformationen an Facebook und Outbrain weitergeben hat. [19] Auch wenn dies gemäß den Cookie-Richtlinien des Unternehmens rechtens war, sofern die Einwilligung durch den Nutzer vorlag, so dies aus ethischen und moralischen Gesichtspunkten bedenklich. Eine Einwilligung liegt unabhängig davon vor, ob diese durch bewusste oder unbewusste Handlung in Form der Studie und Akzeptanz der Richtlinien erfolgt. Im medizinischen Umfeld sollte daher nicht alleinig eine rechtskonforme Anwendung des Datenschutzes[20] als Kriterium für den Umgang mit personenbezogenen Daten gelten. Einer Weitergabe der Daten an Dritte muss jeder Einzelne explizit zustimmen und sofern diese für kommerzielle Zwecke genutzt werden, auch daran partizipieren. Auch eine Umkehr des Zustimmungsprinzips wäre als Lösungsansatz denkbar. Unternehmen, die Daten von Personen nutzen möchten, müssen deren Bestimmungen akzeptieren.

2.1.11 Hersteller von Medizinprodukten

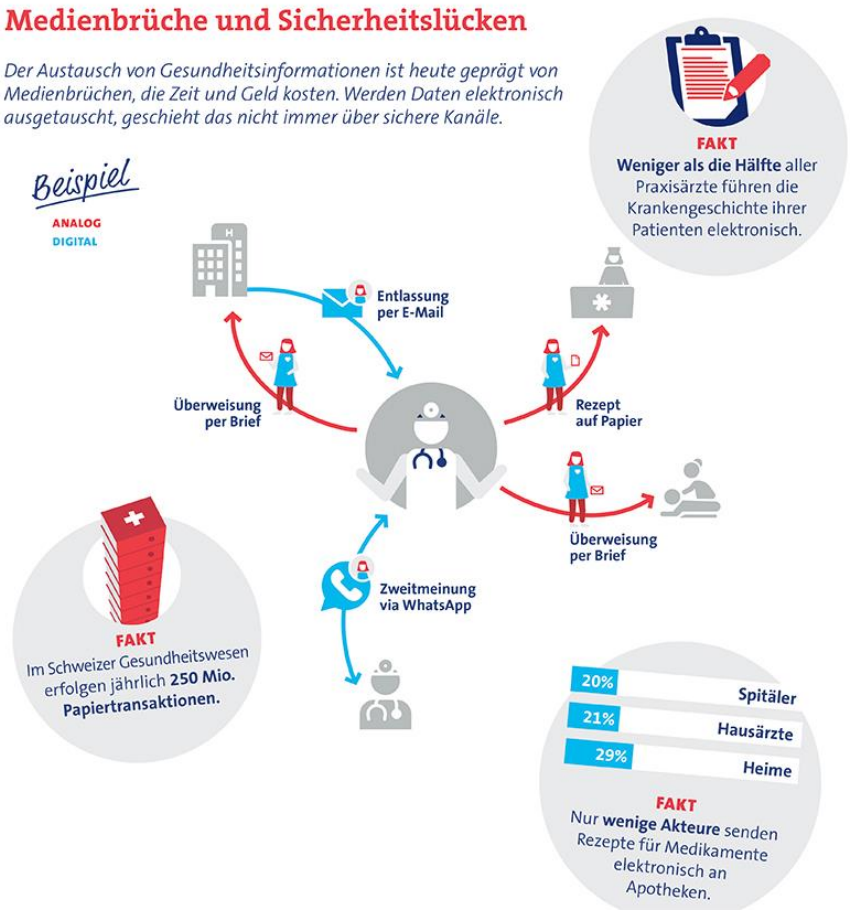
Die Hersteller von Medizinprodukten sollen an dieser Stelle als Akteure im Gesundheitswesen mit aufgeführt werden. Gründe hierfür sind die Anforderung aus den einzelnen Gesetzen, die direkt auf deren Lösungen/Produkte wirken und zu erwarten ist, dass im Zuge der Digitalisierung die Vernetzung zu den Herstellern noch stärker, z.B. durch proaktive Wartung oder Cloud-Angeboten, wachsen wird. In Deutschland gibt es mehr als 13.000 Unternehmen in der MedTech Branche. Hierbei ist die Branche sehr stark von mittelständigen Unternehmen geprägt. Nur ca. ein Prozent der Unternehmen hat mehr als 250 Mitarbeiter.[21] Daher werden die meisten dieser Hersteller nicht als kritische Infrastruktur oder als Unternehmen von besonderem öffentlichem Interesse eingestuft. Dies hat Auswirkung auf die offiziellen Sicherheitsanforderungen an die Unternehmen und birgt die Gefahr der Übernahme durch andere Unternehmen und könnte damit unmittelbare Auswirkung auf die Verfügbarkeit von Produkten und Dienstleistungen haben. Laut der Studie „Sichere Digitalisierung im Mittelstand“, die im Auftrag des Bundesministeriums für Wirtschaft und Energie erstellt wurde, besteht unabhängig von deren Größe auch ein erheblicher Nachholbedarf im Security-Umfeld.[22]

19 Vgl. t3n Magazin (2021).
20 Vgl. datenschutz cert GmbH (2020).
21 Vgl. Bundesverband Medizintechnologie (1. Oktober 2020).
22 Vgl. Martin Lundbor, Pirmin Puhl, Annette Hillebrand, Sebastian Tenbrock, Julia Wielgosch (Januar 2020).

Mögliche Auswirkungen des Ausfalls von Herstellern sollten daher immer mit Bestandteil von Risikoanalysen sein.

2.2 Kommunikationsbeziehungen

Zwischen den Akteuren im Gesundheitswesen und zum Patienten bestehen eine Vielzahl von Kommunikationsbeziehungen und Schnittstellen. Durch die fortschreitende Digitalisierung kommen weitere IT-Schnittstellen und Datenflüsse hinzu und ersetzen bestehende analoge Übergänge und reduzieren somit die Medienbrüche. Jedoch erhöhen weitere IT-Schnittstellen und Datenübertragungen das Risiko für die digitalen Infrastrukturen durch neue Gefährdungen und eine größere Anzahl an potenziellen Angriffsvektoren. Allein zur Meisterung der anstehenden Herausforderungen im Gesundheitswesen durch Überalterung der Gesellschaft und zur Bewältigung der Ressourcen-Knappheit erscheint dieser Weg jedoch alternativlos.



Quelle: Galledia Fachmedien AG 21, June 2017

Abbildung 1: Darstellung von Medienbrüchen und Sicherheitslücken des Schweizer Gesundheitssystems

Die heute vorherrschende Praxis der postalischen Kommunikation über den Arztbrief und Übermittlung von Röntgenbildern via mobile Datenträger, partiell auch über regionale/institutionelle Plattformen, soll über einen gesicherten elektronischen Postversand- und Datenaustausch auf Basis der TI abgelöst werden. Die nachfolgende Darstellung gibt eine Übersicht zu den heutigen Kommunikationsschnittstellen und -medien zwischen den Teilnehmern der klinischen Infrastrukturen.

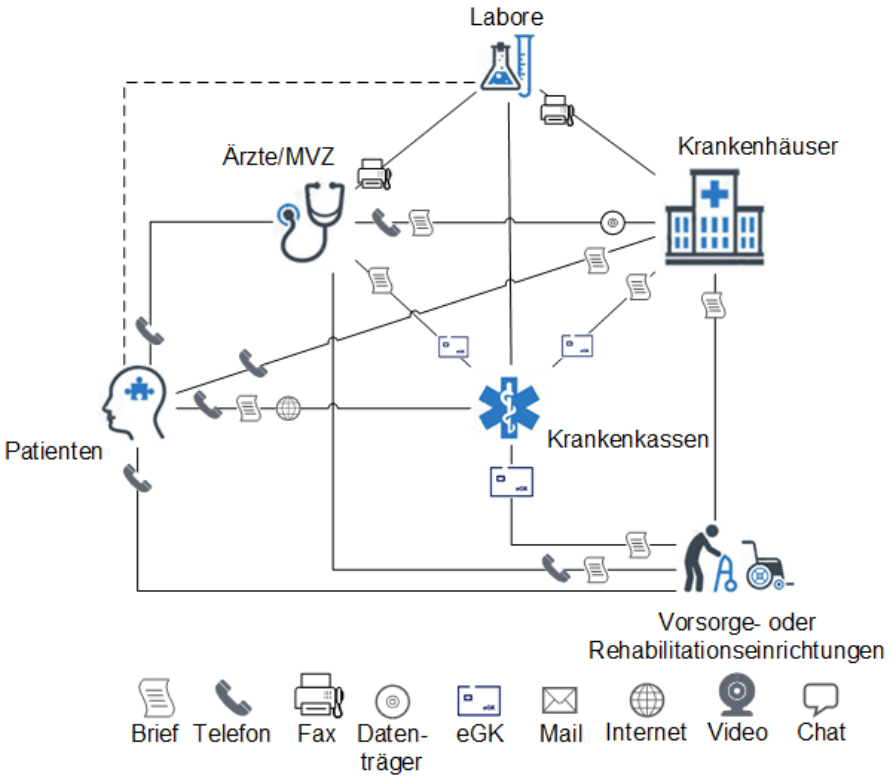


Abbildung 2: Kommunikationsschnittstellen und -medien zwischen den Teilnehmern der klinischen Infrastrukturen

Mit der Digitalisierung ergibt sich durch die Umsetzung von gesetzlichen Anforderungen zur Verschlüsselung und der Signierung der Kommunikation und Datenübertragung auch eine Änderung der Datenflusssteuerung. Dies soll in der nachfolgenden Abbildung veranschaulicht werden.

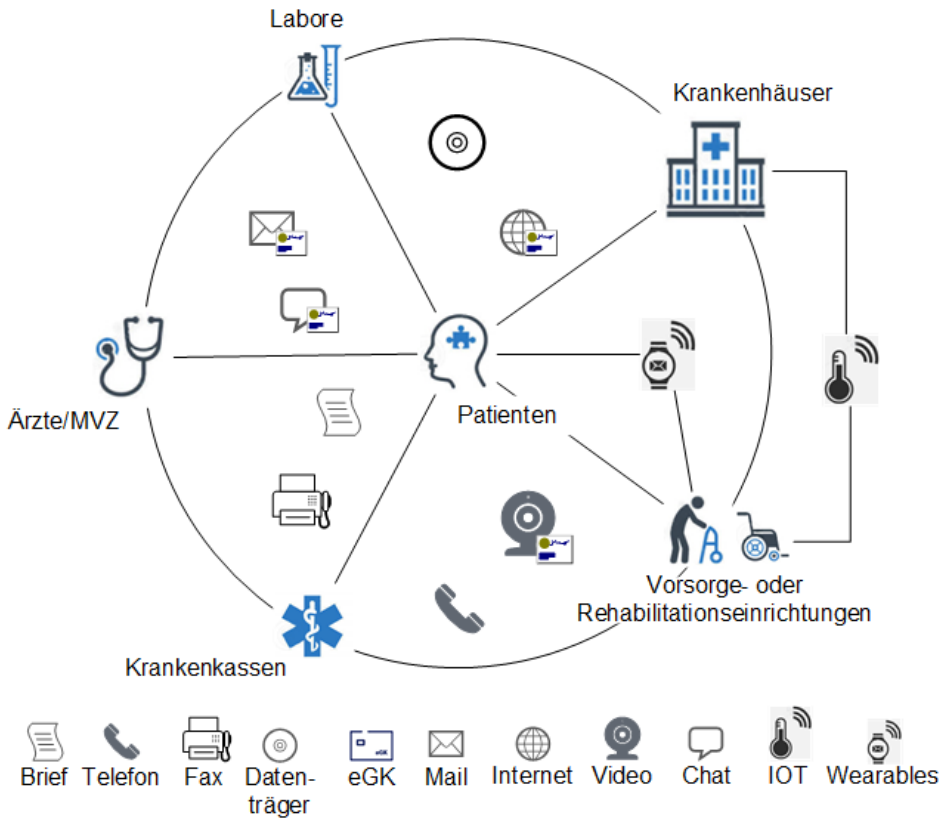


Abbildung 3: Kommunikationsschnittstellen und -medien zwischen den Teilnehmern der klinischen Infrastrukturen

Zusätzlich kommen auch neue Schnittstellen hinzu, deren Betrachtung ebenso erforderlich ist, wie die notwendige Bewertung des Risikos der angestrebten Übertragung der Datenhoheit an den Patienten. Insbesondere die Einbindung von Geräten mit geringen Sicherheitsniveau und fehlenden Managementfunktionalitäten erfordert zusätzliche Maßnahmen zur Abschirmung der Kern-Infrastrukturen und der kritischen Dienstleitung (kDL). Neben den Anforderungen, die sich aus den zusätzlichen Schnittstellen ergeben, können die bestehenden Strukturen nicht gänzlich vernachlässigt werden. Die bisherigen analogen Prozesse müssen im Rahmen des Notfallmanagements weiterhin aufrechterhalten und trainiert werden.

3 Digitalisierung

3.1 Was bedeutet Digitalisierung

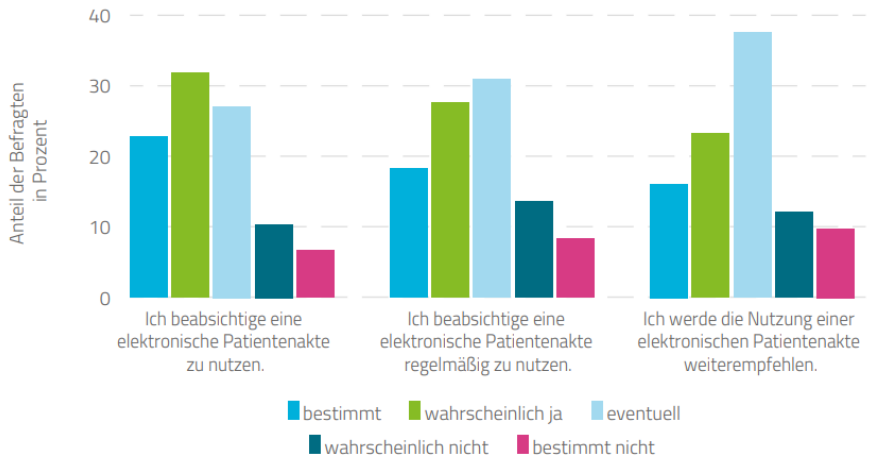
Ursprünglich bedeutet Digitalisierung die Umwandlung von analogen Daten in digitale Formate.[23] Doch um das Potential der Digitalisierung nutzen zu können, ist dies nicht ausreichend, eine Wandlung von Papierdokumenten in ein elektronisch lesbares Format vorzunehmen oder die Daten in einem digitalen Format direkt zu erfassen, um Abläufe effizienter zu gestalten. Es ist erforderlich, die Daten in entsprechend angepassten Prozess für nachgelagerte Anwendung verfügbar zu machen und zu verarbeiten. Das Institute of Electronic Business e.V. sieht in seiner Studie zur Digitalisierung folgende 4 Schlüsselfaktoren:[24]

- Technologie
- Kommunikation
- Gesellschaft & Politik
- Wirtschaft & Arbeit

Die verfügbaren Technologien bilden hierbei die Grundlage für die Digitalisierung. Aber erst durch die Vernetzung der Daten (Kommunikation) kann das ganze Potential entfaltet werden. Die Entwicklung und Impulse aus den Bereichen Gesellschaft & Politik und Wirtschaft & Arbeit beeinflussen die Geschwindigkeit der Transformation durch Faktoren wie Akzeptanz und Veränderungsfähigkeit maßgeblich.

Das derzeit eine hohe Akzeptanz innerhalb der deutschen Bevölkerung für die Digitalisierung im Gesundheitswesen vorhanden ist, zeigt zum einen die Studie der BARMER Krankenkasse aus 2019, welche eine hohe Nutzungsabsicht der elektronischen Patientenakte attestiert, und die Bevölkerungsumfrage des Bundesverband Digitale Wirtschaft e.V. zum Thema Digitalisierung in der Gesundheitsversorgung.[25]

23 Vgl. Luber (26.06.2021).
24 Vgl. Prof. Dr. Dr. Thomas Schildhauer (2018).
25 Vgl. Daniel Sonnenberg (August 2019).



Quelle: Repschläger/Schulte/Osterkamp, 2019

Abbildung 4: Bewertung der Nutzungsabsicht der ePA, n = 1.000

Auf die Frage

*„Wenn Künstliche Intelligenz Krankheiten mit einer **höheren Wahrscheinlichkeit** erkennen kann bzw. Diagnosen treffender erstellen kann als Menschen, sollten dann Ärzte dazu verpflichtet werden, diese Technik als automatisierte **Zweitmeinung** in die Untersuchung miteinzubeziehen?“*[26]

haben sich mehr als die Hälfte der Befragten dafür ausgesprochen.

Quelle: Jennifer Hammel, 25.06.2019a

Abbildung 5: Bundesverband Digitale Wirtschaft e.V. Grafik Health Studie

Die Akzeptanz der Lösung schwindet hierbei gleichermaßen mit nachlassendem Vertrauen in die Sicherheit. Daher ist die Grundlage einer erfolgreichen Digitalisierung die Schaffung einer sicheren Infrastruktur und des Bewusstseins für Sicherheit bei den handelnden Personen. Denn wenn dieses Vertrauen in die Technologie durch Sicherheitsvorfälle zerstört und damit nicht mehrgeben ist, wird die

26 Vgl. Jennifer Hammel (25.06.2019b).

Digitalisierung nicht die Ziele erreichen, die man sich von ihr erhofft. Besonders treffend hierzu formulierte Dieter Hallervorden folgenden Satz.

„Vertrauen ist wie ein Eiswürfel.
Einmal geschmolzen, kommt es nicht mehr zurück.“[27]

3.2 Status der Digitalisierung im Gesundheitswesen

Die Meinungen zum Digitalisierungsgrad im Gesundheitsumfeld allgemein und im Krankenhaus gehen auseinander. Um den Digitalisierungsgrad innerhalb klinischer Infrastrukturen messen zu können, wurde durch die Healthcare Information and Management Systems Society (HIMSS) das Electronic Medical Records Adoption Model (EMRAM) entworfen. Dieses gibt den Digitalisierungsgrad in 8 Stufen an. Beginnend mit Stufe 0, wo nahezu keine digitalen Systeme implementiert sind, bis Stufe 7, bei der ein Krankenhausbetrieb vollständig papierlos erfolgt.

Stufe	Kriterien	Anteil der KH in D [%]
Stufe 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
Stufe 6	Klinische Dokumentation interagiert mit intelligenter klinischer Entscheidungsunterstützung (basierend auf diskreten Datenelementen) UND Vorhandensein eines IT-gestützten, geschlossenen Medikationsprozesses (*closed loop medication*).	1,2
Stufe 5	Integrierte Bildmanagementlösung (z. B. PACS) ersetzt alle filmbasierten Bilder.	18,0
Stufe 4	Elektronische Verordnung mit klinischer Entscheidungsunterstützung in mindestens einem klinischen Bereich und für Medikation.	5,4
Stufe 3	IT-gestützte klinische Dokumentation sowie Einsatz elektronischer Verordnungen durch Ärzte bzw. Pflegepersonal. Dies beinhaltet auch die Dokumentation der Medikamentengabe (eMAR).	9,0
Stufe 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
Stufe 1	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind installiert.	1,2
Stufe 0	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind nicht installiert.	38,3
	N	167
	EMRAM-Mittelwert	2,3

Quelle: Jürgen Klauber, Max Geraedts, Jörg Friedrich, Jürgen Wasem Hrsg., 2019

Tabelle 1: EMRAM Stufenmodell mit einzelnen Kriterien und Anteil der deutschen Krankenhäuser (2017)

27 Vgl. Dieter Hallervorden (4. März 2021).

Eine pauschale Übertragung der Werte auf alle Krankenhäuser in Deutschland ist nicht möglich. Demnach würden die Stufe 6 in Deutschland 22 Krankenhäuser erreichen. Tatsächlich ist derzeit mit der Medius Klinik Nürtingen[28] nur eine Klinik in Deutschland gemäß dieser Stufen durch die HIMSS zertifiziert.
Wie aus der nachfolgenden Tabelle entnommen werden kann, belegt Deutschland im internationalen Vergleich mit einem Durchschnittswert von 2,3 auf der EMRAM-Scala einen der hinteren Plätze bei der Digitalisierung im Gesundheitswesen. Im europäischen Vergleich liegt der durchschnittliche digitale Reifegrad nach diesem Modell mit 3,6 eineinhalb Stufen über dem von Deutschland. In Bezug auf die Vereinigten Staaten von Amerika ist der Krankenhaussektor in Deutschland in der Digitalisierung sogar bereits mit 3 Stufen im Rückstand.

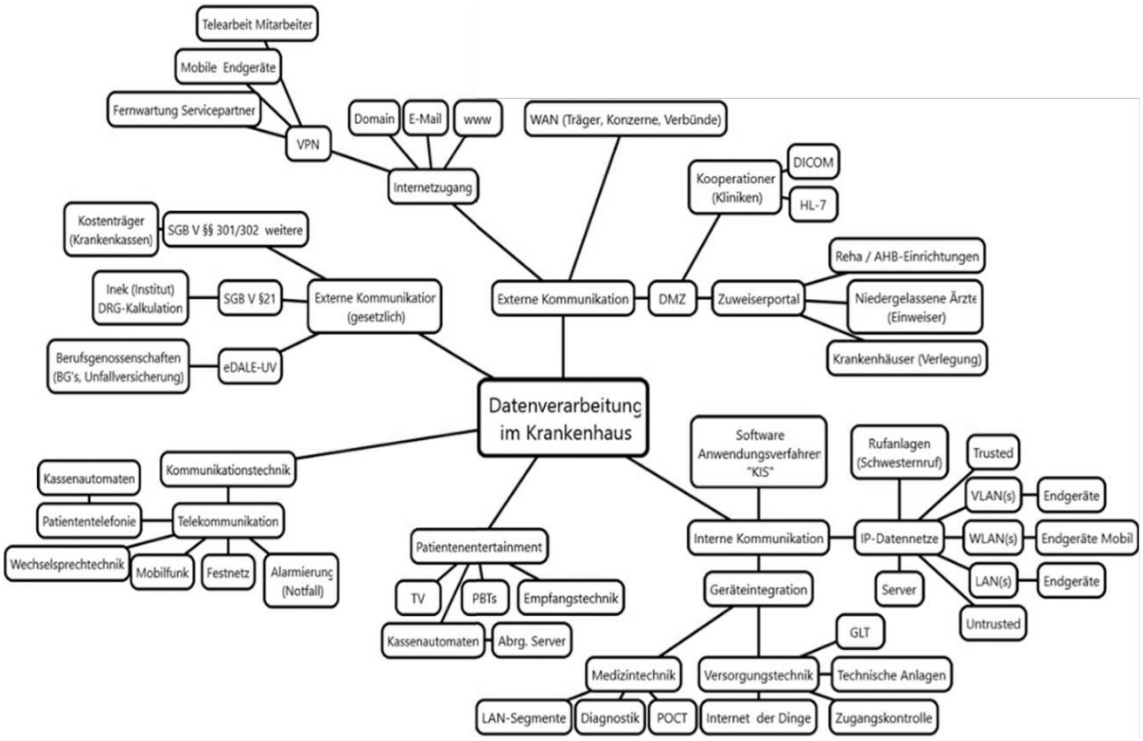
	Deutschland	Österreich	Europa	UK	Türkei	Spanien	Niederlande	USA	Dänemark
Level 7	–	–	0,3	–	0,1	–	5,6	6,4	
Level 6	1,2	5,6	13,4	2,9	24,2	5,1	5,6	33,8	4,2
Level 5	18,0	11,1	30,0	52,4	19,1	50,0	66,7	32,9	95,8
Level 4	5,4	–	4,9	3,8	6,5	4,5	–	10,2	–
Level 3	9,0	–	5,2	–	5,9	3,2	–	12,0	–
Level 2	26,9	50,0	28,8	14,3	32,3	26,3	19,4	1,8	–
Level 1	1,2	5,6	6,0	9,5	5,0	1,9	2,8	1,5	–
Level 0	38,3	27,8	11,4	17,1	7,0	9,0	–	1,4	–
N	167	18	1.455	105	682	156	36	5.487	24
EMRAM-Mittelwert	2,3	2,3	3,6	3,7	3,8	3,9	4,8	5,3	5,4

Quelle: Jürgen Klauber, Max Geraedts, Jörg Friedrich, Jürgen Wasem Hrsg., 2019

Tabelle 2: Anteil der Krankenhäuser in den verschiedenen EMRAM-Stufen in verschiedenen Ländern/Regionen (2017) [%]

Hieraus Rückschlüsse auf die Qualität der Medizinischen Versorgung zu ziehen, wäre sicherlich nicht gerecht und genauso verfrüht, wie die Schlussfolgerung, dass in den Krankenhäusern eine einfache, nicht komplexe IT-Infrastruktur anzutreffen ist. Insbesondere wenn man sich vergegenwärtigt, dass diese Infrastruktur möglichst eine Verfügbarkeit von 100%, zu mindestens für die betriebskritischen Systeme, und dies auch unter Berücksichtigung von planmäßigen Wartungsarbeiten gewährleisten muss. Redundanzen haben daher höchste Priorität und erfordern einen hohen finanziellen Aufwand. Die nachfolgende Übersicht soll die Komplexität der Datenverarbeitung im Krankenhaus verdeutlichen, stellt hierbei jedoch keine abschließende Übersicht der Applikationen im Krankenhaus dar.

28 Vgl. HIMSS Analytics - Europe (2019).



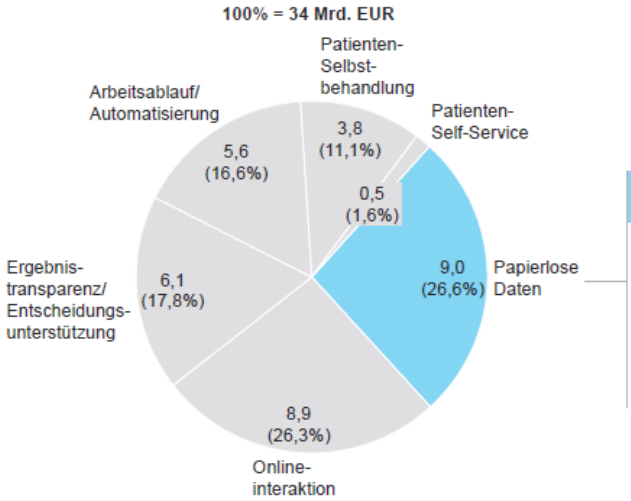
Quelle: Michael Thoss, 30. Mai 2020

Abbildung 6: Übliche Datenverarbeitung im Krankenhaus

Allerdings leistet sich Deutschland, bei einem vergleichsweise geringen Digitalisierungsgrade, eines der teuersten Gesundheitssysteme weltweit. Laut der Studie „Germany: Country Health Profile 2019“ der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung liegt die Prokopfausgabe für das Gesundheitssystem in Deutschland bei 4.300 Euro.[29] Damit wird 11,2% des Bruttoinlandsprodukts für das Gesundheitssystem aufgewendet, was nur durch die Schweiz mit 12,3% des Bruttoinlandsproduktes übertroffen wird.[30]

Inwieweit ein steigender Digitalisierungsgrad zur Kostenreduzierung bei gleichzeitiger Steigerung der Kosten für IT-Infrastrukturen und Sicherheit beitragen kann, so wie dies das Beratungshaus Mc Kinsey&Company in seiner Studie „Digitalisierung in deutschen Krankenhäusern“[31] voraussagt, wird sich nach Umsetzung der angesetzten Maßnahmen zeigen.

29 Vgl. (2019).
30 Vgl. Maier (04.05.2020).
31 Vgl. Dr. Steffen Hehner, Dr. Karl Liese, Gerald Loos, Dr. Manuel Möller, Dr. Stephanie Schiegnitz, Tobias Schneider, Dr. Mark Oellerich, Dr. Max Plischke, Anke Donath, Nadine Erk (September 2018).



	in Mrd.	in %
Einheitliche elektronische Patientenakte/Austausch	**6,4**	**18,8**
Elektronische Rezepte („E-Rezept“)	0,9	2,7
Krankenhausinterne Mitarbeiterkommunikation	0,9	2,6
Virtuelle Arztassistenten (künstliche Intelligenz)	0,8	2,5

Quelle: Dr. Steffen Hehner, Dr. Karl Liese, Gerald Loos, Dr. Manuel Möller, Dr. Stephanie Schiegnitz, Tobias Schneider, Dr. Mark Oellerich, Dr. Max Plischke, Anke Donath, Nadine Erk, September 2018

Abbildung 7: Kosteneinsparungen je digitale Lösungskategorie in Mrd. Euro

Voraussetzung hierfür ist eine möglichst flächendeckende Umsetzung der jeweiligen Lösung. Insbesondere die mehrfach verschobene Einführung der ePA, als eine von der derzeit sechs Digitalisierungsvorhaben auf Basis der Telematikinfrastruktur, spielt dabei mit einem erwartetem Einsparpotential von ca. 6,4 Mrd. Euro eine zentrale Rolle.

Der erste Schritt zu einer flächendeckenden Bereitstellung von digitalen Angeboten innerhalb von klinischen Infrastrukturen scheint jetzt jedoch mit der verpflichtenden Anbindung aller vertragsärztlich tätigen Leistungserbringer zum 01. Juli 2021 und der Anbindung aller Krankenhäuser bis zum 01. Januar 2022 an die TI gemacht zu sein. Zum Start wird das Angebot auf einige wenige Anwendungsfälle begrenzt sein und auch ein spezifisches Rechtemanagement zur dedizierten Bereitstellung von Daten steht nicht zur Verfügung. Nachfolgende Anwendung enthalten allerdings für die Zukunft ein vielversprechendes Potential, das Gesundheitswesen nachhaltig positiv zu beeinflussen.

- Elektronische Arbeitsunfähigkeitsbescheinigung (eAU)
- Notfalldaten-Management
- Elektronischer Medikationsplan (eMP)
- Elektronisches Rezept (e-Rezept)
- Kommunikation im Medizinwesen (KIM)
- Versichertenstammdaten-Management (VSDM)
- TI-Messenger

Bedauerlicherweise fehlen derzeit Ansätze und Bestrebungen, eine dringend benötigte zentrale Speicherung und Verwaltung der Patientendaten in einer „Bundes-eHealth-Cloud“ bereitzustellen. Hiermit müssten z.B. bei einem Wechsel der

Krankenversicherung die Rechte für den Zugriff auf die Daten durch den Nutzer lediglich geändert werden. Derzeit ist es erforderlich, dass er seine Daten selbst sichert und an den neuen Leistungserbringer übermittelt. Dieses Vorgehen bedingt bei dem vormaligen Versicherungsunternehmen zusätzliche Prozesse für die Aufbewahrung und spätere Löschung der Daten gemäß den gesetzlichen Vorgaben. Mechanismen zur Unterstützung des Datentransfers scheinen auch nicht durchgängig zur Verfügung zu stehen.

3.2.1 Status der Anwendungen der Telematikinfrastruktur

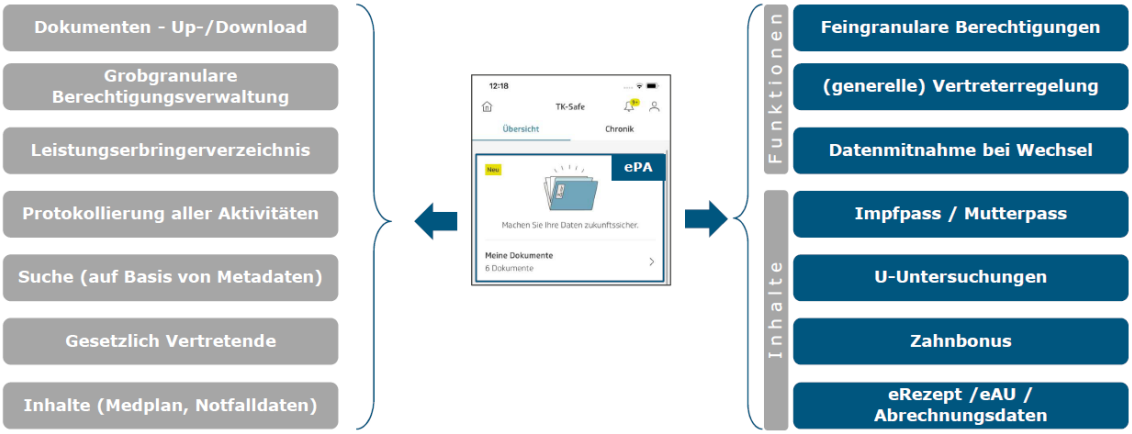
3.2.1.1 Elektronische Patientenakte

Seit dem 01. Januar 2021 haben Versicherte einen gesetzlichen Anspruch auf die Elektronische Patientenakte, wobei das Angebot nicht verpflichtend durch die Versicherten genutzt werden muss. Hierfür muss der Versicherte einen entsprechenden Antrag bei seiner aktuellen Krankenversicherung stellen. Im zweiten Schritt ist die Installation der ePA-App seiner Krankenversicherung auf dem Smartphone oder Tablett erforderlich, eine Version für Desktop-Computer mit Windows oder Linux-Betriebssystem oder der Zugriff über Browser steht derzeit nicht zur Verfügung. Dies liegt laut der gematik GmbH in der mehrheitlichen Nutzung von mobilen Anwendungen durch die Versicherten und in den Sicherheitsvorteilen von Apps gegenüber browserbasierten Zugriffen begründet. So sind Authentifizierungsverfahren, z.B. über das Scannen von biometrischen Merkmalen, über Apps auf mobilen Endgeräten auf Grund deren dort häufig verfügbaren Lösungen einfacher realisierbar. [32]

In der ePA sollen folgende Daten gespeichert werden.[33]

- Diagnosen und Befunde
- Vorerkrankungen
- Allergien
- Impfungen
- Medikationspläne, Therapien, Behandlungsmaßnahmen
- ärztlicher Schriftverkehr
- Blutwerte
- Röntgenbilder
- Impfausweis, Zahn-Bonusheft, Mutterpass, Kinder-Untersuchungsheft (ab 2022)

32 Vgl. gematik GmbH (2021c).
33 Vgl. VFR Verlag für Rechtsjournalismus GmbH (11. August 2021).



Quelle: Dr. Markus Schlobohm, 28.09.2021

Abbildung 8: ePA-Funktionalitäten und Inhalte in 2022

Auf Grund des fehlenden Rechtemanagements kann der Versicherte nicht unterscheiden, welche Daten, in welchem Umfang und Tiefe er diese bestimmten Einrichtungen, Organisationen und Personen zur Verfügung stellen möchte. Aus Datenschutzgründen wird dies als bedenklich angesehen, insbesondere da es sich hierbei um die Verarbeitung von besonderer Kategorie gemäß Artikel 9 der DSGVO handelt.[34]

Neben der zügigen Abstellung von noch bestehenden Mängel bleibt die Aufmerksamkeit darauf zu lenken, dass die parallele Entwicklung von privatwirtschaftlichen Lösungen den Erfolg der ePA nicht gefährdet. So ist zu prüfen, inwieweit bei der Entwicklung des aktuell in der Einführung befindlichen digitalen Impfausweises die Anforderungen zur Überführung in die ePA berücksichtigt wurden, um eine entsprechende Datenübernahme zu ermöglichen. Eine gesetzliche Regelung zur Pflicht besteht hierzu gemäß §6a der Digitalen Gesundheitsanwendungs-Verordnung (DiGAV) erst ab dem 01. Januar 2023. So erscheint die gleichlaufende Entwicklung von Anwendungen im Rahmen der Covid-19-Pandemie mehr dazu geeignet zu sein, zusätzliche Kosten durch den Betrieb von parallelen Infrastrukturen zu erzeugen, statt dass es zu Kosteneinsparungen kommt.

3.2.1.2 Elektronische Arbeitsunfähigkeitsbescheinigung

Die eAU tritt mit den Zielen an, die Medienbrüche bei der Übermittlung der Daten zur Arbeitsunfähigkeit zu reduzieren, sicherer und schneller zu gestalten und dabei durch Einsparung von Tonnen an Papier für die jährlichen ca. 77 Millionen Krankschreibungen einen Anteil am Umweltschutz zu leisten.[35]

34 Vgl. Detlef Baer (31.07.2021).
35 Vgl. Harald Czycholl (04.01.2021).

Zum Start erfolgt hierbei nur eine Teilautomatisierung des Gesamtprozesses, indem lediglich die Übermittlung der Daten zwischen den Krankenkassen und Ärzten in elektronischer Form erfolgt. Erst 9 Monate später, mit der verpflichtenden Bereitstellung von elektronischen Identitäten für alle Versicherten zum 01. Juli 2022 ist auch eine Übermittlung der Informationen zum Arbeitgeber vorgesehen.[36] Die Übermittlung erfolgt dabei nicht automatisch, sondern der Arbeitgeber muss sich diese Daten abholen. Auch bleibt der Arbeitnehmer weiterhin in der Pflicht, seinen Arbeitgeber über seine Arbeitsunfähigkeit zu informieren. Ebenfalls bestehen bleibt nach §73 Absatz 3 Satz 9 die Pflicht zur Aushändigung einer Arbeitsunfähigkeitsbescheinigung durch den behandelnden Arzt, auch wenn die Übermittlung parallel in elektronischer Form erfolgt. Die gesteckten Ziele dürften damit nicht erreicht werden können, da Medienbrüche über die Übergangszeit hinaus bestehen bleiben und auch weiterhin physische Bescheinigungen genutzt werden.

Der gesteckte Zeitplan erscheint hierbei ebenfalls ambitioniert. Ein Grund hierfür ist die durchgehende notwendige Nutzung des KIM-Dienstes über die TI durch alle beteiligten Akteure. Ein anderer Anhaltspunkt hierfür stellt die kurze Übergangszeit für den Verfahrenswechsel von 10 Monaten zwischen Kommunikation der Verfahrensbeschreibung zum Datenaustausch im Rahmen des eAU-Prozesses zwischen Krankenkassen und AG dar.[37]

3.2.1.3 Notfalldaten-Management

Ein Versicherter hat die Möglichkeit, über seinen Hausarzt eine Notfalldatensatz über sich anlegen zu lassen. Hierzu werden nachfolgend dargestellte Daten über das Praxisverwaltungssystem erfasst und auf der elektronischen Gesundheitskarte (eGK) gespeichert.

Quelle: gematik GmbH, 2021f

Abbildung 9: Daten des Notfalldatensatzes

36 Vgl. GKV-Spitzenverband (28.09.2021a).
37 Vgl. GKV-Spitzenverband (28.09.2021b).

Neben den Informationen der Gesundheitsdaten für die Notfallversorgung kann der Versicherte mit dem Organspendeausweis, der Patientenverfügung und der Vorsorgevollmacht weitere persönliche Erklärungen hinterlegen lassen. Zum Schutz der Daten kann der Zugang via PIN gesichert werden. Wie sicher diese Daten tatsächlich sind, muss vor dem Hintergrund, dass ein Zugriff im Notfall auch ohne Zustimmung des Versicherten möglich ist, hinterfragt werden. Weiterhin ergeben sich zur Datenspeicherung in Bezug auf Datenschutz weitere ungeklärte Fragen. Zum einen wird bei der Erstellung des Notfalldatensatzes (NFD) als auch beim Auslesen eine lokale Kopie auf dem Praxisverwaltungssystem (PVS) bzw. dem Krankenhausinformationssystem (KIS) angelegt. Auch fehlt derzeit ein Ansatz zur Datenübernahme aus der ePA, was eine doppelte Eingabe von Patientendaten erforderlich macht. Beides widerspricht dem Grundsatz der Datensparsamkeit. Die Lösung hierfür könnte auch die Bereitstellung der angesprochenen „Bundes-eHealth-Cloud“ sein.

3.2.1.4 Elektronischer Medikationsplan

Der elektronische Medikationsplan dient dem Informationsaustausch zwischen den Akteuren im Gesundheitswesen, wie Ärzten, Apotheken u.w., über die dem Versicherten verschriebene Medikamente und deren Anwendung (Medikationsplan). Hierdurch sollen unerwünschte Wechselwirkungen durch Verschreibung bzw. der Verschreibung von weiteren Medikamenten vermieden werden. Applikationen, die auf Basis dieser Informationen für den Versicherten oder auch für das Krankenhauspersonal einen automatisierten Medikationsplan mit Erinnerungsfunktion zur Einnahme erstellten und so das Potential der Digitalisierung weiterausbauen, sind aktuell nicht verfügbar. Dies kann zum einen an der geringen Verbreitung des eMP liegen. Vielmehr wird die Ursache aber darin zu suchen sein, dass eMP-Apps als Medizinprodukte einzustufen sind und daher besondere Zulassungsverfahren durchlaufen müssen.
Informationen zur Unterscheidung der Funktionalität des elektronischen Medikationsplans gegenüber den Medikationsplänen auf der ePA sind derzeit nicht verfügbar. Eine Überführung in der ePA ist aber laut Landesärztekammer Baden-Württemberg geplant.[38]

38 Vgl. Landesärztekammer Baden-Württemberg (31.07.2020).

3.2.1.5 Elektronisches Rezept

Das elektronische Rezept ist laut eigener Angabe das erste eigene Produkt der gematik GmbH und soll das Potential zur Erleichterung des Lebens für Millionen Menschen haben und ab dem 01. Juli 2021 zur Verfügung stehen.[39] Nach einer Testphase in der Region Berlin und Brandenburg soll der bundesweite RollOut im Oktober 2021 starten und ab 2022 die Nutzung die Regel sein. Jedoch wurde der bundesweite RollOut einen Tag vor dem geplanten Termin durch die gematik GmbH abgesagt.[40] Angeführt für diese kurzfristige Absage wurden zwei Gründe. Zum einen war nur für zwei von 130 Praxis- bzw. Apothekenverwaltungssystemen das hierfür notwendige Programmupdate verfügbar und anderseits stockt die Ausstattung der Versicherten mit den erforderlichen neuen Gesundheitskarten, so dass nur ca. ein Prozent von den 73 Mio. Versicherten entsprechend ausgestattet sind. Zu dieser Situation hat sicherlich auch die Uneinigkeit hinsichtlich der Bestellung der neuen eGK zwischen den Krankenkassen und der gematik GmbH.[41] Ein weiterer Grund liegt sicherlich auch in der fehlenden Umsetzung der notwendigen flächendeckende Anbindung aller Akteure an die TI. Dass dies noch nicht durchgängig der Fall ist, macht die Ausstellung des digitalen Nachweises zur Covid-19-Impfung deutlich.[42]

Damit der Prozess der papierlosen Medikamentenverschreibung und Ausgabe funktioniert, ist eine hohe Verfügbarkeit der Gesamtlösung erforderlich. Mehrtätige Ausfälle der Anwendung, wie dies nach einem Sicherheitsvorfall am 21. Juli 2021 für den digitalen Covid-19-Impfnachweis der Fall war, würden den gesamten Prozess in Frage stellen und das weitere Vorhalten von entsprechenden Papierrezepten notwendig machen.[43] Da stimmt es doch positiv, wenn das BSI zum 01. Juli 2021 die prinzipielle Sicherheit der Applikation attestiert hat. [44] Inwieweit die Sicherheit tatsächlich dauerhaft gegeben ist, muss bei einer Installationsfähigkeit unter Android 6 in Frage gestellt werden, da für diese Betriebssystemversion keine Security Updates mehr bereitgestellt werden.[45] Ebenfalls ein positiver Ausblick stellt die angestrebte Übernahme der Daten bzw. deren Verknüpfung mit den elektronischen Medikationsdaten dar. Auch wenn noch an einige Prozessschritte, wie z.B. der Abholung von Medikamenten durch Dritte, gearbeitet werden muss, kann man der gematik GmbH in Bezug des Potentials der Anwendung folgen.

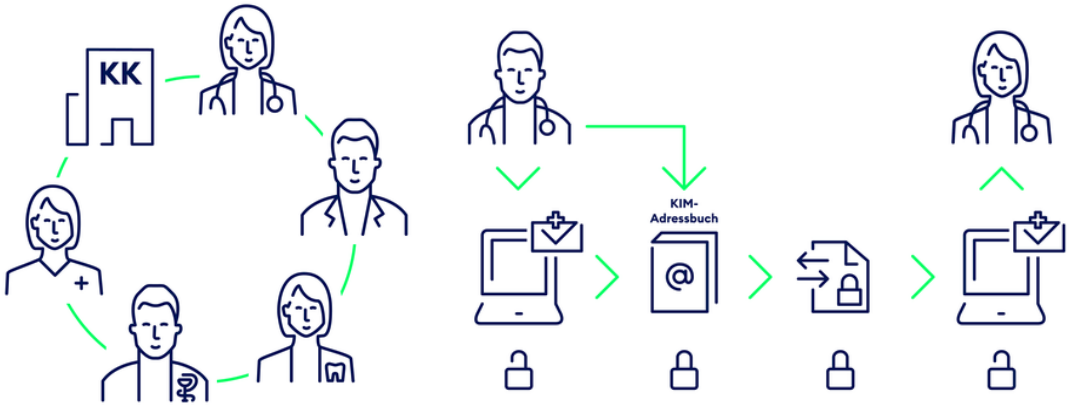
39 Vgl. gematik GmbH (2021b).
40 Vgl. Adhoc (08.10.2021).
41 Vgl. Adhoc (22.08.2021).
42 Vgl. Apotheke Adhoc (30.07.202).
43 Vgl. Einhorn Apotheke am Stern (27.07.2021).
44 Vgl. Bundesamt für Sicherheit in der Informationstechnik (01.07.2021).
45 Vgl. endoflife.date (2021).

3.2.1.6 Kommunikation im Medizinwesen

Mittels der TI-Anwendung KIM soll ein Austausch von Nachrichten und Dokumenten schnell, zuverlässig und sicher zwischen den Akteuren im Gesundheitswesen ermöglicht werden. Hierzu werden die Nachrichten ab der Konnektor-Schnittstelle signiert und verschlüsselt. Ein Austausch ist damit aber nur zwischen Teilnehmern der TI möglich. Die Kommunikation mit anderen Dienstleistern oder Versicherten muss über einen anderen Kommunikationskanal erfolgen, was zu einem Medienbruch führt und damit nicht förderlich für Digitalisierung ist. Daher stimmt die Aussage seitens der gematik GmbH

„KIM vermeidet Medienbrüche und spart Zeit“[46]

nicht für alle am Prozess Beteiligten. Jedoch stellt diese eine sehr gute Alternative zum Austausch von Labordaten zwischen den Laboren und Krankenhäusern via Fax-Kommunikation dar, welche auf Grund der Umstellung der öffentlichen Kommunikationsnetze von ISDN auf IP sehr störanfällig und unzuverlässig geworden ist. Auch in Bezug auf aktuelle Datenschutzanforderungen genügen Fax-Dienste nicht mehr, wenn die Endgeräte nicht nur ausschließlich für den Personenkreis zugänglich sind, der Kenntnis über diese bereitgestellten Informationen erlangen muss bzw. darf.



Quelle: gematik GmbH, 2021d

Abbildung 10: sichere Kommunikation in geschlossener Nutzergruppe auf Basis KIM

3.2.1.7 Versichertenstammdaten-Management

Über das Versichertenstammdaten-Management hat der Leistungserbringer die Möglichkeit, die Versichertendaten direkt von der Krankenkasse abzurufen und ggf. vorliegende Updates in das PVS/KIS zu übernehmen. Diese Anwendung könnte in der ePA aufgehen, wobei dies derzeit nicht beschrieben ist. Auf Grund der freiwilligen Nutzung der ePA werden bis auf weiteres beide Verfahren eine Koexistenz haben.

46 Vgl. gematik GmbH (2021e).

3.2.1.8 TI-Messenger

Mit dem TI-Messenger soll ab 2022 eine Anwendung für dringende Ad-hoc-Messages zur Verfügung gestellt werden. In Abgrenzung zu KIM soll die Kommunikation mittels des TI-Messengers nicht auf die Akteure des Gesundheitswesens begrenzt bleiben, sondern eine Kommunikation auch mit den Versicherten erlauben. Hierbei soll die Kommunikation über alle Medien, via Text, Sprache und Bild, möglich sein sowie die Übermittlung von Dateien ermöglichen. Der Auftrag zur Entwicklung einer entsprechenden Anwendung, deren letzte Ausbaustufe mit allen Anwendungen bereits zum 1. Oktober 2023 verfügbar sein soll, beruht auf dem Digitale-Versorgungs- und Pflege-Modernisierungs-Gesetz (DVPMG).
Als Basis für diese Anwendung wird nach dem Willen der gematik GmbH die open source Anwendung Matrix genutzt. Die Integration des TI- Messengers in die Patientensysteme soll den jeweiligen Anbietern obliegen. Für die Integration in die ePA Anwendung liegt die Umsetzung verpflichtend bei den jeweiligen Krankenkassen.[47] Im Gegensatz zur heutigen Bereitstellung der ePA-Anwendung sollen mit der Integration der IT-Messaging-Anwendung auch eine Desktop-Version bereitgestellt werden. Auch dient für die Kommunikation das WebRTC-Protokoll, wo doch heute browserbasierende Kommunikation für die ePA als unsicher angesehen wird. Neben den Herausforderungen, die die Bereitstellung einer solchen Anwendung mit sich bringt, werden sicherlich etablierte Anbieter, welche bereits heute vergleichbare Angebote in ihrem Portfolio haben, gegen eine mit Steuergeldern finanzierte Anwendung aufbegehren. Sicherlich sind vertrauenswürdige und sichere Anwendungen, gerade im Gesundheitssektor, wünschenswert, jedoch sollte die Schaffung einer marktpolitischen Alleinstellung aus marktwirtschaftlichen Gesichtspunkten gut gegeneinander abgewogen werden. Ausdrücklich sollte geprüft werden, ob die Leistungsfähigkeit zur Bereitstellung gegeben ist, damit Bereitstellungszeiten wie bei der ePA von fast zwei Jahrzenten vermieden werden und die Anwendung für telemedizinische Anwendung in 2023 tatsächlich zur Verfügung steht.

3.2.2 Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz

Die TI ist aber nicht das einzige Digitalisierungsvorhaben der gematik GmbH. Auch für die Bereitstellung des Deutschen Elektronischen Melde- und Informationssystems für den Infektionsschutz (DEMIS) zeichnet sie sich verantwortlich. Wie auch die TI, hat diese Lösung eine längere Vorgeschichte, auch wenn diese

47 Vgl. gematik GmbH (21.07.2021).

erst mit der Bereitstellung der Corona-Warn-App mehr in den Fokus der Öffentlichkeit rückte. Bereits 2013 wurde eine Machbarkeitsstudie durch das Gesundheitsministerium beauftragt und in 2016 das Projekt zur Bereitstellung gestartet.[48] Im Rahmen des Projektes wurde das Augenmerk augenscheinlich nur auf die Entwicklung und Bereitstellung der Konnektoren selbst wertgelegt und auch keine alternative Nutzung von bereits bestehenden Anwendungen geprüft. Die Enabelung der späteren Anwender, sei es durch Schaffung der infrastrukturellen Voraussetzungen als auch durch Wissenstransfer, scheint hierbei nicht erfolgt zu sein. So wurde laut dem Bericht der Deutschen Welle Ende 2020 in nur ca. 1/3 aller Gesundheitsämter die digitale Anwendung zur Kontaktnachverfolgung genutzt. DEMIS war zu diesem Zeitpunkt zwar bereits zu 97% ausgerollt, aber nur in einer abgespeckten Version und befand sich noch in der Testphase, so dass Meldungen immer wieder liegengeblieben sind.[49] Nun wurde durch das BMG das Ziel ausgegeben, alle Akteure bis Ende 2022 an DEMIS anzubinden und auch weitere Infektionskrankheiten/Erreger zu melden. Für Labore und Gesundheitsämter ist die Nutzung im Rahmen der Covid-19-Pandemie allerdings bereits seit dem 01. Januar 2021 verpflichtend.[50] Hierbei muss dies nicht zwingend einheitlich auf Basis der durch das BMG favorisierte SORMAS Anwendung erfolgen, wenn die DEMIS-Adapter und Importer entsprechend funktionieren und in den jeweiligen Anwendungen spezifikationsgerecht implementiert wurden.[51] Dies könnte durch den obligatorischen Zulassungstest geprüft und zertifiziert werden.

3.2.3 Künstliche Intelligenz als Faktor bei der Digitalisierung im Gesundheitswesen

Dass Künstliche Intelligenz auch im Gesundheitswesen ein Faktor werden kann und auch schon auf Grund der notwendigen Kompensation von Personalressourcen werden muss, scheint unbestritten. Insbesondere durch ihre Fähigkeit in der Analyse und Verknüpfung von Daten aus verschiedensten Quellen und der Ableitung von neuen Erkenntnissen hat die KI das Potential, die Gesundheitsversorgung grundlegend zu verändern. Dabei spielt das vielseitig angesprochene Vertrauen eine große Rolle. Es muss aber auch geprüft werden, ob technologisch Machbares auch aus ethischen Gründen umgesetzt werden sollte.

48 Vgl. Deutschlandfunk (2021).
49 Vgl. Welle (01.08.2021).
50 Vgl. Bundesministerium für Gesundheit (2021).
51 Vgl. Deutscher Ärzteverlag GmbH, Redaktion Deutsches Ärzteblatt (2021).

Nicht nur aus diesem Grund sollte daher bei allen zukünftigen Entwicklungen nach der Wladimir Iljitsch Uljanow, besser bekannt als Lenin, zugeschriebenen golden Regel

„Vertrauen ist gut, Kontrolle ist besser!“

verfahren werden.

Bei der in dem Bereich der KI getätigten Grundlagenforschung verfügt Deutschland über einige hervorragende Forschungseinrichtungen, wie das Universitätsklinikum Essen als „Smart Hospital“ eindrucksvoll zeigt.[52] Allerdings mangelt es an der Übertragung der Ergebnisse in die alltägliche Gesundheitsversorgung[53], was auch die im Kapitel 3.2 Status der Digitalisierung im Gesundheitswesen dargelegten Daten wiederspiegeln. Auch aus diesem Grund hat der Bundesverband Gesundheits-IT in seinem Positionspapier zur kommenden Legislaturperiode 13 klare Forderungen an die zukünftige Bundesregierung adressiert.[54] Allerdings muss die Forderung zur Sicherstellung eines hinreichenden Datenpools aus Datenschutzgesichtspunkten kritisch gesehen werden.[55] Die Bereitstellung der Daten sollte immer auf Basis der Freiwilligkeit und persönlichen Selbstbestimmung sowie auch unter möglichen finanziellen Entschädigung der Datenlieferanten erfolgen. Mit Einführung der ePA hätte der Patient die Möglichkeit, nicht nur mit Ärzten auf eigenverantwortlicher Basis Daten zu teilen, sondern seine Daten auch für Forschungs- oder kommerzieller Zwecke zur Verfügung zu stellen. Diese könnten dann dazu beitragen, bestehende Anwendungen weiter zu entwickeln und neue Lösungen zu schaffen. Derzeit werden KI-Lösungen bereits in den Bereichen

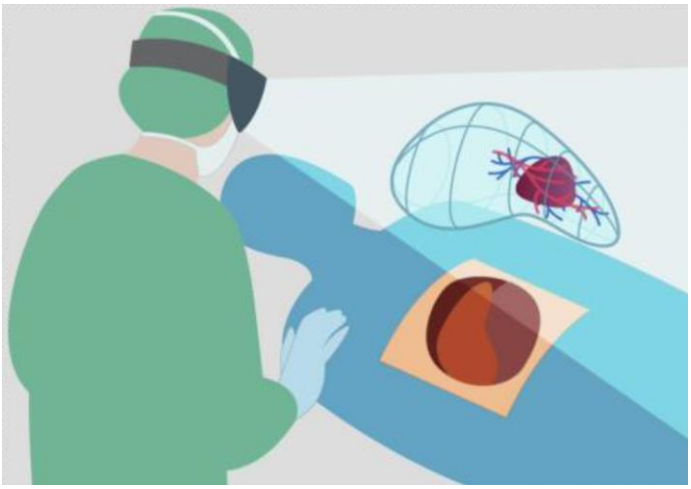
- Patientennahe diagnostische Anwendungen
- radiologischen Bildanalytik
- Entscheidungsunterstützung
- Virtual Reality
- Robotik

eingesetzt.

Virtual Reality hat sich insbesondere im Bereich der medizinischen Ausbildung etabliert. So können Studenten die Operationssäle und medizinische Geräte in virtuellen Umgebungen nutzen und lebensbedrohliche Operationen üben, ohne das Leben des Patienten unmittelbar zu gefährden.[56] Bei komplexen Operationen wird es über die Mixed Realität möglich sein, dem Arzt durch ein Echtzeit-

52 Vgl. huawei (27.042021).
53 Vgl. DMEA – Connecting Digital Health (15.09.2021).
54 Vgl. Bundesverband Gesundheits-IT (01. Juni 2021).
55 Vgl. Bundesverband Gesundheits-IT (21. Juni 2019).
56 Vgl. Healthcare Mittelhessen (2019).

3D-Modell eine bessere Übersicht zu der aktuellen Situation zu geben und über fortlaufende Datenanalyse der Operation Empfehlungen und Hinweise auf mögliche Komplikationen anzuzeigen. Diese Technologie kann auch dazu beitragen, Behandlungsfehler und damit mögliche Komplikationen für den Patienten zu vermeiden.



Quelle: Martin Peuker, 28.09.2021

Abbildung 11: Operation unter Einsatz Mixed Realität

Dieses Beispiel zeigt eindrucksvoll, welche Möglichkeiten in der KI im Bereich des Gesundheitswesens stecken. Eine der großen Herausforderung wird es aber auch sein, zum einen die Balance zwischen der Freiheit für wirtschaftlichen Innovation und zum Wohle der Patienten und zum anderen zwischen wissenschaftlicher Innovation und Ethik zu finden. Auch im Hinblick auf die zunehmende Bevölkerung erscheint eine weitere Verbesserung der Gesundheitsversorgung als nicht unproblematisch.

Damit eine sichere und für alle akzeptier- und nutzbare Bereitstellung von digitalen Diensten möglich ist, bedarf es daher einer soliden Basis auf der Grundlage entsprechender gesetzlichen Regelungen.

4 Gesetzliche Grundlagen

Das Gesundheitswesen ist einer der mit am meisten regulierten Bereiche. In diesem Kapitel soll daher auf die relevanten Regelungen und auf die Zusammenhänge/Abhängigkeiten in klinischen IT-Infrastrukturen eingegangen werden. Hierbei erfolgt eine Einteilung in die Bereiche

- Digitalisierung im Gesundheitswesen
- Medizin-Sicherheit
- IT-Sicherheit
- Datenschutz
- Künstliche Intelligenz
- Finanzierung

4.1 Digitalisierung im Gesundheitswesen

Für die Digitalisierung des Gesundheitswesens als überwiegend steuer- und beitragsfinanziertes System bedarf es der Schaffung entsprechender gesetzlicher Grundlagen, damit eine Umsetzung und Fokussierung auf diese Themen erfolgen und die Mittel hierfür bereitgestellt werden können, sowie auch ein Anspruch für die Bevölkerung auf die Nutzung von digitalen Anwendungen entsteht. Die Inhalte der verabschiedeten Gesetze zur Förderung der Digitalisierung werden in diesem Kapitel zusammengefasst dargelegt und deren Relevanz in Bezug auf die Sicherheit bewertet.

4.1.1 Terminservice- und Versorgungsgesetz

Bereits ca. ein halbes Jahr vor dem Digitale-Versorgungs-Gesetz (DVG) wurde das Terminservice- und Versorgungsgesetz (TSVG) mit dem Ziel der verabschiedet, dass Patienten schneller einen für sie passenden Arzttermin bekommen. Impulse für die Digitalisierung im Gesundheitswesen soll das Gesetz in der Form geben, dass die elektronische Patientenakte ab Januar 2021 durch die Versicherungen zur Verfügung gestellt werden soll. Neben der Einführung der

Patientenakte passiert auch die Einführung der elektronischen Arbeitsunfähigkeitsbescheinigung auf dem TSVG. Mit der zum 01. Januar 2021 wirksam werdenden Änderung des TSVG erfolgt die Anpassung der relevanten Paragraphen des SGB V. Gemäß §295 Absatz 3 Satz 2 SGB V muss die Arbeitsunfähigkeitsbescheinigung ab dem 01. Oktober 2021 in elektronischer Form an die Krankenkasse durch die Akteure der vertragsärztlichen Versorgung übermittelt werden. Hierzu ist gemäß §295 Absatz 1 Satz 10 SGB V verbindlich die TI zu nutzen. Dies erfordert damit eine zwingende Nutzung des KIM-Dienstes für die Kommunikation zwischen diesen Akteuren ab diesen Zeitpunkt, was hinsichtlich einer termingerechten Bereitstellung Fragen offenlässt.
Weiterhin wurde die Verantwortungen zur Gewährleistung der Informationssicherheit, welche bisher beim BSI gelegen haben, mit diesem Gesetz auf Grundlage des §291b Absatz 1a Satz 13 SGB V an die Gesellschaft für Telematik übertragen. Die Zulassung von Komponenten für die TI erfolgt gemäß dieser Gesetzesversion noch in Abstimmung mit dem BSI, um nur 20 Monate später mittels der Verabschiedung des Patientendaten-Schutz-Gesetz (PDSG) ganz auf die gematik GmbH, als Betreiber der TI, übertragen zu werden.

4.1.2 Digitale-Versorgungs-Gesetz

Das am 19. Dezember 2019 in Kraft getretene Digitale-Versorgungs-Gesetz wurde mit dem Ziel verabschiedet, die Digitalisierung des Gesundheitssystems durch die Bereitstellung von 200 Millionen Euro zu fördern. Die Förderung ist angesetzt für Innovationsentwicklungen, um digitale Dienste im Gesundheitsumfeld flächendeckend bereitzustellen und entsprechende digitale Leistungen abrechenbar zu machen. Das Gesetz ist hierbei im eigentlichen Sinne kein eigenständiges Gesetz, sondern umfasst, wie auch alle anderen Gesetzgebungen in Gesundheitsumfeld, im Wesentlichen die Änderungen des fünften Sozialgesetzbuches, mit welchen die angestrebten Ziele sichergestellt werden sollen. Über den Stand der Umsetzung und den erreichten Ergebnissen muss der Spitzenverband Bund der Krankenkassen erstmals bis zum 31. Dezember 2021 berichten.
Die herausgestellte jährliche Innovationsförderung von 200 Millionen Euro ist auf die Jahre 2020 bis 2024 begrenzt und stellt gegenüber der Förderung in den Jahren 2016 bis 2019 eine Reduzierung der Fördersumme um 100 Mio. Euro dar.
In Bezug auf den Anspruch der Versicherten auf „digitale Medizinprodukte“ auf Grundlage des Gesetzes lässt sich festhalten, dass dieser gemäß §33a Absatz 1 SGB V ausschließlich für Medizinprodukte der Klasse I oder IIa besteht und diese in der Datenbank für Digitale Gesundheitsanwendungen (DiGA) des Bundesministeriums für Arzneimittel und Medizinprodukte gelistet sind. Wie in den

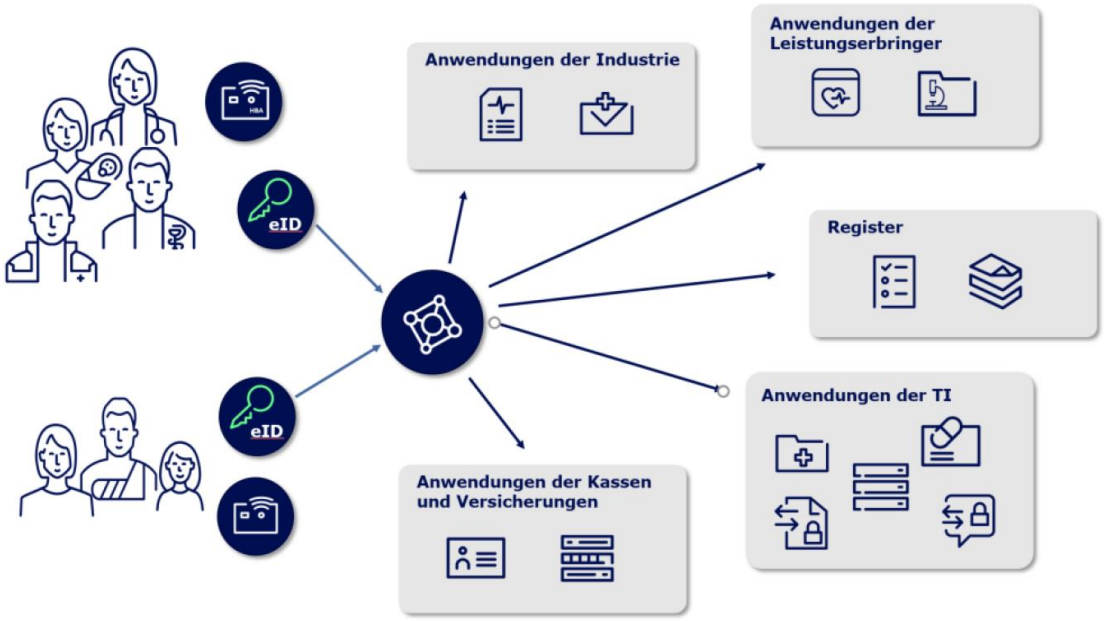
Ausführungen im Kapitel 4.2.1 Medical Device Regulation – Medizinprodukteverordnung noch dargelegt wird, ist eine Einstufung in Klasse I nahezu ausgeschlossen. Für Produkte der Klasse IIa erhöhen sich die Anforderungen in Bezug auf Risikobewertung, Qualitätssicherung und Dokumentationspflichten für die Hersteller gegenüber der Klasse I erheblich, so dass diese die Zulassung als Medizinprodukt offenbar abschreckt. Zur Aufnahme in das DiGA muss gemäß §139e Absatz 2 SGB V neben den Medizinproduktnachweis auch der Nachweis zur Sicherstellung des Datenschutzes erbracht werden. Es erscheint daher weniger verwunderlich, dass mit Stand 08. Oktober 2021 erst 22 Anwendungen in dieser Datenbank aufgenommen wurden, [57] wobei mit 2/3 der Anwendung der überwiegende Teil erst eine vorläufige Zulassung hat, was auf einen fehlenden positiven Versorgungsnachweis zurückgeführt werden könnte.
Im Rahmen der Anpassung des SGB V auf Grundlage des Digitale-Versorgung-Gesetz wurde der §75b neu aufgenommen, welcher die verbindliche Einführung und Umsetzung einer IT-Sicherheits-Richtlinie für die sichere Inbetriebnahme und den Betrieb der Komponenten der Telematikinfrastruktur für alle vertragsärztlichen und vertragszahnärztlichen Leistungserbringer vorsieht. Weiterhin sind in Abstimmung mit der gematik GmbH auch die Sicherheitsanforderungen für eine sichere Vernetzung und Kommunikation zwischen den Leistungserbringern zu deklarieren. Ausgenommen hiervon sind die Betreiber von Kritischen Infrastrukturen gemäß §8a des BSI-Gesetzes.

4.1.3 Digitale-Versorgungs- und Pflege-Modernisierungs-Gesetz

Das Digitale-Versorgungs- und Pflege-Modernisierungs-Gesetz ist am 09. Juni 2021 in Kraft getreten. Zentrale Bestandteile des DVPMG sind weitere grundlegende Änderungen des SGB V, Änderungen des SGB XI - Sozialen Pflegeversicherung und die Anpassung/Ergänzung weiterer Gesetze. Mit Erweiterung der gesetzlichen Grundlage zur Digitalisierung auf den Pflegebereich wird eine große gesetzliche Lücke im Bereich des digitalen Gesundheitssektors geschlossen.
Neben der Erweiterung der ePA ist die grundlegendste Neuerung der notwendige Schritt zur Bereitstellung einer digitalen Identität für alle Versicherten. Als spätestens Erfüllungstermin ist hierfür der 01. Januar 2023 beschlossen worden. Damit wird die heute bestehende Praxis der Speicherung der Patientendaten auf der elektronischen Gesundheitskarte durch die Hinterlegung in der ePA abgelöst und

57 Vgl. Bundesministerium für Arzneimittel und Medizinprodukte (03.07.2021).

die eGK dient dem Identitätsnachweis. Zu diesem zukünftigen Vorgehen bestehen geteilte Meinungen. Wo die Krankenkassen mehrheitlich diesen Schritt begrüßen und teilweise wie z.B. die BARMER diesen Schritt als unumgänglich erachten[58], stößt er bei der Ärzteschaft eher auf Ablehnung.[59]



Quelle: Volker Mielke, 28. September 2021

Abbildung 12: Zugang zu den digitalen Diensten mittels eID

Grundlegend für diesen Schritt ist die Bereitstellung der hierfür erforderlichen Infrastruktur zur Datenhaltung. Dieser sollte durch die gematik GmbH über die TI bereitgestellt werden und nicht außerhalb bei externen Dritten liegen, wobei dies nach aktueller Gesetzgebung aus Datenschutzgründen nicht zulässig wäre. Inwieweit die gematik GmbH ihrer Rolle gerecht werden kann, muss die Zukunft zeigen. Derzeit wird auch hier die Entwicklung nicht durchgängig positive bewertet. Hierzu hat auch die gematik GmbH durch ihr bisheriges Handeln, verbunden mit vielmals der Nichteinhaltung von angekündigten Terminen, selbst beigetragen. Kritisch wird vor allem die gleichzeitige Einnahm von verschiedenen Rollen durch die gematik GmbH gesehen. Sie tritt in Abhängigkeit der Situation sowohl als Entwickler, Anbieter und Genehmigungsbehörde auf, was erhebliches Konfliktpotential bis hin zur Gefahr der Wettbewerbsverzerrung durch Marktbeeinflussung und Wissensvorsprung birgt.[60] Aber auch die beschlossene finanzielle Ausstattung der gematik GmbH wird hinterfragt, was bei Erhöhung der jährlichen Umlage auf die gesetzlichen Krankenkassen von kollaborierten ca. 26,5 Mio. Euro verständlich erscheint. Damit erhöht sich die Umlage pro Versicherten auf 1,50 Euro pro Jahr.

58 Vgl. Barmer (03.07.2021).
59 Vgl. AerzteZeitung.de (2021).
60 Vgl. Avoxa – Mediengruppe Deutscher Apotheker GmbH (03.07.2021).

Der Sicherheit betreffend, beinhalt das DVPMG die grundlegende Festlegung der Zuständigkeit des BSI in Zusammenarbeit mit dem Bundesbeauftragten für Datenschutz und dem Bundesinstitut für Arzneimittel und Medizinprodukte für die Informationssicherheit und den Datenschutz der Gesundheitsanwendung gemäß §139e Absatz 10 und 11 des SGB V. Für die Sicherheit der Infrastruktur selbst ist die gematik GmbH in Abstimmung der KBV gemäß §75b und §311 Absatz 1 Satz 1 SGB V zuständig. Die Gründe für die Trennung der Verantwortlichkeiten für die Sicherheit der Anwendungen auf der einen Seite und des Betriebs der Telematikinfrastruktur auf der anderen Seite sind nicht bekannt und damit nicht nachvollziehbar.
Die DiGAV wurde knapp ein Jahr zuvor ebenfalls in einem wesentlichen Punkt angepasst. In diesem wird von den Herstellern von Gesundheitsanwendungen, verpflichtend ab dem 01. Januar 2022, der Nachweise eines geeigneten Informationssicherheitsmanagements verlangt. **Um Jahresfrist** später muss die Datensicherheit durch ein Zertifikat des BSI nachgewiesen werden.
Die Sicherstellung des Datenschutzes für die TI obliegt dem Betreiber dieser Infrastruktur. Einer zusätzlichen Regelung im Rahmen der DVPMG hätte es daher nicht zwingend bedurft. Zur Infrastruktur der TI gehören auch die dezentralen Konnektoren in den Praxen und medizinischen Einrichtungen. Diese Konnektoren sind daher im Datenschutzkonzept des Betreibers mit zu berücksichtigen, zu welchem auch eine Datenschutzfolgeabschätzung gemäß Artikel 35 der DSGVO gehört. Hieraus im Rahmen der Gesetzesverabschiedung durch den Deutschen Bundestag eine Einsparung für die Leistungserbringer in Höhe von 730 Mio. Euro einmalig und 980 Mio. Euro jährlich abzuleiten und gar mit dem Gesetz die Leistungserbringer von der Pflicht der Bestellung eines Datenschutzbeauftragten zu endbinden, ist nicht dem Ziel der Verbesserung der IT-Sicherheit und der Einhaltung des Datenschutzes zuträglich.[61] Wie es auch dann richtiger Weise im Anhang zu Artikel 1 Nummer 84 des DVPMG selbst dargelegt wird.

4.1.4 Digitale-Gesundheitsanwendungen-Verordnung

Mit der Digitale-Gesundheitsanwendungen-Verordnung soll die Grundlage zur Bereitstellung von qualitativ hochwertigen, sicheren, praxistauglichen und akzeptierten Anwendungen geschaffen werden. Das Gesetz wirkt hierbei mehr wie ein Leitfaden und Gebührenordnung für die Anbieter zur Aufnahme ihrer Produkte in das DiGA-Register und der damit verbundenen Erstattungsfähigkeit der Kosten für diese Anwendungen durch die Krankenkassen.

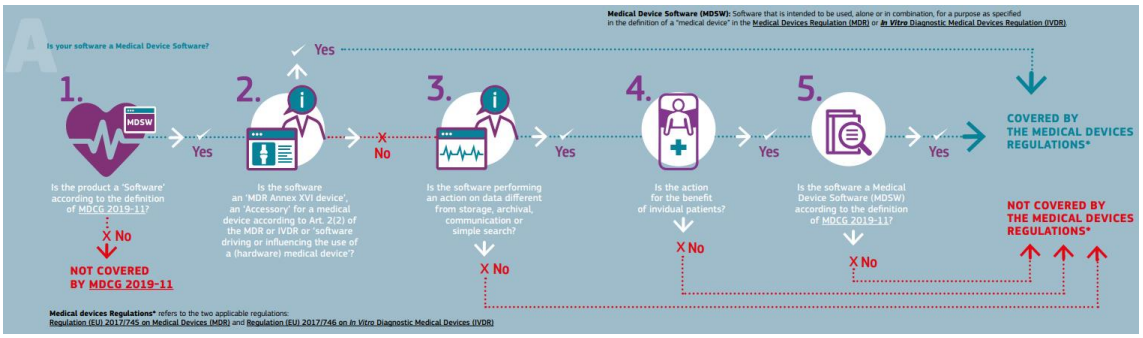
61 Vgl. Bundesanzeiger Verlag GmbH (17.03.2021).

Damit eine Zulassung erfolgen kann, werden hohe Anforderungen an die Produkte gestellt, so dass die meisten Anbieter derzeit Abstand davon zu nehmen scheinen. Die Sicherheit der Nutzer muss natürlich immer im Vordergrund stehen und sollte daher auch keine Grundlage für Kostendiskussionen sein. Jedoch erscheint eine Zulassung als Medizinprodukt in Verbindung mit der Sicherstellung der Informationssicherheit hinreichend für die Zulassung zu sein. Eine zusätzliche Erbringung von Nachweisen für die Einhaltung des Datenschutzes, der Qualitätsanforderungen und eines positiven Versorgungsnachweise ist nicht erforderlich, da diese Nachweise bereits Bestandteil einer Zulassung als Medizinprodukt sind.

4.2 Sicherheit von Medizinprodukten

4.2.1 Medical Device Regulation – Medizinprodukteverordnung

Medizinprodukte nehmen in klinischen Infrastrukturen eine besondere Stellung ein. Um den Aufbau dieser Infrastrukturen und den hierdurch bedingten Hemmnissen hinsichtlich einer durchgehenden Gestaltung von digitalen Prozessen zu verstehen, müssen die Anforderungen an Medizinprodukte betrachtet werden. Die Regelung zu dieser Produktgruppe ist in der neue europäische Medical Device Regulation (MDR), welche zusammen mit der In-Vitro-Diagnostik die bisher geltende Medizinprodukte-Richtlinie abgelöst hat, festgeschrieben.
Bevor eine Bewertung der Einstufung des Produkts erfolgt, ist im ersten Schritt zu klären, ob es sich um ein Medizinprodukt handelt. Diese ist der Fall, wenn die Zweckbestimmung des Produktes für die medizinische Anwendung am Menschen bestimmt ist. Diese Frage sollte durch die Anbieter sehr sorgfältig geprüft werden, da hiervon abhängig ist, welche Pflichten der Anbieter beim Inverkehrbringen des Produktes erfüllen muss. Hierzu kann in Bezug auf Software die Leitlinie MDCG 2019-11 zur Qualifizierung und Klassifizierung von Software der Medical Device Coordination Group genutzt werden. Der Prozess hierzu ist in der nachfolgenden Abbildung dargestellt.



Quelle: Medical Device Coordination Group, October 2019

Abbildung 13: Prozess zur Prüfung der Software auf hinsichtlich der Relevanz der Einstufung als Medizinprodukt

Folgt man dieser Leitlinie, so handelt es sich bei fast allen auf dem Markt befindlichen Apps um Medizinprodukte, sofern diese als Zweck die Diagnose, Prävention, Überwachung oder Prognose einer Krankheit, z.B. Bluthochdruck, haben. Zur weiteren Spezifikation definiert das MDR für Medizinprodukte dann gemäß Artikel 51 4 Produktkategorien unter Berücksichtigung ihrer Zweckbestimmung und den damit verbundenen Risiken, wobei die Klasse I zusätzlich in 1. einmalig nutzbare und 2. wiederverwendbare Produkte unterteilt wird. In folgende Klassen wird hierbei unterschieden:

- Klasse I bzw. Klasse Ir (geringes Risiko bei der Anwendung)
- Klasse IIa (mittleres Risiko bei der Anwendung)
- Klasse IIb (erhöhtes Risiko bei der Anwendung)
- Klasse III/Aktive Implantate (hohes Risiko bei der Anwendung)

Die Einstufung in die entsprechenden Klassen erfolgt gemäß Anhang VIII „Klassifizierungsregeln“ des MDR. In Bezug auf die Thematik der Digitalisierung sind insbesondere die Punkte zur Klassifizierung von Software von Interesse. Folgende prinzipielle Aussagen lassen sich hierzu treffen:

1) Software bzw. Apps, welche zur Steuerung von Produkten genutzt werden oder dessen Anwendung beeinflussen, erhalten die gleiche Einstufung wie das Produkt selbst.
2) Software, wie sie in vielen Wearables eingesetzt wird, ist in die Klasse IIa einzustufen, wenn die Daten zur Entscheidung für diagnostische oder therapeutische Zwecke herangezogen werden.
3) Sind die Auswirkungen der Entscheidung, welche aus den bereitgestellten Informationen abgeleitet werden, dazu geeignet, zum Tod oder zu einer nicht wieder umkehrbaren Verschlechterung des Gesundheitszustandes führen, erfolgt eine Einstufung in Klasse III. Die Einstufung in Klasse IIb wäre nur gerechtfertigt, wenn dies auszuschließen wäre. Ein Anwendungsbeispiel für diese Kategorie sind Anwendungen zur Medikamentengabe.

Auf Grund dieser Prinzipien kann festgestellt werden, dass kaum eine Einstufung von Software in die Klasse I erfolgt, wie auch das Johner Institut in seiner Analyse feststellt.[62] Entscheidend für die medizinische Risikoklassifizierung ist daher die Zweckbestimmung und damit die Einstufung in medizinische und nicht medizinische Anwendungen.
Im Rahmen des Zulassungsverfahrens als Medizinprodukt muss die Lösung ein Konformitätsbewertungsverfahren durchlaufen. Essenzieller Bestandteil des Verfahrens sind die Durchführung entsprechender Risikoanalysen, Aufbau eines entsprechenden Qualitätsmanagements, Entwicklung auf Basis „Stand der Technik“ und Bereitstellung einer entsprechenden Dokumentation. Die zu erfüllenden Anforderungen an ein Medizinprodukt innerhalb des Produktentwicklungszyklus in Abhängigkeit ihrer Einstufung in eine der Medizinprodukteklassen können der Übersicht im Anhang F entnommen werden. Die Anforderungen an die Software beschreibt hierbei die Aussage in der durch die europäische Kommission herausgegebene Leitlinie zur Cybersicherheit für Medizinprodukte aus meiner Sicht treffend.

*„Geräte müssen die vom Hersteller vorgesehene Leistung erbringen und so konstruiert und hergestellt sein, dass sie unter normalen Einsatzbedingungen für ihren vorgesehenen Zweck geeignet sind. Sie sollen **sicher und effektiv sein** und dürfen weder den klinischen Zustand, noch die **Sicherheit der Patienten,** noch die Sicherheit und Gesundheit der Anwender oder gegebenenfalls anderer Personen **gefährden**, sofern alle Risiken, die mit ihrer Anwendung verbunden sein können, im Verhältnis zum Nutzen für den Patienten vertretbar sind und sind unter Berücksichtigung des allgemein anerkannten **Stands der Technik** mit einem hohen Schutzniveau für Gesundheit und Sicherheit vereinbar.“*[63]

4.2.2 Medizinprodukte-Betreiberverordnung

Die Beachtung der Sicherheits- und Qualitätsanforderung alleinig garantiert nicht die Freiheit von vertretbaren Risiken. Hierfür muss auch für einen entsprechend sicheren Betrieb der Lösung Sorge getragen werden. Die Pflichten für Betreiber sind daher in einer entsprechenden Betreiberverordnung für Medizinprodukte festgeschrieben. Diese Pflichten gehen auch über den Betrieb in den reinen klinischen Infrastrukturen hinaus, so muss er diesen auch dann nachkommen,

62 Vgl. Wissen zu medizinischer Software (2019).
63 Vgl. Directorate-General for Health and Food Safety (Dezember 2019).

wenn diese Lösung z.B. in der häuslichen Pflege eingesetzt wird. Sofern die Geräte privat erworben und nicht durch eine Institution bereitgestellt werden, findet die Betreiberverordnung keine Anwendung und obliegt jedem Einzelnen selbst. Dies gilt auch in Bezug des Erwerbs der entsprechenden Fähigkeiten zur sachgemäßen Nutzung der Anwendung.
Nicht hinreichend berücksichtigt ist in der Betreiberverordnung möglichweise eine fortlaufende Risikobewertung der Anwendung durch sich verändernde Umgebungsbedingung, wie sich diese z.B. im Rahmen der Digitalisierung durch Vernetzung von Systemen ergeben können. Sicherheitstechnische Kontrollen beschränken sich auf die Sicherheit des Produktes selbst und deren Verfügbarkeit. So sieht es auch Armin Gärtner in seinem Beitrag auf e-Health-com.de.[64] Daher findet in Bezug auf den Betrieb und die Risikobetrachtung die DIN EN 80001-1 ihre Anwendung.

4.2.3 Betrieb medizinischer Netze gemäß DIN EN 80001-1

Ziel der Norm 80001-1 ist der sichere Betrieb von medizinischen Netzwerken. Eine Infrastruktur bezeichnet man als medizinisches Netzwerk, wenn mindestens ein Medizinprodukt angebunden ist. Im Wesentlichen beschreibt die Norm ein Risikomanagement in medizinischen Netzwerken. Hierzu könnte aber auch jedes andere Risikomanagementsystem genutzt werden. Allerdings verweist auch der branchenspezifische Standard, der B3S Krankenhaus, zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) auf die Norm, so dass diese in vielen Krankenhäusern wieder verstärkt in den Fokus rücken sollten, da zum 1. Januar 2022 alle Krankenhäuser unabhängig von deren Größe gemäß §75c SGB V verpflichtet sind, ein entsprechendes ISMS zu implementieren.
Da die Medizinprodukte einem eigenen Risiko-Managementprozess unterliegen, liegt der Fokus der Norm auf der Risikobewertung der Infrastruktur- und dem Kommunikationsnetzwerk. Hierbei werden alle beteiligten Komponenten und Abläufe, die einen Einfluss auf die sichere Kommunikation bzw. die Ausfallsicherheit haben können, in die Risikobetrachtung einbezogen. Im Rahmen des Risikomanagements werden daher die Kommunikationsbeziehung zwischen den einzelnen Komponenten des medizinischen Netzwerks hinsichtlich der auf sie wirkenden Gefährdungen bewertet. Dies erfolgt dabei in Bezug der durch die Norm definierten drei Schutzziele:

- Safety (Sicherheit von Patienten, Anwendern und Dritten)
- Effectiveness / Wirksamkeit (der Behandlung) und

64 Vgl. Armin Gärtner .

- Security (Daten- und Systemsicherheit)

4.3 IT-Sicherheit

Digitalisierung ohne Berücksichtigung der IT-Sicherheit ist nicht ohne eine Gefährdung der gesamten Gesundheitsinfrastruktur umsetzbar und ist wie Kapitel 4.1 Digitalisierung im Gesundheitswesen bereits dargelegt, ein integraler Bestandteil der Gesetzgebung. Innerhalb der angesprochenen Gesetzgebung wird immer wieder auf die Zuständigkeit des BSI oder Institutionen, wie die gematik GmbH oder das BMG, verwiesen. Letztere könnten in Abstimmung mit dem BSI entsprechende Sicherheitsanforderungen definieren. Im Folgenden sollen die bestehenden Regelungen und die hieraus erwachsenden Vorgaben für die einzelnen Akteure in den klinischen Infrastrukturen und dem Digitalisierungsvorhaben erörtert werden.

4.3.1 Das IT-Sicherheitsgesetz

Das BSI-Gesetz legitimiert das BSI als zentrale Stelle für Informationssicherheit in Deutschland und wurde in seiner überarbeiteten Fassung am 03. Juni 2021 durch den Bundesrat verabschiedet. Viele Verbände und Interessenvertreter haben vor, bei und nach der Verabschiedung des erneuerten Gesetzes, auch als BSI-Gesetz 2.0 bezeichnet, nicht mit Kritik gespart. So schrieb Stefan Krempl auf heise online in seinem Beitrag *„IT-Sicherheitsgesetz 2.0: Mittelfinger ins Gesicht der Zivilgesellschaft“* von einem Ausbau des BSI zur Cyber-Behörde mit Befugnis zum Hacken und prangerte die fehlende Einbindung anderer Verbände oder Ressorts an.[65] Auch die fehlende Evaluierung der Ergebnisse zu den mit der ersten Fassung des Gesetzes gesteckten Zielen und Erwartungen wird immer wieder moniert. Doch dies soll nicht Gestand der hiesigen Betrachtung sein. Zur Steigerung der Akzeptanz bei zukünftigen Anpassungen sollte dies aber zwingender Bestandteil des Prozesses sein. Ohne die bestmögliche Transparenz zu den Tätigkeiten des BSI wächst das Misstrauen in diese Behörde weiter und schadet damit der Sicherheit der öffentlichen Infrastrukturen.
Neben den für klinische Infrastrukturen relevanten Artikel 1, umfasst das ITSiG noch weitere Artikel, auf welche jedoch auf Grund der fehlenden Relevanz für die weitere Betrachtung nicht weiter eingegangen werden soll.

65 Vgl. Krempl (10.12.202).

4.3.1.1 BSI-Gesetz in Bezug auf klinische Infrastrukturen

Die Anforderungen, die sich aus dem BSIG ergeben, sind für Betreiber von Klinische Infrastrukturen relevant, insofern diese gemäß der im §6 und Anhang 5 der BSI-KritisV als kritische Infrastrukturen einzustufen sind. Demnach müsste auch die Telematikinfrastruktur als kritische Dienstleistung eingestuft werden, da diese eine Kommunikationssystem zur Auftrags- und Befundübermittlung darstellt, mit welchem mehr als 1,5 Mio. Aufträge pro Jahr übermittelt werden und das Funktionieren der klinischen Infrastruktur in dem Sinne davon abhängig ist, dass deren Ausfall bzw. Schädigung zu entscheidenden Behinderungen in der Versorgung führen würde oder gar eine Gefährdung der öffentlichen Sicherheit darstellen könnte. Allerdings sind nicht alle Anforderungen aus dem BSIG für die TI zutreffend. So müssen keine technischen und organisatorischen Maßnahmen zur Sicherstellung der Schutzziele im Sinne des BSIG getroffen werden und es besteht auch keine Meldepflicht für Sicherheitsvorfälle an das BSI als zentrale Meldestelle für entsprechende Vorkommnisse. Dies begründet sich aus §8d Absatz 2 Satz 3 und Absatz 3 Satz 3 BSIG. Wie bereits im Kapitel 4.1.3 dargelegt, ist eine Trennung der Verantwortlichkeiten im Sinne einer durchgehenden Sicherheitsstrategie für klinische Infrastrukturen nicht zuträglich und bedarf zusätzlichen Aufwand in der Definition und Umsetzung. Ausdrücklich stellt diese Trennung bei der Zulassung von Komponenten und Diensten für die TI sowie die Definition der Schnittstellen für die informationstechnischen Systeme einen Zwiespalt dar, da hierfür gemäß §311 Absatz 1 Satz 4 und 5 bzw. §§ 371-373 SGB V die gematik GmbH zuständig ist, das BSI auf Grundlage §3 Absatz 3, 5 und 5a BSIG, sowie §139e Absatz 10 SGB V aber die Zertifizierung von entsprechenden Systemen und Anwendungen, insbesondere auch für digitale Gesundheitsanwendungen, verantwortet. Betroffen von dieser überschneidenden Zuständigkeit sind Teilnehmer der TI, die als kritische Infrastruktur eingestuft sind und Anbieter von digitalen Anwendungen, welche den Anforderungen des BSI und Betriebsumgebung gerecht werden müssen. Auswirkungen könnten Wiedersprüche in der Beschreibung der Schnittstellenanforderungen in Bezug auf Sicherheitsmerkmale, unterschiedliche Sicherheitsvorgaben und erhöhte Aufwendung für diese Unternehmen sein.

4.3.1.2 Änderungen gegenüber der BSIG V1.0

Wie bereits einleitend erwähnt, wurden in der aktuellen Version teilweise grundlegende Änderungen gegenüber der vorhergehenden Version eingebracht. Auf Modifikationen mit Relevanz für klinische Infrastrukturen soll nachfolgend eingegangen und diese bewertet werden.

1. Definition von Kritischen Komponenten

Im §2 Absatz 13 erfolgt die Definition von kritischen Komponenten im Bereich von als kritische Infrastrukturen eingestuften Unternehmen im Sinne von §10 Absatz 1 Satz 1 BSIG, die bei Störung die Sicherheitsziele beeinträchtigen. Eine Einstufung von entsprechenden Komponenten ist nach aktuellem Stand noch nicht erfolgt. Die Deutsche Krankenhaus Gesellschaft geht in ihrer Stellungnahme zum BSIG 2.0 davon aus, dass z.B. für das Krankenhaus-Informationssystem als zentrale Komponente im Krankenhaus eine entsprechende Einstufung erfolgen könnte.[66] Diese hätte allerdings kaum Einfluss auf den heutigen Betrieb der Krankenhäuser, da gemäß §9b Absatz 1 nur beim erstmaligen Einsatz eines als kritische Komponente eingestuftes System an das BSI zu melden ist. Auswirkungen würden sich nur dann ergeben, wenn der Hersteller gemäß §9b Absatz 5 als nicht mehr vertrauenswürdig eingestuft werden würde und auf Basis dieser Einschätzung der Betrieb der Komponente durch das BMI untersagt werden würde. Das davon ausgehende Risiko sollte in die Risikobetrachtung aufgenommen werden.

2. Unternehmen von besonderem öffentlichem Interesse
   Über diesen neuen Passus, §2 Absatz 14, besteht die theoretische Möglichkeit, weitere Einrichtungen in klinischen Infrastrukturen als eine kritische Infrastruktur einzustufen. Auf Grund der Ausrichtung nach wirtschaftlichen Gesichtspunkten kann der Einschätzung der Deutsche Krankenhausgesellschaft e.V. (DKG), dass keine weiteren Krankenhäuser und Labore auf Basis dieser Änderung eine entsprechende eine Einstufung erfahren, nur in Bezug auf Einzeleinrichtungen gefolgt werden. Klinikverbünde dahingegen stellen auf Grund ihrer jeweiligen Gesamtbedeutung für die Gesundheitsversorgung durchaus Infrastrukturen dar, deren Ausfall als kritisch einzustufen ist und damit im Sinne des Gesetzes eine kritische Infrastruktur darstellen.
   In Bezug auf die Herstellung und Logistik werden möglicherweise vor dem Hintergrund der Covid-19-Pandemie weitere Unternehmen als kritische Infrastruktur auf Basis dieser Passus eingestuft, wenn gleich dies auf Grund der Pandemie und der damit verbunden Überschreitung der definierten Schwellwerte nicht ohnehin für weitere Firmen zu erwarten ist.
3. Sicherheitsdefinition nach Stand der Technik für IT-Produkte
   Der Begriff „Stand der Technik“ lässt einen gewissen Interpretationsspielraum. Er beschreibt ein System, was den Anforderungen gemäß der

66 Vgl. Deutsche Krankenhausgesellschaft e. V. (14. Januar 2021).

durchgeführten Risikospezifikation erfüllt. Neben technischen Gesichtspunkten spielen hier auch finanzielle Gegebenheiten eine Rolle, wobei im medizinischen Umfeld in der Regel vom maximalen Risiko ausgegangen werden müsste, wodurch sich die Risikobetrachtung in der Softwareentwicklung sehr schwierig gestaltet. Daher sollte diese Regelung, sofern das BSI hier ihre Aufgabe gerecht werden kann, mehr Klarheit bei der Gestaltung der der geforderten technischen und organisatorischen Vorkehrungen schaffen. Die heutige Formulierung im §8a Absatz 1 BSIG lässt in Bezug der Auslegung und Risikobewertung einen sehr großen Spielraum mit einer stärkeren Gewichtung der wirtschaftlichen Interessen zu, welche in Bezug auf das Gesundheitswesen allerdings nicht der wesentliche Maßstab sein sollte, auf Grund der finanziellen Ausstattung und Gewichtung der Mittelverteilung innerhalb der Einrichtungen aber darstellt.

Quelle: IT-Sicherheit-und-Recht.de, 2017

Abbildung 14: Stand der Technik – Ein Zustand zwischen dem Möglichen und dem Notwendigen

4. Aufhebung des Datenschutzes gemäß §3a
   Die Aufhebung des Datenschutzes im klinischen Umfeld ist ein schwerwiegender Eingriff in die Persönlichkeitsrechte, insbesondere da hier von der Verarbeitung von Daten mit besonderer Kategorie angenommen werden darf. Insofern muss hier davon ausgegangen werden, dass das BSI sehr sorgsam mit diesem Recht umgeht und entsprechend der Notwendigkeit dahingehend abwiegt, bevor diese Maßnahme getroffen wird.
5. Auskunftspflicht der Hersteller zu informationstechnischen Produkten
   Über §7a BSIG wird dem BSI das Recht eingeräumt, Auskunft zu technischen Details der Produkte und Systeme einzuholen. Hierdurch besteht die Einflussnahme auf die Produktentwicklung, die Chancen und Risiken birgt. Es besteht die Möglichkeit, die Sicherheit der Produkte nachhaltig bereits bei der Entwicklung zu verbessern und Schwachstellen bereits frühzeitig zu eliminieren. Anderseits könnte diese Einflussnahme zu Ver-

zögerung in der Bereitstellung von Lösungen führen und auch eine Einflussnahme auf den Markt ist denkbar. So werden bereits heute in Bundesbehörden informationstechnische Sicherheitsprodukte vorgeschrieben, welche eine BSI-Zertifizierung besitzen, unabhängig davon, ob andere Lösungen am Markt die gleiche Zertifizierungsstufe gemäß Common Criteria durch einen der zugelassenen Member besitzt. Sollte diese Praxis, welche mit Bezug auf die Bundesbehörden auf Grundlage §8 BSIG gestützt wird, auch für klinischen Infrastrukturen angewandt werden, stehen bestimmte Produkte nicht mehr zur Verfügung. Zwangsläufig führt dies zu einer Marktbeschränkung und Kostensteigerung, was gerade im Umfeld von klinischen Infrastrukturen mit stark begrenztem IT-Budget eher zur Schwächung als zur Stärkung der IT-Sicherheit beitragen würde.

6. Verbindlicher Einsatz von Angriffserkennungssystemen
   Zur Erhöhung der IT-Sicherheit in kritischen Infrastrukturen müssen mit Stichtag dem 1. Mai 2023 Intrusion Detection Systeme (IDS) in diesen Netzen eingesetzt werden. Wie auch die DKG in ihrer Stellungnahme zum Entwurf des heute gültigen BSIG schreibt, bedeutet die Einführung eines IDS nicht nur die Implementierung einer entsprechenden technischen Lösung, sondern es sind auch umfassende organisatorische Änderungen notwendig, sofern nicht bereits vergleichbare Systeme betrieben wurden.[67] Auch folgen möchte ich der Ansicht, dass die Einführung der Systeme innerhalb von 20 Monaten nach Verabschiedung der Gesetzesänderung viele Organisationen überfordert sein dürften. In Hinsicht der Auffassung zur Verbesserung der IT-Sicherheit muss ergänzt werden, dass eine direkte Verbesserung sicherlich schwer messbar ist, im Fall eines Angriffes jedoch eine schnellere und zielgerichtete Reaktion zur Reduzierung der Auswirkung eines Angriffes und eine Erhöhung der Verfügbarkeit der kritischen Infrastruktur führt, was indirekt einen Sicherheitsgewinn darstellt. Ob ein IDS-System in den kritischen Infrastrukturen zur Verbesserung der Sicherheit in der klinischen Infrastruktur beiträgt oder eine Sicherheitsmaßnahme zum Schutz dieser Infrastrukturen, welche auf Grund der steigenden Vernetzung im Rahmen der Digitalisierung notwendig ist, ist eine separate Fragestellung. Da die Wahrscheinlichkeit eines Angriffs jedoch mit der Größe des Gesamtsystems wächst, stellen Lösungen zur schnellstmöglichen Eindämmung eines Angriffs und der Isolation der betroffenen Infrastruktur vom Gesamtsystem einen nachvollziehbaren und zu empfehlenden Ansatz dar. Daher sollte zusätzlich zur Implementierung

67 Vgl. Deutsche Krankenhausgesellschaft e. V. (14. Januar 2021).

in den einzelnen Häusern über ein entsprechendes Umbrella-System nachgedacht werden, damit der Informationsfluss über Angriffe und Angriffsmuster entsprechend schnell innerhalb der gesamten Infrastruktur erfolgen und Maßnahmen zum Schutz aller anderen Teilnehmer getroffen werden können kann.

7. Verpflichtung zur Herausgabe von Informationen zur Bewältigung einer erheblichen Störung

   Im Rahmen der Unterstützung zur Bewältigung einer Störung von erheblichem Ausmaß kann das BSI die Herausgabe von personenbezogenen Informationen verlangen, insofern dies zur Störungsbehebung beiträgt. Die Wahrscheinlichkeit der Verletzung des Datenschutzes durch die Betreiber der kritischen Infrastruktur wird als gering angesehen, da für Anforderung der Daten ein begründeter Verdachtsfall vorliegen muss und damit eine Rechtfertigung im Rahmen einer möglichen Strafverfolgung darstellt. Eine Absicherung durch eine entsprechende Strafverfolgungsbehörde ist dennoch geboten. Diese wäre dann erforderlich, wenn durch die Datenerfassung des Betreibers Persönlichkeitsrechte der verdächtigen Person, aber auch von anderen Patienten verletzt werden. Die unbefugte Erfassung von Daten ist gemäß §202b StGB strafbar. Werden Computerprogramme, Passwörter oder andere Informationen, die als Vorbereitung einer Straftat zugeordnet werden könnten, ohne Autorisierung erfasst, ergibt sich aus §202c StGB eine besondere Bedeutung für die §202a, §202b StGB.

8. Telematikinfrastruktur – bleibt keine kritische Infrastruktur

   Die Änderung zur Nichtanwendbarkeit der §8a und § 8b Absatz 4 und 4a BSIG beinhaltet keine wesentliche Änderung gegenüber der vorhergehenden Version des BSIG, sondern bezieht sich ausschließlich auf die Anpassung der sich geänderten Paragraphen im SGB V. Auf Grund des möglichen Konfliktpotentials im Bezug der klinischen Infrastrukturen soll diese Änderung, welche den Standpunkt zur gewollten Trennung mit Hinblick der durchgeführten Anpassung untermauert, nicht unerwähnt bleiben.

9. Zertifizierung

   Einen unmittelbaren Einfluss der Ergänzung des §9 des BSIG auf klinische Infrastrukturen lässt sich nicht ableiten. Allerdings könnte über das eingeräumte Vetorecht des BMI bzgl. der Vergabe von Zertifikaten oder die Notwendigkeit der Erbringung eines Vertrauenswürdigkeitsnachweises für die Lösung sowie deren Anbieter/Hersteller auf die Bereitstellung von Digitalisierungslösungen hemmende Wirkung in Bezug auf Zeit und Quantität haben.

Inwieweit die freiwillige IT-Sicherheitskennzeichnung von Produkten zur tatsächlichen Erhöhung der Sicherheit beitragen kann, muss abgewartet werden, wobei der Digitalexperte der FDP, Manuel Höfering, und Anke Domscheit, Netzpolitikerin der Linken, hieran berechtigt Zweifel hegen. [68] Der Chaos Computer Club geht sogar noch einen Schritt weiter und bezeichnet dies in Anbetracht der eingeplanten 25 zusätzlichen Stellen beim BSI als Ressourcenverschwendung.[69] Die im Rahmen der Überarbeitung des BSIG gehegten Bedenken bzgl. des §9c können auch nicht durch den Referentenentwurf der Rechtsverordnung zur IT-Sicherheitskennzeichen entkräftet werden. Vielmehr könnte die geplante Gültigkeit für die IT-Sicherheitskennzeichnung von 2 Jahren und eine fehlende deutliche und transparente Abgrenzung gegenüber gemäß BSI-ZertV-zertifizierten IT-Systemen ein falsches Sicherheitsgefühl bei den Nutzern der Lösung erzeugen.

10. Bußgelder

    Deutlich angepasst wurden die Strafen bei Nichteinhaltung oder verspäteten Erbringungen von Anforderungen auf bis zu 2 Mio. Euro. Hierbei wurden die Strafen in der verabschiedeten Fassung klar gegenüber der ursprünglichen Planung abgemildert und eine Angleichung dieser an die Strafen in Bezug auf ein mögliches Strafmaß für Datenschutzverletzung gemäß DSGVO nicht vollzogen und damit weitestgehend dem Vorschlag der Deutsche Krankenhausgesellschaft e.V. gefolgte.[70]

4.3.2 BSI-KritisV

Auf Basis der Verordnung für Kritische Infrastrukturen erfolgt die Einteilung von klinischen Infrastrukturen in KRITIS-relevante Infrastrukturen und gemessen an den festgelegten Kriterien in weniger relevante Infrastrukturen. Durch die Verordnung werden aber nicht alle Akteure im Gesundheitswesen betrachtet. So werden Vorsorge- oder Rehabilitationseinrichtungen, MVZs und Krankenkassen als wesentliche Player innerhalb der klinischen Infrastruktur nicht mit in die Betrachtung einbezogen. **Klinikverbünde** werden gemessen an ihrer Bedeutung für die Versorgung **nicht** auf Basis der BSI-KritisV als **kritische Infrastruktur eingestuft**, auch wenn dies auf Basis Punkt 4d) des Anhangs 5 „unter gemeinsamer Leitung stehen“ durchaus möglich wäre. In Bezug auf Bewertung der TI als kritische Infrastruktur wurde bereits unter Punkt 4.3.1.2 eingegangen.

68 Vgl. Krempl (29.07.2021).
69 Vgl. Linus Neumann, Frank Rieger, Dirk Engling, Matthias Marx (01. März 2021).
70 Vgl. Deutsche Krankenhausgesellschaft e. V. (14. Januar 2021).

Die Einstufung als kritische Infrastrukturen alleinig auf Basis der definierten Schwellwerte spiegelt die Kritikalität für die Versorgung der Bevölkerung nicht abschließend wieder. So sollte in Bezug auf Krankenhäuser die regionale Lage und die Fachrichtungen in einer Risikobetrachtung mit einbezogen werden. Hierauf wird unter Punkt 6.3 „Auswirkung auf Versorgungssicherheit bei Ausfällen von klinischen Infrastrukturen“ weiter eingegangen.

4.3.3 BSI-Zertifizierungs- und -Anerkennungsverordnung

Die BSI ZertV ermächtigt das Bundesamt für Informationssicherheit Produkte, Systeme, die Informationssicherheit eines Managementsystems einer Organisation, Dienstleister und einzelne Personen zu zertifizieren und damit ihnen ein gewisses Maß an Sicherheit in Bezug von Vertraulichkeit, Authentizität, Verfügbarkeit und Fachkunden zu attestieren.
Im Bereich der Produktzertifizierung besteht die Möglichkeit der Hersteller, eine Zertifizierung gemäß des international anerkannten Common Criteria oder einer durch das BSI herausgegebenen Technischen Richtlinie. Mit dem ISO-27001-Zertifikat kann dem ISMS einer Organisation die Umsetzung des IT-Grundschutzes bescheinigt werden. IT-Sicherheitsdienstleiter und Personen können zum Nachweis deren Fachkunde entsprechende Zertifikate erlangen und sich darüber hinaus als externe Prüfstellen bzw. Auditoren akkreditieren lassen.
Die Zertifizierung von Produkten oder Systemen nach den technischen Richtlinien erfolgt eher selten, da diese keine internationale Anerkennung finden und daher für die Hersteller nicht interessant sind.
Eine Gewähr für die Zulässigkeit des Einsatzes von Geräten mit entsprechender Common Criteria-Zertifizierung von einem durch die Common Criteria for Information Technology Security Evaluation akkreditiertes Institut indes besteht nicht. Zum einem könnte das BMI gemäß §9b Absatz 4 BSIG den Einsatz in kritischen Infrastrukturen untersagen und zum anderen hat das BSI als nationale Akkreditierungsstelle die Möglichkeit, den Einsatz von Produkten, die durch eine andere Common Criteria Akkreditierungsstelle zertifiziert wurde, in kritischen Umgebungen zu untersagen, wenn deren Zertifizierungslevel höher als ELA4 ist.[71]
Auch besteht derzeit kein unmittelbarer Zusammenhang zwischen einer Zertifizierung und den Anforderungen hinsichtlich kritischer Komponenten gemäß §2 Absatz 13 BSIG und wird ebenfalls nicht bei der Definition von Sicherheitsanforderungen für Medizinprodukte berücksichtigt.

71 Vgl. Bundesamt für Sicherheit in der Informationstechnik (07.01.2021).

Überdies besteht seitens der gematik GmbH noch keine Spezifizierung hinsichtlich des Einsatzes von entsprechend zertifizierten Produkten innerhalb der TI zur Gewährleistung der Informationssicherheit; alleinig auf Basis einiger Technischer Richtlinien, z.B. TR-03110[72], TR-03114[73] und TR-03116[74], wird derzeit in den TI-Konzepten abgestellt, so das daraus derzeit nicht auf eine signifikante Bedeutung der Zertifizierung für die TI geschlossen werden kann.

4.3.4 Rechtsverordnung zum IT-Sicherheitskennzeichen

Die IT-Sicherheitskennzeichnung von informationstechnischen Produkten und Angeboten zielt insbesondere auf die Endverbraucher ab und soll damit Vertrauen in digitale Angebote schaffen und so zur vermehrten Nutzung dieser anregen. Mit der Kennzeichnung ihrer Produkte und Angebote verpflichten sich die Hersteller, innerhalb der Gültigkeitsdauer des Zertifikats die bestehenden IT-Sicherheitsanforderungen für die jeweilige Produktkategorie einzuhalten, mögliche Vulnerabilities schnellst möglich zu beheben und das BSI zu Sicherheitsvorfällen unverzüglich zu informieren. Der Nachweis über die Einhaltung der Anforderung kann durch eine Zertifizierung gemäß verabschiedeten technischen Richtlinien und Normen erfolgen.
Zum Zeitpunkt der Erstellung der Arbeit sind mit Breitbandroutern und E-Mail-Diensten bisher lediglich zwei Produktkategorien durch das BSI definiert.[75] Diese Produktkategorien für bereits weitverbreitete und mehrheitlich genutzte Angebot erscheinen allerdings nicht geeignet, nachhaltig die Sicherheit für neue Digitalisierungsangebot zu beeinflussen. Wie bereits im Kapitel 4.3.1.2 Änderungen gegenüber der BSIG V1.0 beschrieben, kann die Kennzeichnung auch ein falsches Sicherheitsgefühl verursachen. Eine Sensibilisierung der Verbraucher zu Sicherheitsthemen muss daher mit dieser Maßnahme einhergehen. Hierzu müssen unter anderem die Informationen zu den Produkten einfach und verständlich zugänglich gemacht werden. Planungen für ein entsprechendes Angebot scheinen nicht zu bestehen. Die durch das BSI eingerichtete Verbraucherseite[76] scheint hierfür weniger geeignet. Auch für die Erfüllung der Aussage

„Das IT-Sicherheitskennzeichen kann wichtige Fakten zu Sicherheitseigenschaften eines vernetzten Produkts verständlich zusammenfassen.“[77]

72 Vgl. gematik GmbH (02.03.2020).
73 Vgl. gematik GmbH (12.11.2020a).
74 Vgl. gematik GmbH (12.11.2020b).
75 Vgl. Bundesamt für Sicherheit in der Informationstechnik (16.07.2021a).
76 Vgl. Bundesamt für Sicherheit in der Informationstechnik (16.07.2021b).
77 Vgl. Bundesamt für Sicherheit in der Informationstechnik (16.07.2021c).

gibt es derzeit keine Anhaltspunkte.

Hier möchte man dem Vorschlag des Chaos Computer Club folgen, welcher eine Produkthaftung und Updatezwang zur Verbesserung der Sicherheit zur Diskussion stellt.[78] Insbesondere die Versorgung von Produkten mit aktuellen Patchen, mit definierter Nachsorgeregelung bei Vertriebsstopp, erscheint besser geeignet, das Sicherheitsniveau zu erhöhen, als dies die aktuelle Laufzeitregelung zur Zertifikatsgültigkeit vermag.

4.3.5 IT-Richtlinien der Deutschen Krankenhaus Gesellschaft

Dem branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus wurde 2019 durch das BSI die Eignung als Sicherheitsframework zur Implementierung von geeigneten Sicherheitsmaßnahmen im Sinne des BSI-Gesetzes attestiert. Ein Review des Dokumentes muss aller zwei Jahre erfolgen, was im zeitlichen Bezug der Verabschiedung des ITSiG 2.0 und der erfolgten Anpassung des SGB V im Rahmen des Krankenhauszukunftsgesetzes (KHZG) und dem DVPMG einen idealen Zeitpunkt darstellt.
Insgesamt ist der Standard im ersten Teil sehr generisch aufgebaut und stark an die ISO 27001 angelehnt. Erst im Weiteren über die Definition des Geltungsbereiches mit folgender Beschreibung der Gefährdungslage, der Bezugnahme auf die DIN EN 80001 beim Risikomanagement und der Einbindung von Medizinprodukten in die Netzwerkinfrastruktur bis hin zur Maßnahmenempfehlung wird spezifisch auf die Krankenhausinfrastruktur eingegangen.
Hierdurch bestehen erhebliche Freiheitsgrade, gerade in Bezug der Definition des Geltungsbereiches, bei der Implementierung eines ISMS. Hier sollte in Bezug des Reviews des Dokumentes eine klarere Definition eines mindestens zu betrachtenden Geltungsbereichs erfolgen. Ein weiterer Grund hierfür ist die Anforderung auf Grundlage des §75c SGB V, der die Implementierung eines ISMS auch in Krankenhäuser die nicht als kritische Infrastruktur gemäß der Kritis-Verordnung eingestuft sind vorsieht. Eine zusätzliche Ausrichtung des Rahmenwerks in Bezug zur teilstationären und ambulanten Behandlung könnte helfen die Digitalisierung von klinischen Prozessen sicher zu gestalten und eine Ausweitung auf MVZ, welche heute gemäß §75b SGB V über die IT-Richtlinien der KVB separat betrachtet werden, ermöglichen.

78 Vgl. Linus Neumann, Frank Rieger, Dirk Engling, Matthias Marx (01. März 2021).

Eine **einheitliche Definition des Geltungsbereichs** würde es ermöglichen, für die spezifische Umgebung eine allgemein gültige **Risikobetrachtung von zentraler Stelle** durchzuführen und unter Einbeziehung des Standortfaktors sowie den jeweils angebotenen klinischen Leitungen, im vorliegenden B3S als kritische Dienstleistung spezifiziert, und der damit einhergehenden Kritikalität der jeweiligen Einrichtung für die Gesundheitsversorgung der Bevölkerung **umzusetzende Maßnahmen konkret vorzugeben**. Dies könnte zu einer erheblichen Entlastung der Krankenhäuser in Bezug auf personelle Ressourcen führen und die Bündelung von Einkaufskapazitäten ermöglichen. Insgesamt wäre eine deutliche Erhöhung des übergreifenden Sicherheitsniveaus zu erwarten.
Eine Wirtschaftlichkeitsbetrachtung gemäß Punkt 5.3 im B3S in die Sicherheitsbetrachtung einfließen zulassen, ist insbesondere vor dem Hintergrund der sehr stark begrenzten und reglementierten finanziellen Mittel als nicht zielführend anzusehen. Eine Abwägung aus finanziellen Mitteln zum Tragen des Risikos in Bezug zum Schutz des Lebens erscheint, auch mit Blick zum Vorgehen im Rahmen der Covid-19-Pandemie, wo wirtschaftliche Gesichtspunkte dem Schutz der Bevölkerung untergeordnet wurden, auf Grundlage des hippokratischen Eides unzulässig. Daher ist das Schutzniveau aller Einrichtungen unabhängig von der finanziellen Ausstattung und Möglichkeiten einheitlich und hohem Anspruch zu gestalten. Die Umsetzung kann auch hier nur durch einen zentralistischen Ansatz gewährleistet werden. Unterschiedliche Schutzniveaus für Krankenhäuser und deren Fachabteilungen sind nur auf Basis ihrer Versorgungskritikalität, nicht aber auf Basis wirtschaftlicher Betrachtung zulässig. Eine Risikoakzeptanz durch die Geschäftsführung gemäß AMF-RM 27 aus diesen Gründen sollte daher ausgeschlossen werden.

4.3.5.1 Anpassungsbedarf auf Grund gesetzlicher Regelungen

Die Umsetzung des zentralistischen Ansatzes müsste mit einer Anpassung der Verantwortlichkeit für die Informationssicherheit einhergehen. Auf Grund der aktuellen Gesetzeslage bestehen für die gesamte Infrastruktur verschiedene Verantwortlichkeitsbereiche. Eine Teilung von Verantwortung und/oder Delegierung für einen definierten Bereich ist aber nicht möglich.
So wird beispielsweise in der aktuellen Version des B3S unter Punkt 5.2.1.1 die Betrachtung von unterschiedlichen Schnittstellen zwischen verschieden Akteuren des Gesundheitswesens im Rahmen der Definition des Geltungsbereiches verlangt. Diese Betrachtungen werden zukünftig aber nicht mehr spezifisch je Einrichtung erfolgen müssen, da die Schnittstellen auf Basis der Vorgaben durch die gematik GmbH standardisiert werden und somit auch eine einheitliche zentrale Sicherheitsbetrachtung dafür ermöglicht wird. Ein weiterer Aspekt welcher

für eine zentrale ganzheitliche Betrachtung spricht, ist die notwendige Ausweitung des Geltungsbereiches des ISMS auf Digitale Anwendungen, wenn auf Basis der erhobenen Daten eine Anamnese und Behandlung erfolgt und diesem Fall die Anwendung als kDL zu klassifizieren sind. In diesem Zusammenhang wären digitale Anwendungen auch als Medizinprodukte einzustufen. Für die Einbindung in der Krankenhausinfrastruktur ist dann entsprechend die DIN EN 80001-1 zu berücksichtigen.

Ein weiter kritischer Schnittpunkt von Verantwortlichkeiten könnte aus dem Umstand heraus entstehen, dass Krankenhäuser seit dem 30. Juni 2021 nur noch Informationstechnische Systeme zur Kommunikation mit den Teilnehmern der TI einsetzen dürfen, welche von der gematik GmbH freigegeben sind. Hierzu gehört auch das Krankenhaus Informationssystem. Das KIS unterliegt im Falle der Einstufung der Einrichtung als kritische Infrastruktur aber auch dem BSI, welches auf Basis des IT-Sicherheitsgesetzes Vorgaben für das KIS machen kann, insbesondere dann, wenn diese Anwendung als kritische Komponente eingestuft wird. Dieser sich anbahnende Konflikt hat im ungünstigen Fall negative Auswirkungen auf Hersteller und Betreiber. Hierbei ist das KIS nicht alleinig als kritische Komponente im Sinne §2 Absatz 13 BSIG zu betrachten, auch wenn das BSI in seiner aktuellen KRITIS-Sektor Studie nur explizit auf das KIS dort eingeht.[79] Als kritischen Komponenten sind sicherlich weitere Systeme der Informationstechnischen Systeme im Krankenhaus einzuordnen, auch wenn dem KIS als zentrales System eine übergeordnete Stellung zukommt. Daraus erwächst zusätzliches Konfliktpotential, sofern keine ganzheitliche Regelung für diesen Umstand getroffen wird.

4.3.5.2 Anpassungsbedarf auf Grund fortschreitender Digitalisierung

4.3.5.2.1 Risikoidentifikation

Bei der Risikoidentifizierung auf Grundlage des All-Gefahrenansatzes, siehe Punkt 4.2.3, sollte ausdrücklich auf die Risiken aus der Vernetzung von Systemen eingegangen werden. Mit Blick auf den im Juli 2021 erfolgten Angriff über den IT-Dienstleister Kaseya, welcher nicht als Einzelfall bezeichnet werden kann[80], müssen auch die Sicherheitsspezifika von Supply Chain Beziehungen geprüft werden. Eine Erweiterung der Betrachtung der Bedrohungen, welche außerhalb der eigenen Organisation liegen, sollte entsprechend weiter gefasst werden.

79 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020b).
80 Vgl. Berthold Wesseler (05.07.2021).

4.3.5.2.2 Kommunikationstechnik

Im Punkt 5.2.2.2 des Krankenhaus B3S wird im Rahmen technologischen Fortschritts von der Ablösung der Fax-Technologie durch Multifunktionsgeräte gesprochen. Diese Beschreibung ist irreführend und als Beispiel nicht geeignet. Eine Ablösung von Fax-Geräten durch Multifunktionsgeräten kann allenfalls Einfluss auf die Betrachtung der inhäusigen Kommunikationsbeziehung haben, da die Übertragung der Informationen mittels Simple Mail Transfer Protocol erfolgt. Zusätzlich könnte es hierdurch zu einer Änderung des Übertragungsverfahrens und des Übertragungsmediums kommen, sofern die Faxe vorher noch auf Basis analoger Übertragungstechnik und nicht bereits via Voice over IP übermittelt wurden. In Bezug auf die Übertragung einrichtungsübergreifend, z.B. bei der Kommunikation mit externen Laboren, hat dies jedoch keinen Einfluss, da die Carrier Infrastruktur bereits durchgängig IP-basierend ist und somit spätestens im Vermittlungsknotenpunkt eine Wandlung erfolgt. Da für die Kommunikation mit Akteuren im Gesundheitswesen die Schriftform gemäß §126 BGB nicht als zwingend erforderlich angesehen werden kann, sollte die Kommunikation vollständig auf die TI umgestellt werden und die Fax-Technologie nur noch in Ausnahmefällen, ggf. als Ersatzweg, aufrechterhalten werden.

4.3.5.2.3 Systeme der Versorgungsdienste

Die unter Punkt 5.2.3.9 beschriebene stark variierenden Anforderungen hinsichtlich der Verfügbarkeit und Integrität der Versorgungsdienste, wie Essensversorgung, Bettenmanagement oder Reinigung, erschließt sich nicht. Auswirkungen mögen je Patienten unterschiedlich sein, haben in Bezug der Betrachtung des Gesamtkontextes keine Relevanz auf die Patientensicherheit insgesamt.

4.3.5.2.4 Gefährdungen kritischer branchenspezifischer Technik

Für die branchenspezifische Technik erwachsen mit zunehmender Digitalisierung neue Gefährdungen bzw. müssen bestehende Gefährdungen neu bewertet werden, da Zugriffe auf die Systeme z.B. durch einen erweiterten Nutzerkreis erfolgt. Die Gefährdungen in Relevanz zu den Systemen untereinander bleiben bei Vernetzung der Systeme und damit fortführender Digitalisierung der klinischen Prozesse gleich, dennoch sind die Abhängigkeiten/Einflüsse neu zu bewerten. Dieser Umstand ergibt sich aus ggf. neuen, zeitlichen Parametern als auch daraus, dass heutige Prozesse als Notfall-Prozesse weiterhin etabliert bleiben müssen, damit die Verfügbarkeit des Gesamtprozesses auch bei Ausfall der Vernetzung gewährleistet werden kann.

4.3.5.2.5 Versorgungstechnik

Im Punkt 6.4.8 des Branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus attestieren die Autoren dem Bereich der Gebäudeautomatisierung/Versorgungstechnik einen bestehenden Innovationsdruck und bescheinigen diesem Bereich gleichzeitig enormes Schadenspotenzial. Im Rahmen der Digitalisierung muss in diesem Umfeld besondere Sorge getragen werden, damit diese Systeme nicht zum Einfalltor für Cyber-Attacken durch Anbindung der bisher in sich geschlossenen Netzwerke an die globalen Kommunikationsnetze werden. Ein weiterer Grund hierfür ist die Nutzung von veralten und damit größtenteils unsicheren Protokollen in den Systemen der Versorgungstechnik.

4.3.5.2.6 Redundante Anbindung

Sofern externe digitale Systeme Bestandteil von kDL sind und für deren Verfügbarkeit erforderlich sind, muss die Anbindung gemäß der ANF-MN 56 an diese Dienste redundant ausgelegt sein. Für die meisten Einrichtungen stehen adäquate, leitungsgebundene, redundante Anbindungen nur selten zur Verfügung. Die Verfügbarkeit von mobilen Verbindungen und deren spezifischen Sicherheitsanforderungen sind bei deren alternativen Einsatz zu betrachten. Auf Grund des unterschiedlichen strukturellen Ausbaus in Deutschland stehen in strukturschwachen Umgebungen entsprechende Angebote nicht zur Verfügung, wodurch die Gefahr besteht, dass diese Gegenden bei der Digitalisierung weiter abgehängt werden.
Sieht man die TI als eine Infrastruktur an in die Prozesse und Systeme zur Erbringung der kDL ausgelagert werden, so muss die Anbindung an die TI gemäß ANF-MN 92 redundant erfolgen, da eine Absenkung des Sicherheitsniveaus gemäß dieser Anforderung bei Auslagerung nicht zulässig ist.

4.3.5.2.7 Patch- und Änderungsmanagement

Alle Maßnahmen zur Absicherung einer Infrastruktur verlieren einen Großteil ihrer Wirkung bzw. Nutzung, wenn es potentiellen Angreifern durch nicht geschlossene Schwachstellen einfacher gemacht wird in diese einzudringen. Zur Vorbeugung und Schließung von Schwachstellen ist ein entsprechendes Patchmanagement mit vorgeschaltetem Vulnerability-Management erforderlich. Daher sind unter Punkt 7.13.13 des B3S auch entsprechende Anforderungen zur Implementierung eines entsprechenden Prozesses vorgeschrieben.
Damit aus der Einbringung neuer Software entstehende Risiken minimiert werden können, müssen diese Versionen im Vorfeld getestet werden. Dies sollte in einer realitätsnahen Testumgebung erfolgen um Interoperabilitätsprobleme mit anderen Systemen erkennen zu können. Daher ist zu prüfen, inwieweit die SOLL

Anforderung ANF-MN 138 in Bezug auf die Vorhalten eines Testsystems nicht in eine MUSS Anforderung zu wandeln ist.
Alternative zur Vorhaltung von eigenen Testsystemen je Einrichtung, könnte dies auch auf eine zentrale Organisation übertragen werden, welche entsprechende Interoperabilitätstests auf Anforderung durchführt und die Freigabe in Vertretung zur Organisation erteilt. Eine weitere Möglichkeit wäre die Nutzung von vollständig digitalisierten Umgebungen, welche die Produktivumgebung abbilden. Bei solchen Umgebungen spricht man auch von „Digitalen Zwillingen“. Patche und neue Softwareversionen könnten in diesen Umgebungen vor Einbringung in die Produktivumgebung getestet werden. Mittel KI-Unterstützung werden Abweichungen nicht nur schnell erkannt, sondern es kann auch das Verhalten bei sich verändernden Betriebsbedingungen und Laufzeitauswirkungen simuliert und betrachtet werden.
Medizinprodukte müssen im Rahmen des Patch- und Änderungsmanagement gesondert betrachtet werden, da diese durch Änderung von Softwarekomponenten ihre Zulassung verlieren würden, sofern die neue Software nicht explizit von einer Zertifizierungsstelle erneut zertifiziert wurde. Dies erschwert eine Digitalisierung unter Einbindung von Medizinprodukten erheblich, da diese Systeme in abgeschroteten Umgebunden betrieben werden, damit Angriffe darauf mit hoher Wahrscheinlichkeit ausgeschlossen werden können.

4.3.5.2.8 Beschaffung

Bereits bei der Beschaffung von digitalen Lösungen ist gemäß der ANF-MN 137 die DIN EN 80001 zu berücksichtigen. Häufig definieren Medizinprodukteherstellen Ihre Lösungen gesamtheitlich, was meist auch die Infrastruktur mit umfasst und bauen ihre Risikoabschätzung auf diese Gesamtlösung auf. Allerdings erfolgen die Herstellervorgaben zur Infrastruktur dann überwiegend nicht nur auf generischen Vorgaben, wie zu nutzende Protokolle und bereitzustellenden/einzuhaltenden Netzwerkvorgaben, sondern stützen diese auf bestimmte Produkte ab. Hierbei handelt es sich in der Regel um die in der Entwicklungs- und Testumgebung des Herstellers genutzten Produkten. Damit stehen die Betreiber der klinischen Infrastrukturen in einem Zwiespalt bei der Beschaffung von entsprechenden Geräten. Denn wenn die Systeme in nicht den Vorgaben entsprechenden Infrastrukturen ein- bzw. umgesetzt werden, geht das Haftungsrisikos des Herstellers auf den Betreiber der Lösung über. In diesem Fall ist ein Risikomanagementbetrachtung nach DIN EN 80001 zwingend durchzuführen, wobei die Herstellervorgaben zur Vermeidung des Unterlaufens der herstellerseitigen Risikostrategien beachtet und zu diesem Zweck durch die Hersteller zur Erfüllung gestellt werden müssen.

Da mit zunehmender Digitalisierung von heterogenen Netzen auszugehen ist und Hersteller die Risikoabschätzung nicht mehr vollumfänglich leisten können, muss eine klarere Definition der für die Risikoabschätzung seitens des Betreibers benötigten Informationen zur Absicherung der Hersteller und der Betreiber erfolgen.

4.3.5.3 weiterer Anpassungsbedarf

Die ANF-MN 106 ist gemäß des aktualisierten BSIG, welches einen verpflichtenden Einsatz von Intrusion Detection Systeme ab den 01. Mai 2023 vorsieht, in eine „MUSS"-Anforderung für KRITIS relevante Infrastrukturen umzuformulieren.

4.3.6 IT-Richtlinien der KVB

Die Kassenärztliche Bundesvereinigung ist gemäß §75b der am 09. Dezember 2019 geänderten Fassung des SGB V für die Erstellung einer IT-Richtlinie verantwortlich, welche die Sicherstellung des störungsfreien Betriebs der informationstechnischen Systeme in den vertragsärztlichen und vertragszahnärztlichen Versorgungseinrichtungen ermöglich soll. Mit dem ab den 14. Oktober 2020 gültigen PDSG erfolgte eine Erweiterung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit um nicht näher spezifizierte „weitere Schutzziele", eine Einschränkung der Gültigkeit auf Einrichtungen, welche nicht bereits Vorkehrungen im Sinne des §8a Absatz 1 BSiG oder andere branchenspezifische Sicherheitsstandards umgesetzt haben, sowie der Wechsel von einer Anbieter-Zertifizierung hin zu einer Personen-Zertifizierung.
Die KBV steht bei der Erstellung und Pflege der IT-Richtlinie, was nicht zwangsweise als Kernaufgaben der KBV angesehen werden kann, vor der Herausforderung die Richtlinie in Abstimmung mit zahlreichen Interessenvertretern abzustimmen und weiterzuentwickeln. So erscheint es wenig verwunderlich, dass die Anlage 5 zur sicheren Anbindung an die Telematikinfrastruktur ausschließlich auf Unterlagen der gematik GmbH verweist. Auch der Ansatz der Unterscheidung der Sicherheitsmaßnahmen in Abhängigkeit der Größe einer Einrichtung erscheint wenig geeignet und entspricht nicht der aus dem Gesetz ableitbaren Anforderung. Dort wird im Absatz 2 eine Abstufung der Anforderungen im Verhältnis zum Schutzbedarf der verarbeiteten Informationen gefordert.[81] Die Art der verarbeiteten Informationen können im Allgemeinen aber als Unabhängig von der Größe der Einrichtung angesehen werden. Die getroffene Abstufung scheint maßgeblich aus wirtschaftlichen Beweggründen heraus getroffen worden zu sein. Weiterhin werden wichtige Punkte einer IT-Sicherheitsrichtlinie, wie Geltungsbereich, Verantwortlichkeit und Hinweise bei Missachtung der Richtlinie

81 Vgl. Dr. med. Petra Reis-Berkowicz (16.12.2020).

nicht adressiert. Vielmehr erscheint die Richtlinie mehr als ein Katalog mit sehr unspezifischen Maßnahmen. Eine fachgerechte und zielgerichtete Umsetzung durch die jeweiligen Praxis-Betreiber erscheint auf dieser Basis nur bedingt möglich. Auch fehlt jeder Kontext zwischen der Richtlinie und der Zertifizierung. Vielmehr wird in den FAQs darauf verwiesen, dass nicht zwingend zertifizierte Unternehmen mit der Einrichtung der IT und Umsetzung der Sicherheitsmaßnahmen beauftragt werden müssen.[82] Ein Zugewinn an Sicherheit ist daher mehr als fraglich anzusehen.
Zur einfachen Kontrolle für die Praxis-Betreiber ist eine Liste von einsetzbaren Anwendungen und Systemen zu erstellen sowie die Implementierung nur durch Anbieter mit entsprechend zertifizierten Mitarbeitern als zulässig zu erklären. Die Vorgaben müssen spezifiziert und in leicht verständlichen Tutorials erklärt werden. Aussagen wie

> *„Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.“*

lassen Interpretationsspielraum und ist von nicht technisch affinen Personen nur bedingt umsetzbar.
Absolute Maßnahmen in Bezug auf mobile Anwendungen wie die Anforderung 4, keine vertraulichen Daten über Apps zu versenden, verhindert dahingegen jegliche Umsetzung/Einführung von digitalen Prozessen unter Wahrung der notwendigen Mobilität.
Die KVB sollte daher hier von ihrer Verantwortung entbunden werden und diese an **eine** Organisation wie die gematik GmbH oder das BSI übertragen werden. Diese muss mit der Erstellung einer geeigneten IT-Sicherheitsrichtlinie im Gesamtkontext der Digitalisierungsstrategie beauftragt und deren Durchsetzung sichergestellt werden.

4.3.7 IT-Richtlinien der gematik GmbH

Wie bereits eingehend in Kapitel 2.1.9 dargelegt, betreibt die gematik GmbH im Auftrag des Bundesministeriums für Gesundheit, der Krankenkassen und der Leistungserbringer die Telematikinfrastruktur. Auf Grundlage §311-ff SGB V ist sie als Betreiber auch für die Sicherheit innerhalb dieser Infrastruktur verantwortlich. Hierzu hat die gematik GmbH vielfältige Spezifikationen für die Anforderungen in Bezug auf Schnittstellen, Systeme, Hersteller und Dienstleistern herausgegeben. Eine Übersicht zu den aktuellen Dokumenten kann dem Anhang C ent-

82 Vgl. Dezernat Digitalisierung und IT (2021).

nommen werden. Die Spezifikationen enthalten umfassende Sicherheitsanforderungen, welche auf den BSI Grundschutz, dem BSI-Standards zur Internet-Sicherheit und der ISO 27001 referenzieren. Die Anforderungen aus den Spezifikationen müssen auch durch die IT-Abteilungen bzw. IT-Dienstleistern der Nutzer der Telematikinfrastruktur bekannt sein, da Vorgaben aus den Richtlinien Auswirkungen über die Zugangspunkte hinaus auf die IT-Infrastruktur haben, um die Gesamtfunktionalität sicherzustellen. So werden in der übergreifenden Netzwerkspezifikation zentrale Vorgaben für DiffServ-Klassen gemacht, welche innerhalb der IT-Infrastruktur konfiguriert und weitergegeben werden müssen, um eine End-to-End-Übermittlung und so eine entsprechendes QoS zu ermöglichen.
Insgesamt muss aber festgestellt werden, dass durch die Fülle an Informationen und dem schwierigen Zugang auch die Gefahr besteht, eher das Gegenteilige zu erreichen, als auf das die Maßnahmen, dem Zugewinn an Sicherheit, abzielen. Auch die unterschiedlich gültigen Versionsstände der Richtlinien je Anwendungsfall tragen nicht zu einem besseren Verständnis bei.
Hinsichtlich der Wirksamkeit und Nachvollziehbarkeit der vorgeschlagenen Maßnahmen kann keine abschließende Bewertung vorgenommen werden, allerdings sollten diese, wie am Beispiel der Maßnahme „GS-A_4062 – Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen“ deutlich wird, hinterfragt werden. Gemäß diesen Anforderungen müssen entsprechende zentrale Übergänge (SZZPs) durch ein dreistufiges Firewallsystem in der P-A-P Struktur oder durch ein BSI zertifiziertes Sicherheitsgateway abgesichert werden.[83] Auch eine nach Common Criteria Level EAL-7 zertifizierte Firewall kann das Sicherheitsniveau allenfalls in Bezug auf die Verfügbarkeit einer nach dem Stand der Technik realisierten P-A-P Struktur erreichen bzw. übertreffen, da die Gesamtverfügbarkeiten von hintereinander geschalteten Systemen kleiner ist als die Verfügbarkeit jedes einzelnen Systems. Auf Grund der bestehenden Anforderung der redundanten Auslegung, GS-A_4785, kann der Nachteil der P-A-P Struktur gegenüber dem Einzelsystem als vernachlässigbar angesehen werden.

4.4 Datenschutz

Der Datenschutz spielt bei der Verarbeitung von Gesundheitsdaten eine **außerordentliche Rolle**. Gesundheitsdaten einer natürlichen Person fallen unter Artikel 9 der DSGVO, welche die Verarbeitung besonderer Kategorien personen-

83 Vgl. gematik GmbH (09.07.2021).

bezogener Daten regelt. Neben der Europäischen Datenschutz Grundverordnung sind auch noch weitere Regelungen zum Datenschutz, wie dem Bundesdatenschutzgesetz, der Musterberufsordnung-Ärzte und das Patientendatenschutzgesetz, zu beachten. Neben der Vertraulichkeit, welche sich insbesondere auch durch die im §9 der Musterberufsordnung-Ärzte geregelten Schweigepflicht ausdrückt, gehören auch weitere Schutzziele, wie Integrität und Verfügbarkeit, zum Datenschutz. Dem Rechnung tragend, erfolgte im Rahmen der Verabschiedung des PDSG die Aufnahme des §75c in das fünfte Sozialgesetzbuch. Wie bereits in vorangegangen Kapitel dargelegt, sind alle Krankenhäuser angehalten, entsprechende Technische und Organisatorische Maßnahmen nach dem Stand der Technik zum Schutz der Patientendaten zu treffen. Mit Satz 2 des §75c SGB V werden prinzipiell alle Krankenhäuser in Bezug auf die Einhaltung branchenspezifischer Sicherheitsstandard gleichgesetzt, unabhängig davon, ob diese als kritische Infrastruktur eingestuft sind. Die Möglichkeit einer Eingrenzung des Geltungsbereiches durch Definition eines entsprechenden Informationsverbundes auf die an die Telematikinfrastruktur angeschlossenen IT-Systeme ist hierbei nicht gegeben. Wohl aber werden die Betreiber der dezentralen Komponenten zur Anbindung an die TI von der Notwendigkeit der Durchführung einer Datenschutzfolgeabschätzung gemäß Artikel 35 Absatz 10 der Verordnung (EU) 2016/679 entbunden, sofern die Inbetriebnahme ordnungsgemäß, den Vorgaben der gematik GmbH entsprechend, erfolgt. Eine zentrale, einheitliche Vorgabe in Bezug von Aspekten der Sicherheit ist im Sinne eines ganzheitlichen Ansatzes zu begrüßen, trägt aber möglicherweise zu einer Reduzierung des Schutzniveaus bei. Dies wäre dann gegeben, wenn die Regelung sich ausschließlich auf die Systeme zur Anbindung an die TI bezieht und nicht den Prozess der Erfassung und Eingabe miterfasst. Damit kann der Annahme zum daraus resultierenden Einsparpotential in Höhe von 851 Mio. Euro nicht gefolgt werden, wenn gleich einheitlichen Vorgaben nicht nur für das Schutzziel Vertraulichkeit wünschenswert sind.[84] Darüberhinausgehend werden mit dem PDSG Regelungen zur Bereitstellung der TI-Dienste von

- E-Rezepten,
- elektronischen Patientenakten,
- elektronischen Medikationsplänen und Notfalldatensätzen sowie
- der digitalen Kommunikation

getroffen.

84 Vgl. Gerlof (17.11.2020).

Ab dem 1. Januar 2022 muss dann in der ePA auch ein entsprechendes Rechtemanagement implementiert sein.[85] Darüber soll den Versicherten die Möglichkeit eingeräumt werden, die Freigabe bzw. Weitergabe seiner persönlichen Daten dediziert zu verwalten. Inwieweit dieses Rechtemanagement auch eine Rücknahme der Berechtigung mit gleichzeitiger Löschung der Daten beim jeweiligen Leistungserbringer berücksichtigt, ist nicht bekannt. Hierfür dürfte die Daten nur lesend freigegeben werden oder dürften nur verschlüsselt offline beim Leistungserbringer mit entsprechenden Zugriffsmanagement gespeichert werden. Da eine Datenverarbeitung derzeit nur mit unverschlüsselten Daten möglich ist, würde nur die erste Variante in Frage kommen.

Über die datenschutzrechtlichen Regelungen zur TI hinausgehend spezifiziert das PDSG die Datenschutzbestimmung zum Umgang mit Patientendaten, die durch digitale Systeme erfasst und ausgewertet werden. Grundsätzlich müssen diese den Regelungen der DSGVO entsprechen. Aus diesem Beweggrund heraus ist bei der Einführung und Nutzung von Cloud-basierenden digitalen Anwendungen oder Daten-Analyse, Big-Data, ein besonderes Augenmerk auf die vertraglichen Regelungen zum Datenschutz zu legen. Gerade bei externer Verarbeitung muss eine entsprechende Rechtsgrundlage mit der jeweiligen Person geschaffen werden und die Daten sollten zumindest pseudonymisiert, besser anonymisiert, werden. Bei der Speicherung und Verarbeitung der Daten bei Anbietern außerhalb der Europäischen Union muss sorgfältig geprüft werden, inwiefern die auf diese Anbieter wirkenden Regelungen den Bestimmungen der DSGVO oder dem Bundesdatenschutzgesetz konterkarieren. Insbesondere häufig genutzte amerikanische Anbieter wie Microsoft oder Google erfüllen nicht die europäischen datenschutzrechtlichen Anforderungen. Vormals bestehende allgemeine Regelungen wie der Safe-Harbor-Pakt und dessen Nachfolger, das EU-US Privacy Shield, wurden durch den EuGH aufgehoben bzw. für ungültig erklärt, so dass zum Entsprechen der DSGVO derzeit nur einzelvertragliche Regelungen zum Datenschutz dies gewährleisten können. Aber auch wenn diese Anbieter einer entsprechenden Regelung eingehen würden, sind die Daten auf Grund von nationalen Bestimmungen in den USA, wie dem PATRIOT Act, nicht vor unberechtigtem Zugriff geschützt. Daher muss dringend die Nutzung eines europäischen, der DSGVO unterliegenden Anbieters angeraten werden. Besser wäre hier die Schaffung einer sicheren, datenschutzkonformen Lösung innerhalb der TI. Aber auch die Speicherung der Daten in einer Cloud stellt alleinig nicht die Anforderungen an Verfügbarkeit sicher, wie das Beispiel des Rechenzentrums-

85 Vgl. Baeuerle (2021).

Brandes beim größten europäischen Cloud-Anbieters OVH zeigt[86]. Verantwortlich für die Daten bleibt immer der Auftraggeber und dies entbindet nicht von seiner Verantwortung.
Mit der angestrebten Übertragung der Datenhoheit auf den Patienten, siehe hierzu auch Punkt 2.2 Kommunikationsbeziehungen, muss auch ein Paradigmenwechsel in Bezug der Akzeptanz von Datenschutzbestimmungen einhergehen. Die heute gelebte Praxis, dass der Patient die Bestimmung zur Verarbeitung der Daten der/des Anbieters akzeptieren muss, um das Angebot nutzen zu können, ist nicht verbraucher- und patientengerecht. Die Vorgaben zu dem durch den Anbieter mindestens zu erfüllenden Datenschutzniveau sollten durch die jeweilige Person vorgegeben werden und sind bei Datennutzung durch diesen zu erfüllen. Nur so können Mündigkeit und Datenhoheit des Patienten sichergestellt werden. Der Abgleich der Anforderungen kann im Rahmen der Datenfreigabe digital durchgeführt werden, indem dies Teil der Zugriffsautorisierung ist.

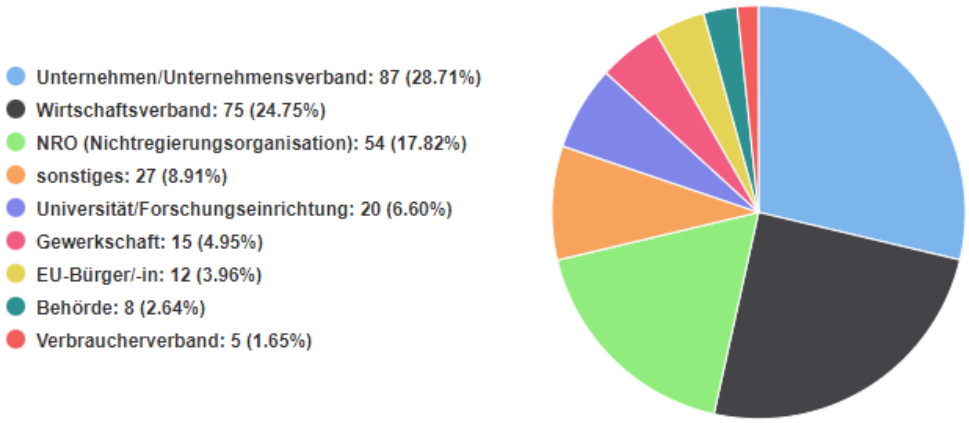
4.5 KI-Verordnung

Ein spezieller rechtlicher Rahmen für die Entwicklung und Nutzung von künstlicher Intelligenz besteht derzeit noch nicht. Dies soll sich durch die am 21. April 2021 vorgelegte KI-Verordnung der Europäischen Union ändern. Die EU verfolgt damit folgende vier Ziele

- Gewährleistung der sicheren Bereitstellung und Verwendung von KI-Systemen
- Rechtssicherheit bei der Förderung und Investition in entsprechende Systeme
- Stärkung der Governance zur Wahrung der Grundrechte und Werte
- Bereiten des EU-Binnenmarktes für rechtskonforme, vertrauenswürdige und sichere KI-Anwendungen

Dem Grundgedanken dieser Verordnung gerecht zu werden und dabei alle Stakeholder so abzuholen, dass diese sich und ihre Anforderungen in der Gesetzgebung wiederfinden, stellt eine der größten Herausforderung seit der Einführung der Datenschutzgrundverordnung dar. Das immense Interesse an diesem Thema wird nicht nur durch tägliche Beiträge über verschiedenste Medien dokumentiert, sondern belegen auch die 303 gültigen Rückmeldung zur KI-Verortung durch verschiedenste Interessengruppen.

86 Vgl. Ehneß (16.08.2021).



Quelle: Europäische Kommission, 16.09.2021

Abbildung 15: Rückmeldung zur KI-Verortung nach Interessensgruppen

Zwar wird die Schaffung eines entsprechenden Rahmens von den meisten Seiten begrüßt, jedoch bestehen unterschiedlichste Anforderungen und damit verbundene Unsicherheiten. Auf Grund der hohen Innovationsgeschwindigkeit in diesem Bereich stellt sich die Frage, inwieweit diese notwendige Zeit tatsächlich noch vorhanden ist oder durch entstehende Lösungen überholt wird. Möglicherweise sollte man sich einem gemeinsamen gesetzlichen Rahmen in der Form nähern, indem sich analog zur Einführung einer Sicherheitsstrategie nach dem Top-Down-Prinzip zuerst auf eine grundsätzliche Policy verständigt wird, welche dann bereits als grundlegender Rahmen dienen kann. Die Ausgestaltung kann dann nachgelagert in entsprechenden Richtlinien und Konzepten angegangen werden. Wichtigste Punkte diese Policy sollte die Sicherheit, der Umgang mit den persönlichen Daten und die Ethik sein.

Hinsichtlich der Sicherheit sollte, unabhängig des von der KI ausgehenden Risikos, der Maxime zur Kontrolle der KI gemäß der von Bosch herausgegebenen Leitlinie Beachtung finden, nach der der Mensch in letzter Instanz die Entscheidung treffen und die KI ihm dienen sollte.[87]

In Bezug zur Ethik würde ich grundsätzlich Prof. Ulrich Kelber folgen wollen, wonach der Einsatz von Künstlicher Intelligenz verboten werden sollte, wenn sie die Persönlichkeit und Würde des Menschen nicht achtet.[88]

Für die Komponente des Datenschutzes steht mit der DSGVO ein wirksames Mittel zur Verfügung. Insbesondere sollten die Grundsätze zur Verarbeitung von personenbezogenen Daten gemäß Artikel 5 DSGVO und Artikel 25 der DSGVO

87 Vgl. Bosch Global (19. Februar 2020).
88 Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (21.06.2021).

in Bezug der Gestaltung von technischen Systemen zu datenschutzfreundlichen Voreinstellungen angewandt werden.[89]

Bevor sich den vorgenannten Punkten zugewandt werden kann, gilt es aber, einen Konsens zur Definition „Was ist Künstlichen Intelligenz“ zu finden, also ab wann ein technisches System zur KI wird. Systeme, die keine maschinellen Lernverfahren nutzen, erfüllen diesen Anspruch möglicherweise nicht. Daher kann die Forderung zur genaueren Spezifizierung der aktuellen Definition nachvollzogen werden. Derzeit werden gemäß Artikel 3 Absatz 1 und Anhang I der KI-Verortung auch Systeme, die auf Basis von Logik- und wissensgestützten Verfahrenstechniken basieren, ebenfalls den KI-Systeme zugeordnet. In Bezug auf Medizinprodukte würde dies für viele Anwendungen eine Einstufung als Hochrisiko-System bedeuten.[90] Offen bleibt in diesem Zusammenhang auch der Umgang mit Bestandsystemen, wobei sich diese Problemstellung mit zunehmender Zeit ohne spezifische Regelung stätig vergrößert. Auch wenn noch viele Fragen nicht im Detail endgültig geklärt sind, sollte hier schnellst möglich eine Rechtssicherheit geschaffen werden und man muss aufpassen, die gesteckten Ziele nicht durch zu viele bürokratische Formalien und vor allem auf Grund des Zeitfaktors zu verfehlen.

4.6 Das Sozialgesetzbuch

Das Sozialgesetzbuch umfasst die gesetzlichen Regelungen im Bereich des öffentlichen Rechts zur Wahrung der Rechte der Bürger im Bereich der Sozialleistungen, wie Arbeit, Gesundheit und Rente, und ist in 12 Teile gegliedert. Für die Betrachtung des Gesundheitswesens ist daher das fünfte Sozialgesetzbuch von hoher Relevanz. Wie bereits in vorangegangen Kapiteln dargestellt, stellen die nachfolgend noch einmal aufgeführten Gesetze vornehmlich eine Erweiterung des SGB V dar und gliedern sich entsprechend ein.

- Digitale-Versorgung-Gesetz
- Digitale-Versorgung- und Pflege-Modernisierungs-Gesetz
- Patientendaten-Schutz-Gesetz
- Krankenhauszukunftsgesetz

Weiterhin bildet das SGB V, wie auch bereits hinreichend dargelegt, die gesetzliche Grundlage für die gematik GmbH zur Bereitstellung und den Betrieb der Telematikinfrastruktur.

89 Vgl. Datenschutzkonferenz (3. April 2019).
90 Vgl. Johner Institut GmbH (06 August 2021).

Von wesentlicher Relevanz mit Bezug auf die Informationssicherheit von klinischen Infrastrukturen sind die Paragraphen

- § 75b - Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung Datenschutz
  (Aufnahme in SBG V im Rahmen des DVG vom 19.12.2019)
- § 75c - IT-Sicherheit in Krankenhäusern
  (Aufnahme in SBG V im Rahmen des PDSG vom 20.10.2020)
- § 139e - Verzeichnis für digitale Gesundheitsanwendungen; Verordnungsermächtigung
  (Aufnahme mit DVG und Erweiterung um Absatz 10 und 11 mit DVPMG vom 03. Juni 2021)
- § 286 - Datenübersicht
- § 291 - Elektronische Gesundheitskarte
- §§ 306-311 - Anforderungen an die Telematikinfrastruktur
- §§ 329-333 - Überwachung von Funktionsfähigkeit und Sicherheit
- §§ 371-375 - Anforderungen an Schnittstellen in informationstechnischen Systemen
- § 389 - Empfehlung von Standards, Profilen und Leitfäden von informationstechnischen Systemen im Gesundheitswesen als Referenz

Damit bildet das SGB V die gesetzliche Grundlage der IT-Sicherheit für den überwiegenden Teil der Akteure im Gesundheitswesen. Ausgenommen von den darin getroffenen Regelungen sind folgende Akteure

- Vorsorge- oder Rehabilitationseinrichtungen
- Kritische Infrastrukturen
  - Krankenhäuser
  - Labore
  - Apotheken
  - Hersteller

Kontrovers ist die Definition der **verschiedenen Verantwortlichkeiten** und Abstimmungsbedarf zwischen einzelnen Parteien zusehen. So werden mit dem BSI, der gematik GmbH und dem KBV drei Parteien eine führende Rolle in unterschiedlichen Bereichen zugestanden, aber **keine** führende Rolle für die **Gesamtverantwortung** benannt.

4.7 Finanzierung

Wie bereits unter Punkt 3.2 ausgeführt, leistet sich Deutschland eines der teuersten Gesundheitssysteme bezogen auf das Bruttoinlandsprodukt. Die Finanzierung des Gesundheitssektors erfolgt hierbei über die Solidargemeinschaft und geht auf die durch Otto von Bismarck 1883 eingeführte Sozialgesetzgebung zurück. Nicht nur auf Grund der enormen Kosten werden fortlaufende Änderungen an dem dualen Finanzierungskonzept durchgeführt und auf Einsparpotential geprüft. Die Digitalisierung soll hierbei ein wesentlicher Baustein darstellen. Allerdings steigen mit zunehmender Digitalisierung auch die Anforderungen an die Informationssicherheit, was dem Einsparpotential entgegenwirkt. Inwieweit die Digitalisierung tatsächlich geeignet scheint, die finanziellen Probleme im Gesundheitsbereich zu lösen, erscheint, vor dem Hintergrund der Aussage, dass dreiviertel der Krankenhäuser in Deutschland nicht investitionsfähig sind, sehr fraglich. Verstärkt wird dieser Eindruck vor dem eingangs erwähnten Hintergrund der hohen finanziellen Aufwendungen für die Umsetzung einer sicheren Digitalisierungsstrategie und dem späteren Betrieb. So ist es nicht verwunderlich, wenn immer wieder eine Neuausrichtung des Gesundheitssektors und dessen Finanzierung gefordert wird.[91]

Das duale Finanzierungskonzept sieht die Abrechnung von medizinischen Leistungen auf Basis von Fallpauschalen vor. Über diesen Fallpauschalen werden allerdings keine Investitionen abgedeckt. So müssen entsprechende Vorhaben über Fördermittel oder Eigenkapital bzw. Bankdarlehens finanziert werden. Für die Förderung von Digitalisierungsvorhaben im Krankenhaussektor wurde zum Zweck der Erhöhung des Digitalisierungsgrades das Krankenhauszukunftsgesetz auf den Weg gebracht. Diese sieht die Förderung von entsprechenden Vorhaben mit einem Volumen von drei Mrd. Euro durch Bundesmittel vor. Voraussetzung für die Bewilligung des Vorhabens ist eine Beteiligung am Gesamtfinanzierungsvolumen vom 30% durch das jeweilige Land und/oder der beantragenden Einrichtung, wodurch ein Gesamtinvestitionsvolumen auf ca. 4,3 Mrd. Euro zur Verfügung steht. Zusätzlich muss das Vorhaben unter einen der folgenden Fördertatbestände gemäß §19 Absatz1 Krankenhausstrukturfonds-Verordnung fallen.

1. Anpassung der technischen/informationstechnischen Ausstattung der Notaufnahme eines Krankenhauses an den jeweils aktuellen Stand der Technik
2. Patientenportale

91 Vgl. VKD Verband der Krankenhausdirektoren Deutschlands e.V (05. Oktober 2021).

3. Digitale Pflege- und Behandlungsdokumentation
4. Einrichtung von teil- oder vollautomatisierten klinischen Entscheidungsunterstützungssystemen
5. Digitales Medikationsmanagement
6. Digitale Leistungsanforderung
7. Leistungsabstimmung und Cloud-Computing-Systeme
8. Digitales Versorgungsnachweissystem für Betten zur Verbesserung der Zusammenarbeit zwischen Krankenhäusern und anderen Versorgungseinrichtungen
9. informationstechnische, kommunikationstechnische und robotikbasierte Anlagen, Systeme oder Verfahren und telemedizinische Netzwerke
10. IT-Sicherheit
11. Anpassung von Patientenzimmern an die besonderen Behandlungsformen im Fall einer Epidemie

Neben dem Fördertatbestand 10 soll mit der Anforderung, min. 15% des Investitionsvolumens in die IT-Sicherheit zu investieren, den in diesem Bereich gestiegenen Anforderungen Rechnung getragen werden.

Die Ermittlung des Fördervolumens scheint hierbei losgelöst von einer tatsächlichen Bedarfsfeststellung erfolgt zu sein, da die Verteilung der Fördermittel nicht projektbezogen, sondern überwiegend pauschal erfolgt. Diese pauschale Verteilung der Mittel liegt auch in dem für eine Projektinitiierung und Ausschreibung der Leistungserbringung zu kurzem Antragszeitraum. Diese Pauschalisierung bezieht sich aber nur auf die Landesebene.[92] Weiterhin erforderlich ist die Bewilligung jedes einzelnen Projektes durch das Bundesamt für Soziale Sicherung. Dort sind, Stand 31. Juli 2021, 413 Anträge mit einem Fördervolumen von erst 244 Mio. Euro eingegangen.[93] Ein weiteres Indiz für eine unzureichende Evaluierung des Bedarfs sind die weit auseinandergehenden Vorstellungen am benötigten Investitionsumfang. Auch wenn das Deutsche Krankenhausinstitut nicht explizit den Bedarf für Digitalisierung beziffert, so ist die jährliche Deckungslücke von mehr als 4 Mrd. Euro doch erheblich und kann durch die aufgelegte zusätzliche Förderung von Digitalisierungsvorhaben nur abgemildert werden.[94] Daher ist anzunehmen, dass viele Häuser die mit der Maßnahme verbundenen Ziele nicht erreichen werden und damit eine Kürzung der Fallpauschalen um bis zu 2% gemäß §5 Absatz 3h Krankenhausentgeltgesetz ab dem 1. Januar 2025 befürchten müssen, was bei viele Häuser zu einer weiteren Schieflage des Haushaltes

92 Vgl. SYNAGON (07.05.2021).
93 Vgl. Antares Computer Verlag GmbH (15.08.2021).
94 Vgl. Dr. Karl Blum (15.08.2021).

führen kann und diese damit ihren Versorgungsauftrag nicht mehr gerecht werden können. Weiterhin ist ab diesem Zeitpunkt ungeklärt, wie die zusätzlichen Betriebskosten für die aufgebauten Infrastrukturen aufgebracht werden sollen.
Die Herausforderung bzgl. der Finanzierung der zukünftigen Betriebskosten, vor der die Krankenhäuser stehen, soll am Beispiel der Vivantes Netzwerk für Gesundheit GmbH aufgezeigt werden. Das IT-Budget für die Digitalisierung von Vivantes lieg bei ca. 25 Mio. Euro/Jahr und gliedert sich in

55% Sachkosten (Wartungs-, Softwarepflege- und externe IT-Kosten)
20% Personalkosten und
25% Investitionskosten

auf.[95] Über das KHZG stehen für Vivantes zusätzliche Gelder von ca. 63. Mio. Euro über die nächsten 4 Jahre zur Verfügung. Bei einer angenommenen Übertragung dieser Verhältnisse auf die zusätzliche Fördersumme ergeben sich heraus ohne die Betrachtung der Ablösung von älteren Systemen zusätzliche jährliche Sachkosten in Höhe von 8,7 Mio. Euro, welch auch über den Förderzeitraum hinaus durch die jeweilige Einrichtung zur Aufrechterhaltung des erreichten Digitalisierungsgrades finanziert werden müssten. Aber auch unter der Berücksichtigung aller Faktoren ist nicht davon auszugehen, dass sich die Sachkosten auf das Niveau vor der Erhöhung der Digitalisierung einstellen, wodurch eine Finanzierungslücke bei den Einrichtungen entsteht. Ein weiteres Problem ergibt sich aus dem Ressourcenbedarf für die Umsetzung der Digitalisierungsmaßnahme. So beschäftigt die Vivantes Netzwerk für Gesundheit GmbH heute 80 Fachkräfte in der IT. Für die Umsetzung der Maßnahmen entsteh ein zusätzlicher Bedarf von 48 Stellen. Mit der notwendigen Bereitstellung zur Umsetzung und dem Umgang mit dem Personal nach der Umsetzung der Projekte ergeben sich zwei Herausforderungen, welche nicht gelöst werden können und damit zum Hemmnis der Digitalisierung werden.
Neben den jeweiligen Digitalisierungsvorhaben der einzelnen Häuser sollten dies auch die Anbindung an die TI bis spätestens Ende 2021 umsetzen. Hierfür erfolgt eine pauschale Erstattung der angenommenen Kosten für die Anbindung und den Betrieb. So wird bespielhaft der Investitionsaufwand für die Anpassung der krankenhausinternen Software mit 50.000 Euro pauschalisiert. Eine notwendige Anpassung der Krankenhausprozesse wurde nicht in die Berechnung der Pauschalen berücksichtigt. Für die anderen Teilnehmer der TI gibt es vergleichbare Erstattungspauschalen für die Erstausstattung und den Betrieb. Alleinig bei den

95 Vgl. Gunther Nolte (11.03.2021).

Krankenhäusern erscheint der Notwendigkeit einer Anbindung mit der Androhung einer Pönale in Höhe von 1% der erstattungsfähigen Fallpauschalen Nachdruck verleihen zu müssen.

4.8 Auswirkungen der gesetzlichen Vorgaben

4.8.1 Fehlenden Gesetzesgrundlagen für IT-Sicherheit

Trotz der umfassenden Regelung zur IT-Sicherheit im Gesundheitsumfeld besteht in Bezug auf die Vorsorge- oder Rehabilitationseinrichtungen und Apotheken, welche nicht als kritische Infrastruktur eingestuft sind, keine gesetzliche Grundlage und Vorgaben für die Umsetzung von IT-Sicherheitsmaßnahmen. Als Teilnehmer der Telematikinfrastruktur stellen diese beiden Akteure daher ein erhöhtes Sicherheitsrisiko dar. Die Bundesvereinigung Deutscher Apothekerverbände definiert in Ihren Ethischen Grundsätzen zu E-Health unter Punkt 8 das zwingende Erfordernis zum Schutz der Informationen und Infrastrukturen, hat aber Stand heute noch keine entsprechende IT-Richtlinie für seine Mitglieder veröffentlich.[96] Als schwerwiegender als das Fehlen von Vorgaben für Apotheken können fehlende Informationssicherheitsanforderungen für die mehr als 1.000 Vorsorge- oder Rehabilitationseinrichtungen angesehen werden, da hier nicht nur Mitarbeiter und Dienstleister Zugang zu IT-Einrichtungen haben, sondern auch weitere Personengruppen wie Patienten und Gäste. Eine Betrachtung dieses Einrichtungstyps sollte daher dringend im Rahmen des Digitale-Versorgung- und Pflege-Modernisierungs-Gesetz erfolgen. Die jeweiligen gesetzlichen Zuständigkeiten sind in der nachfolgenden Abbildung noch einmal graphisch aufbereitet und veranschaulichen die teilweise überschneidenden und auch fehlenden Grundlagen.

96 Vgl. Bundesvereinigung Deutscher Apothekerverbände (29. Oktober 2015).

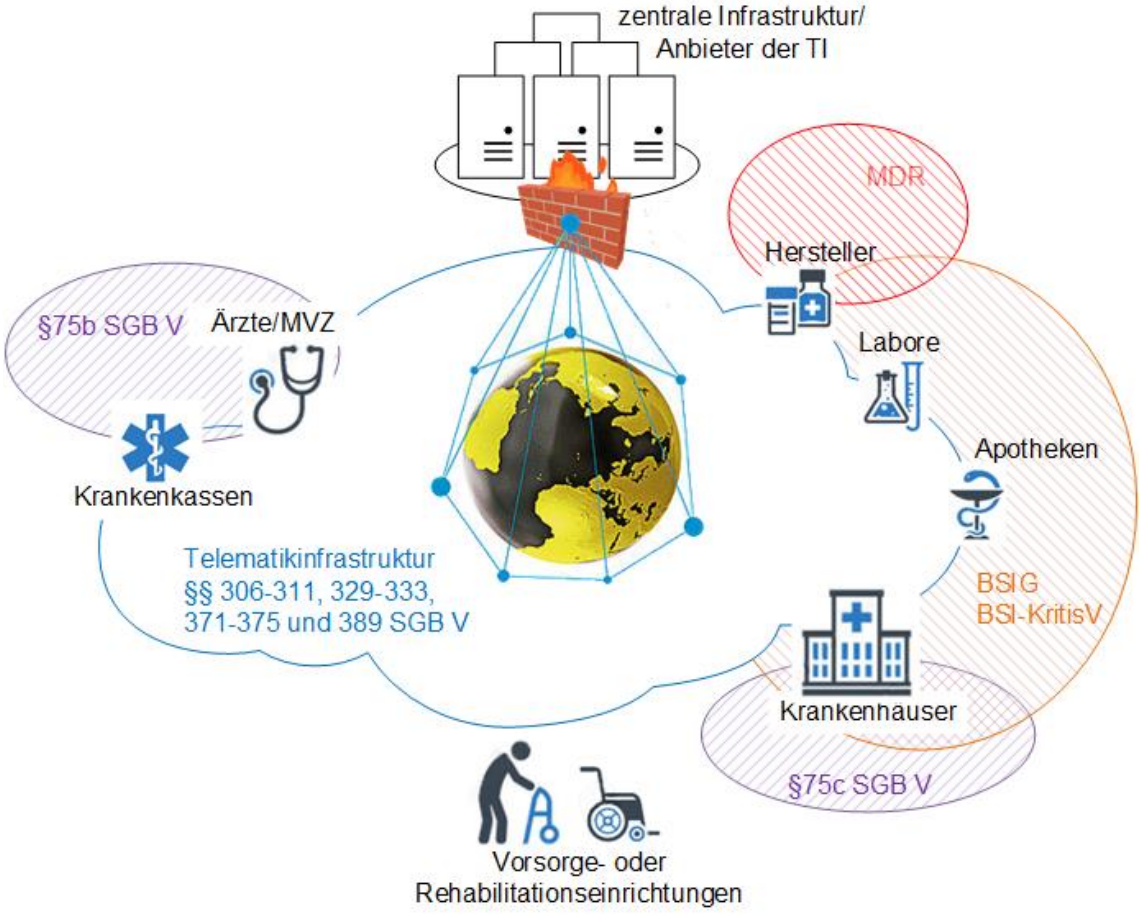


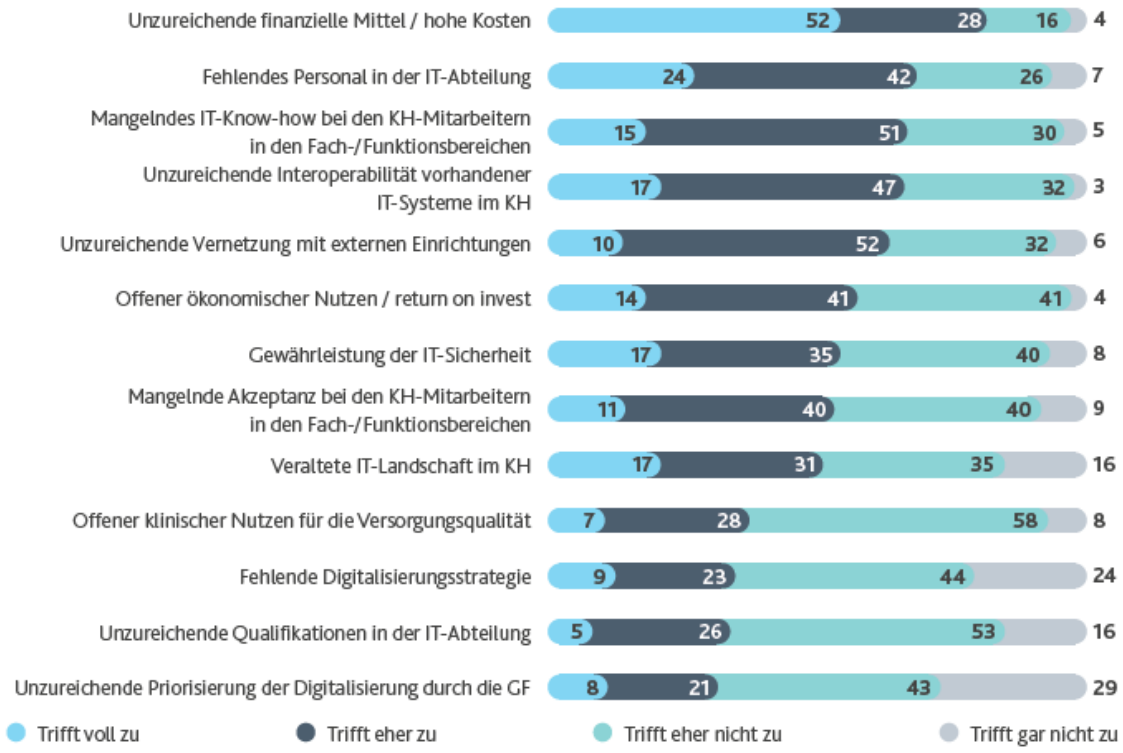
Abbildung 16: Gesetzesgrundlagen IT-Sicherheit im Gesundheitswesen

Die Wirkung der jeweiligen gesetzlichen Regelungen auf die Akteure des Gesundheitswesens kann der Anlage E entnommen werden.

4.8.2 Abhängigkeit der IT-Sicherheit von Förderprogrammen

Die fehlende finanzielle Ausstattung der Akteure im Gesundheitswesen durch Berücksichtigung in leistungsabhängigen kontinuierlichen Zuwendungen, wie z.B. der Fallpauschale oder über Umlage auf Arzneimittel, erschwert das notwendige Aufrechterhalten der Technik auf dem Stand der Technik, sowie eine sichere Betriebsführung erheblich. Projekt zur Erneuerung der Infrastruktur und der Sicherheitskomponenten bedürfen als Voraussetzung zur Förderung eines Ausschreibungsverfahrens. Dies bindet auf der einen Seite finanzielle Mittel für die Planung und Begleitung des Verfahrens durch einen externen „Fachplaner“ und Ausschreibungsstelle und auf der anderen Seite auch Ressourcen bei den Firmen, welche sich an der Ausschreibung beteiligen. Auf Grund fehlenden Fachwissens auf Seiten der ausschreibenden Stelle kommt in den meisten Fällen als einziges Bewertungskriterium der Projektpreis zum Tragen, da eine fachliche In-

Kontextsetzung des Angebotspreises mit der angebotenen Leistung durch die Vergabestelle nicht möglich ist. Hierdurch wird nicht die wirtschaftlichste und den Anforderungen am besten gerecht werdende Lösung realisiert.
Auch die personelle Ausstattung der Leistungserbringer im Gesundheitssektor mit eigener IT-Abteilung würde von einem höheren IT-Budget profitieren. Stand heute wissen die wenigsten Häuser, wie der Betrieb der im Rahmen des KHZG eingeführten neuen Lösungen finanziell und personell abgesichert werden kann. Aktuelle Studien seit der Verabschiedung des KHZG gibt es hierzu allerdings noch nicht, jedoch haben die seitdem getroffenen Entscheidungen und Beschlüsse an der zuvor dargestellten Situation nichts geändert, so dass davon ausgegangen werden kann, dass die Aussagen der 2019 veröffentlichte Studie „Das digitale Krankenhaus“ nach wie vor Bestand haben. Wie aus der nachfolgenden Darstellung entnommen werden kann, sind unzureichende finanzielle Mittel und fehlendes IT-Personal die beiden an den häufigsten genannten Herausforderungen bei der Digitalisierung.



Quelle: Jörg Rauschenberger, Dr. Karl Blum, Prof. Dr. Volker Nürnberg, Dr. rer. pol. Matthias Offermanns, 05. November 2019

Abbildung 17: zentrale Probleme Digitalisierung im Krankenhaus in %

Unabhängig davon, dass eine Änderung der Finanzierung des Gesundheitssystems unumgänglich erscheint, müssen die verfügbaren Mittel effektiv eingesetzt werden. Bestandteil der Überlegungen muss die Rolle der Informationstechnologie, deren Bedeutung für die Gesundheitsversorgung und deren nachhaltige finanzielle Ausstattung sein.

Fehlende Mittel dürfen aber nicht die Basis für eine grundsätzliche Absenkung des notwendigen Sicherheitsniveaus sein. Die Patientensicherheit muss vor Wirtschaftlichkeitsbetrachtungen bei der Betrachtung von Sicherheitsmaßnahmen gehen. Kompromisse, aus welchen Gesichtspunkten heraus diese auch immer getroffen werden, reduzieren das geplante und notwendige Sicherheitsniveau und sollten daher vermieden werden. Dies kann insbesondere dadurch erreicht werden, dass der zu betrachtende Informationsverbund, der Schutzbedarf und die umzusetzenden Maßnahmen für vergleichbare Strukturen einheitlich und zentral festgelegt werden. Neben einem einheitlichen hohen Schutzniveau kann mit diesem Vorgehen auch dem Ressourcenmangel begegnet werden. Hierzu müssen sich die Akteure einvernehmlich in Bezug auf die zu definierenden Sicherheitsmaßnahmen einigen.

5 Sicherheitslage der Kliniken

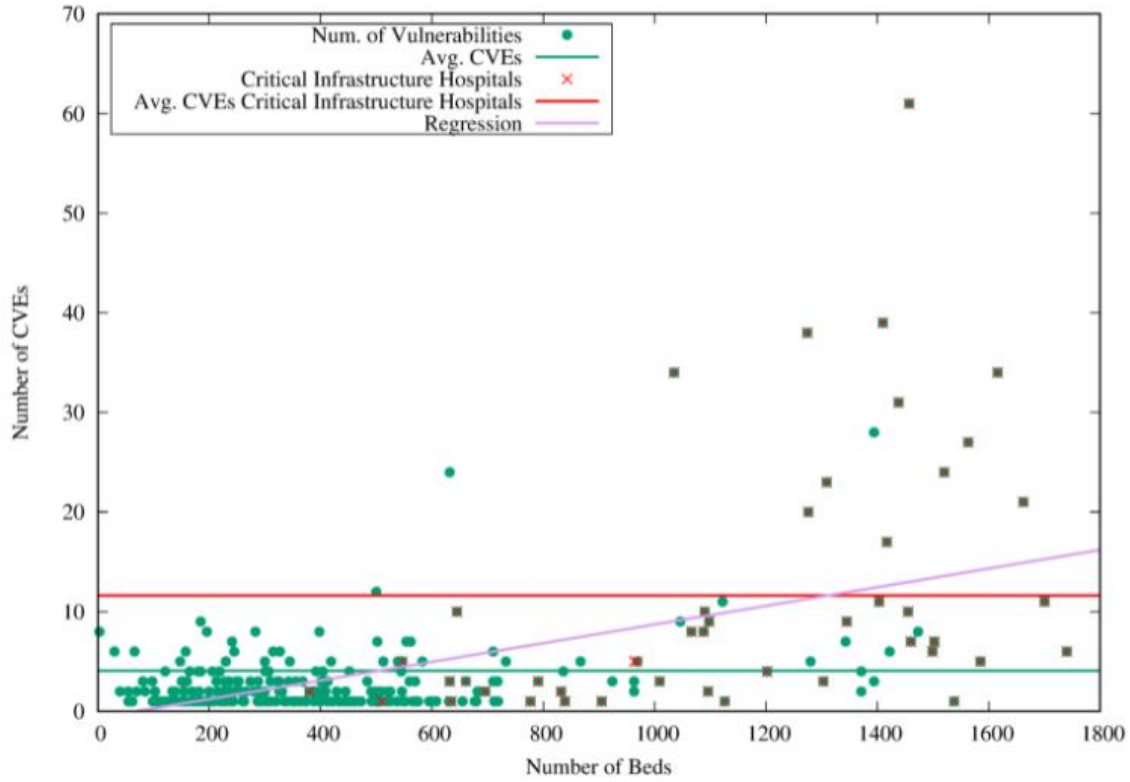
5.1 Allgemeine Einschätzung

Insgesamt ist eine wachsende Bedrohungslage für IT-Infrastrukturen zu beobachten. Klinische Infrastrukturen bilden hierbei keine Ausnahme. Ziel der Angreifer ist die Erbeutung von Daten und/oder die Verfügbarkeit dieser bzw. der jeweiligen Infrastruktur. Beide Angriffsziele haben das Ziel der Erpressung von Lösegeld. Wie aus einer Untersuchung des Bundesverbandes für Informationswirtschaft, Telekommunikation und neue Medien e.V. hervorgeht, haben Angriffe, die auf das organisierte Verbrechen zurückgeführt werden, seit 2017 um 22% zugenommen.[97] Gleichzeitig nehmen auch die Angriffe auf klinische Infrastrukturen zu. Wie aus den Sicherheitsberichten des BSI für die Jahre 2019[98] und 2020[99] hervorgeht, haben binnen Jahresfrist alleinig für die der BSI-KritisV unterliegenden Einrichtungen die Sicherheitsvorfälle um 87 Vorfälle zugenommen, was einem Anstieg von 185% entspricht. Die Zunahme der Cyber-Attacken auf Krankenhäuser wird durch den Anstieg der Hackerangriffe von 11 Angriffen im Jahr 2018 auf 43 entsprechende Vorfälle im Jahr 2020 bestätigt.[100]

Diese wachsende Anzahl an Angriffen trifft auf nicht hinreichend abgesicherte Infrastrukturen und zunehmende Sicherheitsrisiken bei Medizinprodukten. So zeigt das BSI-Projekt MainMed zur Untersuchung der Manipulation von Medizinprodukten 150 IT-Schwachstellen auf.[101] Auch wenn der Großteil der identifizierten IT-Schwachstellen nicht direkt den Produkten selbst, sondern den Infrastrukturkomponenten zugeschrieben werden, ist dies nicht minder besorgniserregend. Hinweise auf fehlendes Sicherheitsbewusstsein liefert auch der durchgeführte Scann auf öffentlich zugängliche Informationssysteme von 1.555 Krankenhäusern. Dieser deckte 1.882 Schwachstellen auf, wobei mit 931 Schwachstellen knapp die Hälfte mit einem Score zwischen 9,0 und 10 des Common Vulnerability

97 Vgl. Bitkom e.V. (05. August 2021).
98 Vgl. Bundesamt für Sicherheit in der Informationstechnik (Oktober 2019).
99 Vgl. Bundesamt für Sicherheit in der Informationstechnik (September 2020).
100 Vgl. Dr. Timo Braun, Patrick Winter (08. Dezember 2020).
101 Vgl. Bundesamt für Sicherheit in der Informationstechnik (11. 12. 2020).

Scoring Systems als besonders kritisch einzustufend sind. Ein weiteres besorgniserregendes Ergebnis der noch in Revision befindlichen Studie, ist der Umstand, dass mit zunehmender Bedeutung der Einrichtung für die Versorgung der Bevölkerung und damit als kritische Infrastruktur eingestuft sind, auch die Anzahl der identifizierten Schwachstellen wächst und damit die Wahrscheinlichkeit eines Angriffs zunimmt. Dieses Ergebnis kann der nachfolgenden graphischen Auswertung entnommen werden.



Quelle: Klick/Koch/Brandstetter, 20.01.2021

Abbildung 18: Anzahl der Schwachstellen in Krankenhäusern in Bezug auf die Anzahl der Betten

Eine Ursache hierfür könnte im höheren Digitalisierungsgrad dieser Einrichtungen gegenüber kleineren Häusern und der nicht im gleichen Maße gewachsenen bzw. berücksichtigten Absicherung dieser zusätzlichen Anwendungen durch entsprechende IT-Security Maßnahmen zu suchen sein.

5.2 Stand Umsetzung gesetzlicher Vorgaben

Wie bereits im Kapitel 4.6 dargelegt, sollten allen Krankenhäusern bis Ende 2021 ein Informationssicherheitsmanagementsystem eingeführt haben und auf Basis dessen entsprechend notwendige Maßnahmen zur Stärkung der IT-Sicherheit identifiziert und dessen Umsetzung geplant haben.

Auf Grund der allgemeinen Einschätzung und der am Markt verfügbaren Ressourcen sowie der finanziellen Rahmenbedingungen kann davon ausgegangen werden, dass ein nicht unerheblicher Anteil der Häuser kein ISMS eingeführt haben wird und auch notwendige technische organisatorische Maßnahmen nicht umgesetzt sein werden und sich damit die Sicherheitslage durch die wachsende Bedrohungslage weiter verschlechtern wird. Aktuelle Studien hierzu liegen derzeit noch nicht vor.
Dahingegen wird die Umsetzung der Anbindung an die TI weitestgehend abgeschlossen sein, was allerdings eher als Unsicherheitsfaktor in Bezug auf die (IT-)Sicherheit angesehen werden kann, da zusätzliche Gefährdungen bei gleichzeitig hinterherhinkender Cyber-Security-Strategie geschaffen werden.

5.3 Auswirkungen aus Erhöhung des Digitalisierungsgrades

Ohne die Verbesserung der Sicherheitsprozesse und -maßnahmen ist eine Erhöhung des Digitalisierungsgrades nur unter Inkaufnahme von größeren Risiken möglich. Die Akzeptanz/Übernahme von Sicherheitsrisiken zu Gunsten der Digitalisierung ist aber nicht vor- und darstellbar. Daher kann dies nur in abgestimmten Schritten erfolgen. Eine dafür notwendige Koordination der Akteure scheint aber nicht gegeben zu sein. So bestehen zur Umsetzung des e-Rezeptes unterschiedliche Vorstellung bei der gematik GmbH und GKV-Spitzenverband, welche zur Rücknahme der Beantragung der eGK mit NFC-Funktion über die App durch die gematik GmbH führte.[102] Wie bereits im Kapitel 3.2 Status der Digitalisierung im Gesundheitswesen dargelegt, können bereits wenige Sicherheitsvorfälle das Vertrauen in die Digitalisierung nachhaltig schaden und eine Umsetzung weiter verzögern.

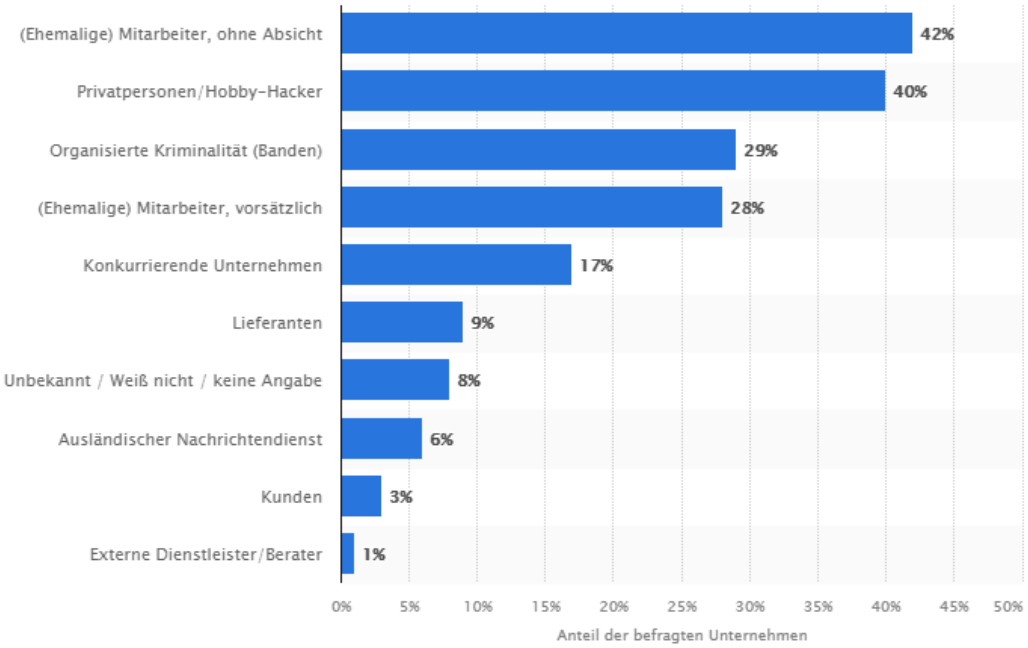
102 Vgl. Adhoc (22.08.2021).

6 Risikobetrachtung für klinische Infrastrukturen

6.1 Bedrohungen und Gefährdungen

6.1.1 Motivation für potentielle Angriffe

Für Angriffe als vorsätzliche Handlung bedarf es eines Motivs, sofern dieser nicht aus reiner Zerstörungswut heraus in Form von Vandalismus erfolgt. Daher und um mögliche Angreifer und deren Fähigkeiten besser einschätzen zu können, muss analysiert werden, wer Interesse an Angriffen auf klinische Infrastrukturen haben könnte. Eine statistische Erhebung zu den Motiven von Cyber-Attacken im Bereich des Gesundheitswesens gibt es derzeit nicht. Aus den bekannt gewordenen Angriffen lässt sich allerdings ableiten, dass die Angreifer in den meisten Fällen finanziellen Nutzen daraus ziehen wollen. Motive wie die Durchsetzung von politischen Zielen oder persönlicher Interessen spielen eher eine untergeordnete Rolle, dürfen aber keinesfalls aus diesem Grund unterschätzt und ausgeschlossen werden, da aus diesen Gründen motivierte Angriffe häufig durch Innentäter durchgeführt werden.



Quelle: J. Bolkart, 09.08.2021

Abbildung 19: Täterkreis von Cyber-Attacken im Jahr 2021

Deren Fähigkeiten und Mittel, wie auch der von Script-Kiddies, können im Gegensatz zum organisierten Verbrechen allerdings als gering bis mittel eingeschätzt werden. Ein alleiniger, direkter Rückschluss auf das von Mitarbeitern ausgehende Sicherheitsrisiko lässt sich daraus nicht ableiten, da hier auch unbeabsichtigte Handlungen/Vorfälle eingehen. Daher ist es nicht verwunderlich, dass knapp ein Drittel der befragten 150 IT-Entscheider im Gesundheitswesen als höchstes Sicherheitsrisiko die Mitarbeiter angeben und diesen fehlendes Cybersicherheitsbewusstsein attestieren.[103] Gerade in Hinblick auf die fortschreitende Digitalisierung muss diese entsprechend bewertet und entsprechende Maßnahmen in Form von Mitarbeiterschulungen für Security Awareness eingeführt und fortlaufend weiterentwickelt werden. Das gewünschte Verhalten der Mitarbeiter kann durch Umsetzung von unterstützenden Maßnahmen, wie z.B. der einfachen Möglichkeit zur Meldung von Phishing Versuchen und das Vorleben einer gewünschten Feedback Kultur, gefördert werden.

6.1.2 Neue Gefährdungen im Rahmen der Digitalisierung

Der IT-Grundschutz unterteilt mögliche Gefährdungen in fünf Klassen

- **Höhere Gewalt** - wie Personalausfall, Unwetter, Ausfall von Lieferanten, technische Katastrophen
- **organisatorische Mängel** - wie mangelhafte Kontrollen, unzureichende Dokumentation, Fehlen von Regelungen
- **menschliche Fehlhandlungen** - wie Fehlbedienungen, Fehlverhalten
- **technisches Versagen** - wie Ausfall von IT-Systemen, Stromausfall
- **vorsätzliche Handlungen** - wie Missbrauch, Vandalismus, Diebstahl

Durch die Erhöhung des Digitalisierungsgrades ergeben sich an sich keine neuen grundlegenden Gefährdungen, jedoch verändert sich die Bedrohungslage durch zusätzliche Schnittstellen und Systeme. Diese werden in Bezug auf Gefährdungskategorien nachfolgend bewertet.

6.1.2.1 Höhere Gewalt

Bei der Abhängigkeit von externen Dienstleistern ist von einer deutlichen Zunahme auszugehen. Gerade in Bezug auf die TI muss davon ausgegangen werden, dass ein Dienstleisterausfall großen Einfluss haben wird, da viele bis alle Teilnehmer der Telematikinfrastruktur betroffen sein können. Dem Ausfall von Dienstleistern soll mit entsprechenden Zertifizierungen entgegengewirkt werden.

103 Vgl. Kaspersky (14. Juli 2021).

Eine Feststellung der technischen und qualifizierten Leistungsfähigkeit eines Anbieters stellt aber dessen Verfügbarkeit nicht alleinig sicher. Auch wirtschaftliche Aspekte müssten in die Überprüfung einbezogen werden sowie deren Übernahme durch ausländische Konzerne untersagt werden können. Ein entsprechendes Vetorecht nach §56 Außenwirtschaftsverordnung wurde unter anderem mit der Aufnahme des §55a zum 01. Mai 2021 in diese Verordnung für die Betreiber von kritischen Infrastrukturen und Hersteller von kritischen Komponenten gemäß §2 Absatz 13 BSI-Gesetz aufgenommen.

6.1.2.2 Organisatorische Mängel

Durch Digitalisierung können sich nachfolgend aufgeführte Gefährdungen ergeben bzw. verstärkend zu den bereits im jeweiligen Bereich bestehenden Mängeln auswirken.

- fehlendes Notfallmanagement und -pläne
- unzureichende Dokumentation der digitalen Prozesse
- nicht eindeutige Klassifizierung und datenschutzkonforme Speicherung von erfassten Daten
- ungenaue Spezifizierung von Zugriffsberechtigungen
- unklare Verantwortungsverteilung

Digitale Systeme sind von vielen Komponenten, wie Energieversorgung und Netzwerke, abhängig. Im Rahmen der Erstellung von Notfallplänen für entsprechende Anwendungen werden die Notfallpläne für diese Komponenten nicht entsprechend auf die Anforderungen, die sich aus der Verfügbarkeit der digitalen Systeme ergeben, angepasst. Auch werden die Abhängigkeit und akzeptable Ausfalldauer unterschätzt. Ein weiterer Aspekt für die unterbewerte Toleranz zur Wiederherstellung sind falsche Annahmen für die Wiederherstellungszeit für entsprechende Systeme. Dies liegt unter anderem auch an der unzureichenden Dokumentation von digitalen Prozessen. In der Medizintechnik bestehen zwar umfangreiche Dokumentationsanforderungen, welche sich aber im Allgemeinen auf die jeweiligen Produkte bzw. einzelnen Lösungen, nicht aber auf den gesamten Prozess beziehen. Dies trifft gewöhnlich dann zu, wenn mehrere Dienstleister einzelne Komponenten bereitstellen, eine Gesamtverantwortung und -koordination aber nicht sichergestellt ist und auch der Betriebsprozess nicht durchgehend übergreifend geregelt ist. Bestehende Qualitätsmanagementprozesse wiederum erfassen die notwendigen technischen Parameter nicht hinreichend. Diese unklare Verantwortungsverteilung kann zu offenen, nicht gesicherten Schnittstellen und fehlender prozessualen Absicherung führen.

Patientendaten als besonders schützenswerte Personendaten dürfen dazu nur autorisierten Personen zugänglich gemacht werden und müssen fälschungssicher gespeichert werden. Damit dies in digitalen Prozessen gewährleistet werden kann, muss bei der Datenerfassung eine entsprechende Klassifizierung erfolgen. Über ein Rechtemanagement ist der datenschutzkonforme Zugriff auf diese Daten sicherzustellen. Dies gilt auch bei Weitergabe der Daten für Forschungszwecke.

6.1.2.3 Menschliche Fehlhandlungen

Gefahren aus menschlichen Fehlhandlungen oder auch Fehlbedienung ergeben sich im Zuge von zunehmender Digitalisierung aus mehreren Gründen. Mit wachsendender Komplexität sind Abhängigkeiten nicht mehr für jeden Einzelnen direkt erkennbar und können auch erst in Abfolge von verschiedenen Prozessen zu einer ungewünschten Reaktion bei fehlerhafter Bedienung/Eingabe führen. Bei Lieferkettenangriffen können Angreifer den Zugang zu Systemen bei Firmen/Instituten erlangen, welche an sich keine direkten Angriffspunkte geboten haben. Ein Beispiel für einen entsprechenden Angriff aus der jüngsten Vergangenheit ist der Angriff über den IT-Dienstleister Kaseya[104]. Auch wenn der Angriffsvektor der Ausnutzung eines Zero Day Exploits mehr in die Gefährdungskategorie des technischen Versagens eingeordnet werden kann, so verdeutlicht er doch die Auswirkungen von automatisierten digitalen Prozessen mit Maschine-zu-Maschine-Kommunikation, wo Systeme sich gegenseitig vertrauen.
Eine andere Art von Fehlhandlungen sind durch Social-Enginiering-Angriffe veranlasste Aktionen, indem z.B. Aktionen durch Vortäuschen falscher Tatsachen ausgelöst werden. Angriffswerkzeuge hierfür können sein

- **Spyware** – wird verwendet, um Informationen über einen Nutzer durch den Einsatz von Systemmonitor, Trojaner, Adware, Tracking-Cookies und Keylogger zu sammeln und die Informationen ohne Zustimmung des Nutzers an eine andere Entität zu senden.
- **Scareware** – umfasst Betrugssoftware, die mithilfe von Social Engineering schockiert oder Angst einflößt, indem sie die Wahrnehmung einer Bedrohung erweckt. Im Allgemeinen an einen ahnungslosen Benutzer gerichtet und versucht, den Benutzer davon zu überzeugen, einen Computer zu infizieren, indem Maßnahmen ergriffen werden, um die gefälschte Bedrohung zu bekämpfen.

104 Vgl. Schmidt (06.07.2021).

- **Phishing** – Versuch, Personen davon zu überzeugen, sensible Informationen preiszugeben. Beispiele hierfür sind der Erhalt einer E-Mail von vermeintlichen Empfängern oder auch Telefonanrufe, in der Benutzer aufgefordert werden, ihre Informationen preiszugeben oder auch unbemerkt Download von Schadsoftware zu veranlassen.
- **Spear Phishing** – hier handelt es sich von einer besonderen Art von Phishing-Angriffen, da diese sehr qualifiziert vortäuschen, von einer vertrauenswürdigen Quelle zu stammen und gezielt einzelne Personen oder einen kleinen Personenkreis ansprechen, um bestimmte Informationen zu erlangen

Eine weitere beachtliche Gefährdung geht von der „Digitalen Demenz“ aus, indem durch die intensive Nutzung von Digitalisierung eine Abhängigkeit von diesen digitalen Systemen entsteht und dadurch eine Kontrolle dieser Systeme und deren Ergebnisse nur unzureichend erfolgen kann sowie deren Ausfall durch manuelle Handlungen nicht mehr kompensiert werden kann. Der Neurowissenschaftler Manfred Spitzer, der Studien zu den Auswirkungen der digitalen Welt auf die Gehirnfunktionen betreibt und den Begriff der „Digitalen Demenz“ in diese Richtung maßgeblich geprägt hat, sieht eine systematische Verdummung der nächste Generationen bis hin zur Schädigung des Gehirns durch die fortschreitende Digitalisierung.[105] Diese Annahme wird zwar kontrovers diskutiert und andere Forscher sehen keine Anhaltspunkte für Gehirnschädigungen durch die Nutzung von digitalen Medien[106], jedoch ist eine Zunahme des „blinden Vertrauens“ in Maschinen und künstlicher Intelligenz, wird auch als „Overtrust“ bezeichnet, nicht von der Hand zu weisen und endet, wie z.B. Unfälle mit autonom fahrenden Autos zeigen, in extremen Fällen auch tödlich.[107]

Neben den zuvor aufgezeigten Gefährdungen durch menschliches Versagen gilt es vor allem, die Systeme vor unbewusster Fehlbedienung und Falscheingabe zu schützen. Menschen neigen dazu, Dinge auszuprobieren, anstatt im Vorhinein sich der genauen Funktionsweise und Bedienung zu vergegenwärtigen bzw. zu erlernen. Dabei muss auch ein besonderes Augenmerk auf die ältere Generation und nicht-technikaffine Personen gelegt werden, um diese an der Digitalisierung teilhaben zu lassen, ohne dass eine Gefährdung für die Funktion des Gesamtsystems und deren Nutzer entsteht.

105 Vgl. Wohlhüter (21.01.2017).
106 Vgl. Lossau (02.01.2013).
107 Vgl. Dr. Holger Schmidt (2016).

6.1.2.4 Technisches Versagen

Gefährdungen durch technisches Versagen von Systemen werden durch die Zunahme von Schnittstellen und der Anzahl der Systeme selbst erhöht bzw. neu geschaffen. Ein Beispiel für neuen externen Schnittstellen stellen die Patientenportale, über welche Patienten nicht nur Informationen abrufen können, sondern auch bereits im Vorfeld von geplanten Krankenhausaufenthalten Informationen, z.B. über die elektronische Patientenakte, zur Verfügung stellen können, umso den Prozess der Aufnahme im Krankenhaus zu entlasten, dar. Hierdurch erfolgt ein Datenaustausch mit dem Krankenhausinformationssystem, dem Herz eines jeden Krankenhauses. Ohne ein entsprechend verfügbares KIS ist ein effektiver Krankenhausbetrieb nicht durchführbar und beeinträchtigt den Betrieb auf nicht unerhebliche Weise, wie das Beispiel des Ransomware-Angriffs auf das Lukaskrankenhaus in Neuss im Jahr 2016 zeigt.

Weitere Gefährdungen ergeben sich durch nicht gemanagte Geräte, die mit der zu schützenden Infrastruktur z.B. über Gesundheits-Apps und Wearables interagieren. Wird bei der Entwicklung und Pflege der Software die Sicherheit nur ungenügend Aufmerksamkeit gewidmet, entstehen schnell Sicherheitsrisiken. Dies zeigt auch die für die Nachverfolgung von Covid-19-Infektionsketten entwickelte Luca-Software. So war es dem Sicherheitsforscher Markus Mengs gelungen, mittels Code Injection Schadcode zu übertragen, mit dem er in der Lage gewesen wäre, Personendaten abzugreifen und die Infrastruktur der Behörden nachträglich durch Verschlüsselung lahmzulegen.[108]

Eine große Herausforderung bei der Umsetzung und Bereitstellung von digitalen Anwendungen für eine breite Bevölkerungsschicht stellt die Einbindung der Endgeräte der Systeme dar, da der Spagat zwischen einer großen Verbreitung/Nutzung der Anwendungen einerseits und die Einbindung unterschiedlichster Geräte mit den verschiedensten technischen Voraussetzungen anderseits gelingen muss. Dabei stellen besonders Geräte mit veralteten, nicht mehr unterstützten Betriebssystem eine Gefahr dar. So unterstützen viele Apps sogar noch die Android KitKat 4.4, obwohl Google hierfür das letzte Update am 19.06.2014 bereitgestellt hatte.[109] Diese unterschiedlichen Patch Level und Softwarestände stellen Gefährdungen durch nicht behobene Fehler im Programmcode dar und eröffnen damit entsprechende Angriffsvektoren. Inwieweit die Endgeräte mit den letzten aktuellen Softwareständen betrieben werden, ist für die Anbieter der digitalen Dienste nicht vorhersehbar und beeinflussbar. Eine Überwachung und das Managen der genutzten mobilen Endgeräte, wie es bei Mitarbeitern üblich sein sollte, ist nicht durchsetzbar. Zur Risikominimierung ist daher ein Mitwirken und

108 Vgl. Reuter (26.05.2021).
109 Vgl. Tim Aschermann (11.12.2020).

eine entsprechende Security Awareness des Nutzers erforderlich. Aber auch Design Fehler in Chip-Hardware können durch Angreifer ausgenutzt werden, wobei die Wahrscheinlichkeit der Ausnutzung mit fortschreitender Verbreitung und Verfügbarkeit steigt und bei Risikoeintritt möglichweise nur durch softwareseitige Sperrung der betroffenen Hardware begegnet werden könnte, was bei den Anwendern zur Unzufriedenheit führen kann. Hierdurch besteht die Gefahr der Entstehung von neuen Bedrohungen für den Betreiber und den Anbieter, welche in die Risikobetrachtung bei Ermittlung und Bewertung der Auswirkungen mit einbezogen werden sollten.

6.1.2.5 Vorsätzliche Handlungen

Der Schutz von Systemen vor vorsätzlicher Handlung aus den unterschiedlichsten Bewegründen heraus kommt in dem Sinne eine große Bedeutung zu, da in diesen Fällen von einer hohen Kriminalität ausgegangen werden muss, welche das Ziel einer wirtschaftlichen Schädigung und/oder die Gefährdung der Gesundheit von Menschen verfolgt. Dabei muss ausdrücklich oberste Priorität der Schutz der Personen gelten. Durch die Digitalisierung besteht die Möglichkeit, Angriffe anonym aus großer schutzbietender Entfernung durchzuführen. Der Zeitfaktor spielt speziell bei der Vorbereitung eine untergeordnete Rolle. Auch die Mittel und Wissen für gezielte Angriffe sind nicht mehr zwingende Voraussetzung. Angriffswerkzeuge, wie Botnetze oder Ransomware, können heute im Darknet angemietet und/oder gekauft werden. In der nachfolgenden Übersicht aus dem Bundeslagebild | Cybercrime 2020 des Bundeskriminalamtes sind einige ausgewählte dargestellt.

Service	**Preis in US $** (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ Desktop-Version	1.000 - 10.000 $	bei Kauf
▪ Mobile-Version	1.000 - 10.000 $	bei Kauf
RAT (Remote Administration Tool)	89 - 530 $	pro Monat bei Miete
	Ca. 3.000 $	bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	20 - 100 $	bei Kauf von einem Crypt
	360 - 500 $	bei einem Wochen-Abo mit 50 Crypts pro Tag
Spam	10 ct - 4 $	pro Spam
DDoS as a Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ Shared	5 - 50 $	pro Monat bei Miete
▪ Dedicated	50 - 700 $	pro Monat bei Miete

Quelle: Bundeskriminalamt, April 2021

Tabelle 3: Übersicht krimineller Services im Darknet

Die Aufklärungsquote für erfasste Cybercrime-Fälle in Deutschland lag im Jahr 2020 bei ca. ein Drittel der Fälle und damit um knapp 7% niedriger als noch in 2016. Hierbei hat sich allerdings die absolute Zahl der aufgeklärten Fälle erhöht. Diese Zahlen zeigen zum einen den starken Anstieg der Vorfälle insgesamt bei einer um 25% geringeren Aufklärungsquote gegenüber der durchschnittlichen Quote.

6.2 Kritikalität von klinischen Systemen in Bezug auf die Aufgabenerfüllung

Zur Erbringung der kDL bedarf es des Einsatzes von spezifischen medizintechnischen und organisatorischen Systemen/Anwendungen. Ziel der Digitalisierung ist eine technische und prozessuale Vernetzung der Systeme zur Verbesserung und Optimierung der kritischen Dienstleistungen. Zur Risikoeinstufung eines jeden der Systeme in Bezug zur Aufgabenerfüllung zur Erbringung der kDL ist deren Wichtigkeit in jedem Teilprozess zu evaluieren. Aus den einzelnen Risiken ergibt sich das Gesamtrisiko, woraus sich im Umkehrschluss die Bedeutung ableiten lässt. Zur Risikoreduzierung sind Netzwerke in dedizierte Zonen aufgeteilt und waren bzw. sind in den überwiegenden Fällen völlig separiert als Insellösungen aufgebaut.

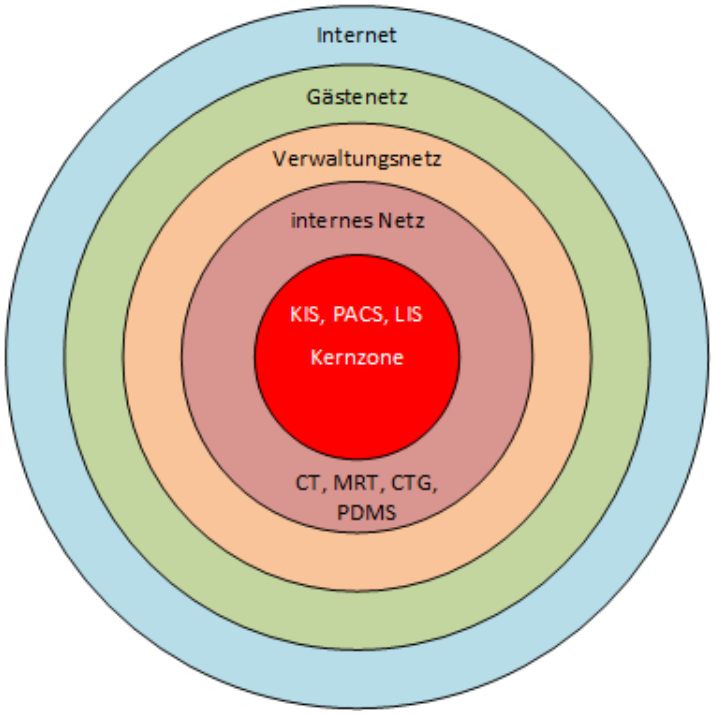


Abbildung 20: Zonen-Konzept klinischer Infrastrukturen[110]

110 Vgl. eigene Darstellung in Anlehnung Michael Thoss (30. Mai 2020).

Mit der Vernetzung der Systeme zur Digitalisierung der Prozesse, was durch die Einführung von Picture Archiving and Communication Systems zur fachbereichsübergreifenden Verteilung von Bildmaterialen begonnen hat, ist eine Aufrechterhaltung dieser üblichen Praxis nicht mehr länger möglich. Dadurch werden Übergänge zwischen Zonen mit unterschiedlichem Schutzniveau geschaffen, was zu einer entsprechenden Risikoerhöhung führt. Dieses Risiko steigt mit zunehmender Distanz der Netze. Die Kritikalität eines Systems lässt sich auf dieser Basis nicht mehr alleinig nach dessen tolerierbaren Ausfallzeit, welche die Bedeutung der Anwendung für die Erfüllung der kDL zum Ausdruck bringt, bemessen. Neben der Klassifizierung der Systeme nach den drei Klassen des B3S für den Gesundheitssektor bedarf es daher der zusätzlichen Bewertung nach deren Kritikalität für den Prozess auf Grundlage von Ausfallwahrscheinlichkeit und Schadensausmaß in Bezug auf die Schutzziele. Die Norm DIN EN 80001-1 gewinnt daher zunehmend an Bedeutung bei der Risikobewertung von klinischen Infrastrukturen. Eine entsprechende Risikobetrachtung ist daher nicht nur für unmittelbare Anwendungen innerhalb des medizinischen Netzwerkes erforderlich, sondern grundsätzlich bei Einbindung in die klinische Infrastruktur, da davon ausgegangen werden muss, dass über jegliche Netzwerkkomponente ein Zugriff ermöglicht werden kann. Bei Betrachtung des Gesamtprozesses sind daher auch Anwendungen außerhalb von klinischen Infrastrukturen einzubeziehen. Dies betrifft beispielsweise Anwendungen wie

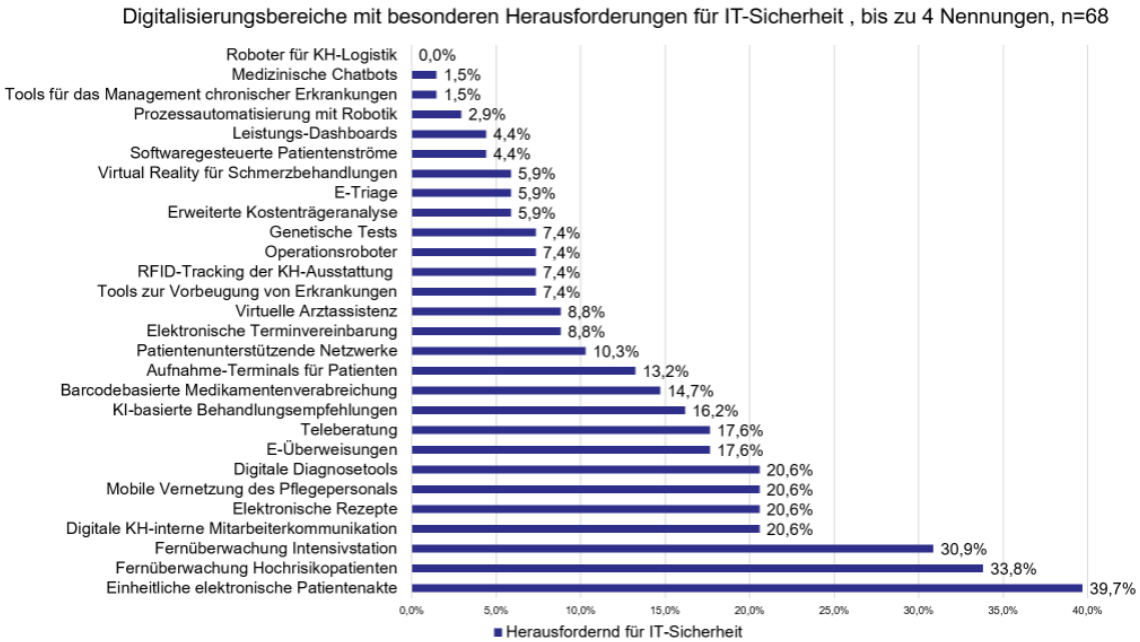
- Praxisverwaltungssoftware
- Zahnarztpraxisverwaltungssystem
- Apothekensoftware
- Versichertenstammdatenmanagementsystem

die über die TI mit den klinischen Anwendungen vernetzt sind und im Datenaustausch stehen. Wenn in Bezug auf die Aufgabenerfüllung von kDL deren Kritikalität als gering angesehen werden kann, so sollte diese aber nicht vernachlässigt werden, da ein mögliches Schadensausmaß nicht unerheblich ist. Neben den externen Anwendungen können auch die Patienten- und Gastanwendungen, deren Ausfall längerfristig kompensiert werden kann, der niedrigsten der drei Risikoklasse zu zuordnet werden.
Ausfälle von Systemen der Primär- und Sekundäranwendungen dahingegen können nur mittelfristig bis kurzzeitig aufgefangen werden. Ebenso ist von einem hohen bis sehr großen Schadensausmaß auf die Patientensicherheit bei Einschränkung der Verfügbarkeit, Verlust der Integrität und Vertraulichkeit auszugehen. Das KIS kann dabei als eine der kritischsten Anwendung in klinischen Infrastruk-

turen betrachtet werden. Als zentrale Informationsdrehscheibe, wo alle Patientendaten in der Patientenfallakte dokumentiert werden, hat es direkte Kommunikationsbeziehung zu allen anderen Primäranwendungen wie:

- Laborinformationssystem
- Radiologieinformationssystem
- Picture Archive and Communication System
- Dokumenten-Management-System

Neben der internen Kommunikation erfolgt über die TI ein Datenaustausch mit weiteren Systemen. Unter anderem werden hieraus auch die Daten zur Befüllung der ePA bereitgestellt. Seitens der Hersteller gibt es Bestrebungen, diese ohnehin vielfältigen Beziehungen durch Implementierung von Patientenportale noch zu erweitern. Dabei werden neue Angriffsvektoren auf diese sehr kritische Anwendung durch Implementierung eines direkten Internetzugangs aus nicht vertrauenswürdigen Quellen, wie es bei Remotezugängen von Dienstleistern der Fall ist, hinzugefügt. Damit wird die maximale Distanz zwischen den Zonen erreicht und stellt damit das größtmögliche Risikopotential für die klinische Infrastruktur dar. Diese Auffassung scheinen auch die Verantwortlichen der bayrischen Krankenhäuser zu teilen, welche in der einheitlichen elektronischen Patientenakte die größte Herausforderung für die IT-Sicherheit in den nächsten 10 Jahren sehen.

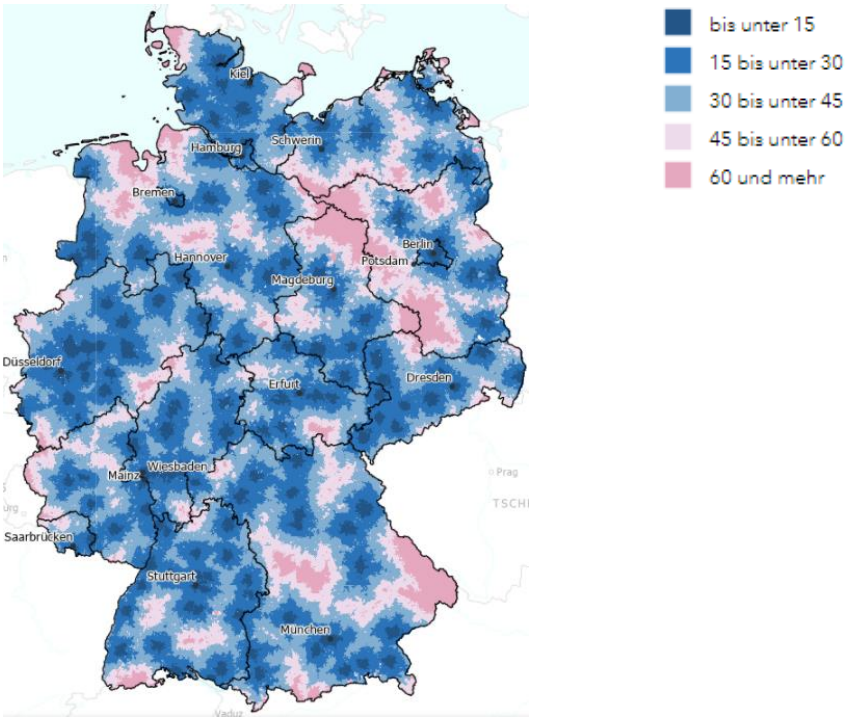


Quelle: Universität der Bundeswehr München, Juni 2019

Abbildung 21: IT-sicherheitskritische Digitalisierungsthemen

6.3 Auswirkung auf Versorgungssicherheit bei Ausfällen von klinischen Infrastrukturen

Wie bereits unter Punkt 4.3.5 aufgeführt, sollte der Standortfaktor eine wichtige Rolle innerhalb der Risikobewertung spielen, da die Auswirkung von Krankenhausausfällen auf die medizinische Versorgung der Bevölkerung in Abhängigkeit zum des Krankenhausstandortes stehen. Die Verfügbarkeit von einzelnen Häusern beeinflusst so möglichweise die Hilfsfristen, welche als die Zeit vom Eingang des Notrufs bis zum Eintreffen am Einsatzort definiert ist. Die Fristen werden durch die jeweiligen Bundesländer festgelegt und liegen im Bereich zwischen 10 und 15 Minuten.[111] Auch wenn diese Zeiten durch autarke, nicht in die Krankenhausinfrastruktur eingebundene Einrichtung wie Feuerwachen mit stationierten Rettungswagen zumeist eingehalten werden können, so verlängert sich bei Ausfall eines Krankenhauses der Transport zu einer adäquaten ärztlichen Versorgung. Wie aus der nachfolgenden Darstellung entnommen werden kann, bestanden bereits 2016 erhebliche regionale Unterschiede in der Erreichbarkeit von Krankenhäusern. Seit dieser Zeit wurden allein zwischen 2016 und 2019 37 Krankenhäuser - mit Auswirkungen auf die Versorgungslage - geschlossen.



Quelle: S. Neumeier, 2016

Abbildung 22: Pkw-Fahrzeit zum nächsten Krankenhaus mit Schwerpunkt- und/oder Maximalversorgung in Minuten

111 Vgl. DeWiki (22.08.2021).

Klinikschließungen erfolgen in den meisten Fällen aus Rentabilitätsgründen. Jedoch führen die Schließungen nicht immer zur Reduzierung von Krankenhauskapazitäten, wie das Beispiel der Schließung des Krankenhauses Kloster Lehnin zum Ende des Jahres 2020 zeigt.[112] Der Erhalt der Versorgungskapazität ändert gleichwohl nichts an dem Umstand der Erhöhung der Anfahrtszeit und -wege. Neben diesem Fakt erhöht sich gleichzeitig die Anforderung an die Verfügbarkeit der anderen Krankenhäuser, da deren Kapazitäten durch Aufnahme von Versorgungsleistungen der geschlossenen Einrichtung wachsen und damit der Einfluss auf die regionale Versorgung bei deren Ausfall steigt.

Die unterschiedlichen infrastrukturellen regionalen Gegebenheiten sollen am Beispiel des Flächenlandes Mecklenburg-Vorpommern und Berlin verdeutlicht werden. Kommen in Berlin auf 1.000 Einwohner ca. 5,64 Planbetten, verteilt auf 87 Krankenhäuser,[113] so sind es in Mecklenburg-Vorpommern (MV) sogar 6,2 Betten auf 1.000 Einwohner, was dem Bundesdurchschnitt von 6,04 näherkommt als die Versorgung in Berlin.[114] Aus diesen Zahlen ließe sich schlussfolgern, dass das Risiko bei Ausfall eines Hauses im Land Berlin größer ist als in MV. Auf Grund der Verteilung der Häuser ergibt sich jedoch eine deutlich höhere Abhängigkeit in MV von deren Verfügbarkeit. Liegt die durchschnittliche Erreichbarkeit eines Hauses in MV bei einer Fahrzeit von 14,4 min, so steigt diese bei einer notwendigen Schließung auf Grund eines Sicherheitsvorfalls auf 27 min. In Berlin hingegen kann der Ausfall eines Krankenhauses von der Erreichbarkeit her viel besser kompensiert werden. Die Fahrzeit erhöht sich hier im Durchschnitt um 6 Sekunden von 5,8 auf 5,9 min.[115] Welche Auswirkungen die Verlängerung der Anfahrtszeit auf Grund eines Aufnahmestopps indes auf Notfallpatienten haben kann, zeigt leidvoll der Ransomware-Angriff auf die Uniklinik Düsseldorf, wo der Patient verstarb, weil der Rettungswagen die Klink nicht anfahren konnte und damit adäquate medizinische Hilfe nicht in der dafür erforderlichen Zeit verfügbar war.[116] Noch gravierender als dieses Beispiel auf zeigt, würde sich der Ausfall der Universitätsmedizin Rostock auf die unfallchirurgische Versorgung auswirken, da neben dieser Einrichtung nur noch die Universitätsmedizin Greifswald über entsprechende Versorgungskapazitäten in MV verfügt.[117]

112 Vgl. Ärzte Zeitung (24.11.2020).
113 Vgl. Amt für Statistik Berlin-Brandenburg (2019).
114 Vgl. Ministerium für Wirtschaft, Arbeit und Gesundheit Mecklenburg-Vorpommern (Juni 2021).
115 Vgl. Anhang D - Ergebnisse Datenanalyse zu Auswirkungen von Krankenhausausfällen
116 Vgl. Guntram Doelfs (08.04.2021).
117 Vgl. Datenbasis Statistisches Bundesamt (April 2021) und Versorge- oder Rehabilitationseinrichtungen in Deutschland und der GKV-Kliniksimulator

Gemäß 4.3.1 des Krankenhaus-B3S ist die betrachtete Zeitspanne des Ausfalls von kDL mit zu betrachten. Dies gilt auch für die gesamtheitliche Aufgabenerfüllung, da ein Ausfall immer Auswirkung auf die gesamte klinische Infrastruktur hat. Eine entsprechende Prüfung kann aber nicht im jeweiligen Haus erfolgen, sondern muss auf Landesebene im Rahmen der Krankenhausplanung betrachtet werden. Hier muss in diesem Zusammenhang auch die Einstufung der Kritikalität jeder Einrichtung erfolgen und in Vorgaben bzgl. der sicherheitstechnischen Anforderungen, einschließlich der Bereitstellung der zweckgebundenen finanziellen Mittel, münden.
Gerade die aufkommenden Forderungen zur Reduzierung der Krankenhäuser von derzeit etwas mehr als 1.900 Einrichtung auf eine Zielgröße von 1.200 Häuser, wie Josef Hecken der Vorsitzende des Gemeinsamen Bundesausschusses am 03. Juli 2021 im Interview mit der Frankfurter Allgemeinen Sonntagszeitung erklärte, birgt hier zusätzliche Herausforderungen.
Simulationen zur ausreichenden klinischen Versorgung, wie sie für den Großraum Köln durch das IGES Institut im Auftrag der Bertelsmann Stiftung durchgeführt wurden, berücksichtigen keine Annahmen zur Verfügbarkeit dieser Infrastrukturen.[118] Lediglich in der Zusammenfassung wird darauf abgestellt, dass im Falle von grundsätzlich notwendigen Mindesterreichbarkeiten zusätzliche Maßnahmen getroffen werden müssen.[119] Diese nahezu ausschließlich auf wirtschaftlichen Aspekten getriebene Diskussion zeigt auf, dass das Bewusstsein und Verständnis für notwendige Sicherheitsmaßnahmen im Rahmen der Digitalisierung nur gering ausgeprägt ist. Doch gerade bei der Schaffung neuer digitaler Prozesse müssen Sicherheitsmaßnahmen von Anfang an mitberücksichtigt werden, da eine spätere Integration mit erheblichen Mehrkosten verbunden ist, sofern diese dann überhaupt noch umsetzbar sind.

6.4 IT-Sicherheitsmaßnahmen zur Risikoreduzierung

Risiken kann auf vier verschiedenen Wegen begegnet werden. Im Umfeld des Gesundheitswesens sollte das oberste Ziel der Risikobewältigung die Risikovermeidung sein. Sofern Risiken nicht vermieden werden können, müssen diese Risiken insoweit reduziert werden, dass diese getragen werden können, das heißt die Gefährdung von Menschenleben nahezu ausgeschlossen ist und möglichst keine nicht wiederumkehrbaren Einschränkungen der Gesundheit hervorgerufen

118 Vgl. IGES Institut GmbH (07.09.2021).
119 Vgl. Dr. Stefan Loos, Dr. Martin Albrecht, Karsten Zich (Juli 2019).

werden können. Die Möglichkeit der Risikotransferierung sollte nicht genutzt werden, auch wenn Versicherungen zur Absicherung der Patienten bestehen müssen, ist eine bewusste Übernahme von Risiken mit hohen Gefährdungspotential in diesem Kontext unmoralisch und nicht akzeptabel. Daher sollte zur Risikoreduzierung dem Ansatz von Zero Trust gefolgt werden, um eine möglichst hohes Sicherheitslevel zu erreichen. Zero Trust bedeutet in diesem Zusammenhang, dass prinzipiell keinem Nutzer, keiner technischen Lösung und keiner Anwendung oder Diensten, weder innerhalb noch außerhalb der eigenen Organisation, vertraut wird.

Konsequenzen hieraus sind

- Umsetzung des minimalen Rechteprinzips auf allen Ebenen
  - Netzwerk, Dienste, Applikationen, Daten, Nutzer, ….
- fortwährende und dynamische Authentisierung
  - abhängig vom Nutzer, dem Ort des Zugriffs, über welches Netz und System der Zugriff erfolgt
  - situationsabhängige Anpassung der genutzten Authentisierungsverfahren
- Nutzung von End-to-End-Verschlüsselung
- ständige Kontrolle statt Vertrauen
  - Was passiert gerade und ist dies ein gewünschtes/erwartetes Verhalten?
  - Neubewertung bei jeder Anfrage/Session

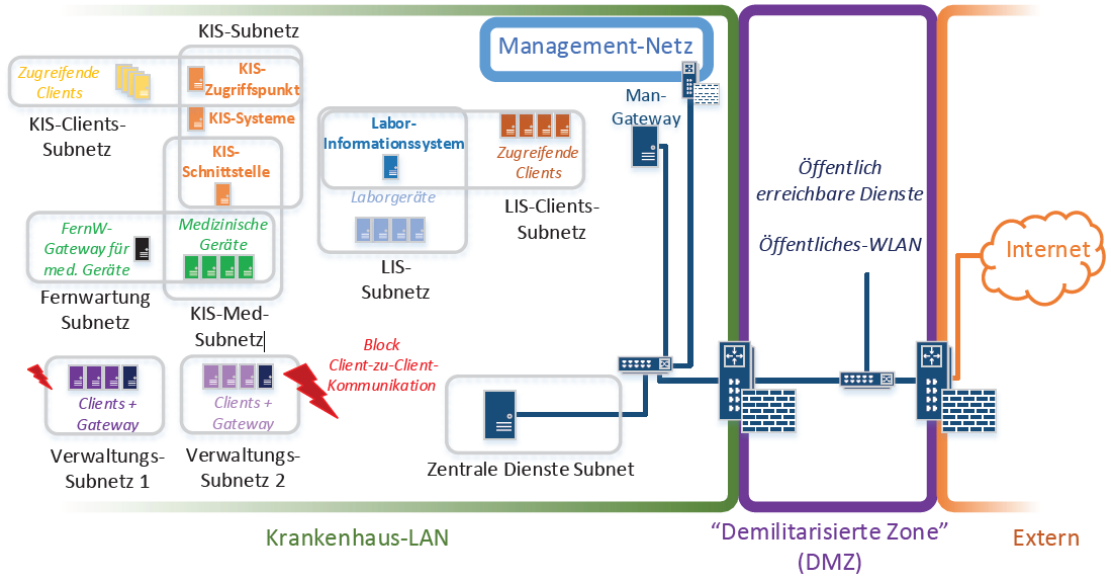
Im Gegensatz zu bisherigen Sicherheitskonzepten, wo internen Nutzer, Geräte und Anwendungen/Dienste als vertrauenswürdig eingestuft werden, wird die Vertrauensfrage bei jedem Zugriff neu gestellt und geprüft. Damit dieser vorlaufende Authentisierungsprozess keine Einschränkung im Hinblick auf die Digitalisierung darstellt, muss dieser Prozess hoch automatisiert gestaltet werden und mit einer fortlaufenden Überprüfung der definierten Sicherheitspolicies gepaart werden. Im Nachfolgenden wird auf hierfür empfohlene und geeignete Maßnahmen eingegangen.

6.4.1 Technische Maßnahmen

6.4.1.1 Netz-Segmentierung

Da die heute praktizierte strikte Trennung von Netzen im Rahmen der Digitalisierung nicht mehr aufrechterhalten werden kann, sollte eine Mikrosegmentierung auf Anwendungsebene erfolgen und die Übergänge zwischen den Netzen entsprechend mit geeigneten Regelwerken versehen werden. Für die Einbindung

der Systeme in TI sollten separate Netzwerkschnittstellen genutzt werden, um einen ersten Zugriffsschutz aus diesem Netz auf die übrige Netzinfrastruktur des Teilnehmers zu erschweren. Diese anwendungsspezifische Separierung in einzelne Subnetze ist anschaulich in der folgenden Abbildung für das KIS-System dargestellt.



Quelle: Michael Steinke, Laura Stojko, Siegfried Brunner, Volker Eiseler, Julia Hofmann, Marko Hofmann, Wolfgang Hommel, Uwe Langer, Jasmin Riedl Juli 2021

Abbildung 23: Beispiel Netzsegmentierung

Für die Anwendung KIS, die neben der Einbindung in die interne Infrastruktur auch an die TI angebunden ist, würde sich anbieten, über Software-Defined-Network-Lösungen die Trennung der Datenströme über die Infrastrukturgrenze des Krankenhauses hinaus über den Ansatz einer SD-WAN-Lösung beizubehalten und die Kommunikationsströme entsprechend zu kanalisieren und abzusichern. Dies ist über die heute vorgesehenen Konnektoren leider nicht möglich. Hier handelt es sich um „einfache“ VPN-Gateways zur Herstellung einer gesicherten Punkt-zu-Punkt Verbindung. Quality of Service und applikationsorientierte Performance, wie es z.B. für die Bereitstellung von Sprach- und Video-Lösungen benötigt wird, können damit nicht realisiert werden.

6.4.1.2 Network Access Management

Neben der Trennung von Anwendungen im Netzwerk muss es oberstes Ziel sein, keine unbekannten Endgeräte im Netzwerk zu betreiben und unkontrollierten Zugang von Endgeräten in das Netzwerk zu zulassen. Technisch lässt sich dies über entsprechende Netzwerkzugangskontrollsysteme unter Verwendung verschiedener Kriterien steuern. Zur Anwendung kommen hierzu:

- Authentifizierungsmerkmale – MAC-Adresse, Zertifikate, Token
- Sicherheitsmerkmale – aktuelle Firmware, Virenschutz, Firewall

- Bedrohungsanalyse – Kompromittierung von Geräten durch Malware, Viren, Würmer

Die Zugangssteuerung kann nach erfolgreicher Legitimation Geräte dem entsprechenden Netzsegment zuweisen. Im Falle der Verletzung von Richtlinien kann eine Alarmierung, Sperrung und automatische Behandlung des Vorgangs erfolgen. So können Geräte in Quarantäne-Netzsegmente verschoben werden und die Aktualisierung der Firmware veranlasst werden. Hierdurch kann sichergestellt werden, dass ausschließlich Geräte im Netzwerk betrieben werden, die den Sicherheitsrichtlinien entsprechen. Weiterhin kann mit dieser Maßnahme die Einbindung von Rogue-Access-Points unterbunden werden. Insbesondere die zunehmende Nutzung von IoT-Geräten macht es erforderlich, Transparenz über die im Netz betrieben Geräte zu behalten und deren Nutzern richtlinienbasiert automatisch Zugang zu gewähren.
Die im Rahmen der Netzwerkeinbindung gesammelten Informationen können an darüber liegende Sicherheitsanwendungen weitergegeben werden. IDS-Lösungen können beispielsweise über die Komponente selbst und deren Berechtigungen informiert werden, so dass hieraus Kommunikationsmuster abgeleitet werden und Anomalien erkannt werden können.

6.4.1.3 Endpoint Detection and Response

Mittel bisherigen Antiviruslösungen erfolgte eine Reaktion auf Schadprogramme, wie Viren, Trojaner, Maleware oder Würmer, auf Basis der Erkennung von bekannten Signaturen und Angriffsmuster in Form von Meldung und Isolation/Löschung der Schadsoftware. Endpoint Detection and Response-Tools dahingegen sammeln mittels auf den Geräten installierten Agenten Informationen aus verschiedene Datenquellen. Als Datenquellen kommen hierbei

- Datei-, Registry-Zugriff
- Reservieren von Speicher
- Schreiben in fremde Prozesse
- Starten von Prozessen
- Anmeldung
- Passwortänderung
- Verbindungsaufbau
- DNS- und ARP-Abfragen
- IP-Adressen
- Hardware-Typen

in Betracht.[120]

120 Vgl. LogPoint (23.06.2015).

Auf Grundlage dieser Informationen erfolgt ein Abgleich zum normalen Verhalten und ermöglich so die Erkennung von Hacking-Versuchen oder anderen unerwünschten Eingriffen auf dem jeweiligen Endgerät auch für fortgeschrittene und unbekannte Bedrohungen. Indessen Folge kann auf Vorfälle entsprechend schnell und zielgerichtet reagiert werden.

6.4.1.4 Intrusion Detection Systeme

Nicht nur in kritische Infrastrukturen, dort aber ab den 01.05.2023 verpflichtend, sollten IDS Lösungen eingesetzt werden, da mit diesen Lösungen nicht nur bekannte Angriffe mittels signaturbasierter Analyse erkannt werden, sondern auf Basis von Anomalie-basierter Erkennung auch auf unbekannte Vorgänge in der Infrastruktur reagiert und Gegenmaßnahmen eingeleitet werden können. Damit kann unbekannten Sicherheitsbedrohungen effektiv entgegengewirkt werden. Allerdings kommt es hier im Vergleich zu DER- und XDR-Lösungen zu einer zeitlichen Verzögerung, da Antworten und Reaktionen auf Vorfälle nicht automatisiert erfolgen. Um auch zukünftig angemessen auf Bedrohungen durch zunehmend intelligente Schadprogramme reagieren zu können, sollten anstatt des angestrebten Einsatzes von Intrusion Detection Systemen auf aktuelle DER- und XDR-Lösungen gesetzt werden. Es ist allerdings zu befürchten, dass auf Grund von Unkenntnis dieser Technologien und deren Vorteile bei den zuständigen Stellen diese Systeme nicht im entsprechenden Maße eingesetzt und gesetzeskonforme, „veraltete“ Lösungen zum Einsatz kommen, was im ersten Augenblick eine kostengünstigere Lösung darstellt, sich im Nachhinein aber als die teurere Alternative herausstellen wird.

6.4.1.5 Security Information and Event Management

Security Information and Event Management (SIEM) Lösungen können ergänzend zu IDS-Lösungen eingesetzt werden. Mit einer entsprechenden Lösung können erfasste Ereignisdaten über verschiedene Systeme hinweg korreliert und damit Möglichkeiten der Erkennung von Angriffen erheblich verbessert werden. So ist es zu begrüßen, dass eine entsprechende Lösung zur Überwachung der TI eingesetzt wird, um frühzeitig Angriffe erkennen zu können und über ein entsprechendes Incident-Response-Team oder eine KI kurzfristige Schutzmaßnahmen zu ergreifen und so die Teilnehmer der TI vor Angriffen über diese Infrastruktur zu schützen und gleichzeitig deren Verfügbarkeit sicherzustellen. In Verbindung mit einem SD-WAN könnten das Potential der Gesamtlösung weiter erhöht werden, indem betroffene Netzsegmente schnell isoliert werden, ohne dass die nicht betroffene Infrastruktur davon beeinträchtigt wird. Eine Ausweitung dieses zentralisierten Ansatzes auf die Infrastrukturen von Teilnehmern der TI sollte in Betracht gezogen werden. Insbesondere bei kleineren Infrastrukturen, wie z.B.

es bei Arztpraxen, welche keine eigene SIEM Lösung betreiben können, könnte ein Zugewinn an Sicherheit und damit auch für die Sicherheit der gesamten Infrastruktur erreicht werden.

6.4.1.6 Extended Detection and Response

Extended Detection and Response Systeme beziehen zusätzlich zu den von DER-Lösung erfassten Informationen Daten der Netzwerkinfrastruktur, Anwendungsserver und weiteren Sicherheitslösung, wie z.B. Firewall- und SIEM-Lösungen, in die Bewertung des Gesamtsystems mit ein und kann hieraus Abweichungen erkennen und Maßnahmen ableiten. Dies könnte sich darin äußern, dass

- Prozess gestoppt
- Host isoliert
- VPN oder RDP Zugänge blockiert
- AD-User deaktiviert

werden. Wie auch bei der EDR-Lösung kann durch die automatische Ableitung und Durchführung von entsprechenden Maßnahmen die Zeit von der Angriffserkennung bis zur Einleitung von notwendigen Aktionen erheblich verkürzt werden. Dennoch können XDR-Lösungen SIEM-Anwendung derzeit nicht ersetzen. Über Threat Detection und Investigation & Response hinausgehend werden SIEM-Lösung zur Überwachung und Einhaltung von Compliance-Regelungen eingesetzt und stellen ein entsprechendes Reporting zur Verfügung. XDR-Lösungen haben ihre Stärken mehr in der KI-basierten Behandlung von Threat Detection, Investigation & Response und können damit das einer SIEM-Lösung nachgelagerte Security Operations Center entlasten.

6.4.1.7 Data Loss Prevention

Mit DLP-Lösungen kann wirkungsvoll dem ungewollten Abfluss von Informationen entgegengewirkt werden, um damit deren Vertraulichkeit sicherzustellen. Hierbei ist es unerheblich, ob Mitarbeiter die Daten entgegen möglicher Richtlinien auf Cloud-Laufwerken speichern, auf mobilen Datenträger verloren gehen oder Daten im Rahmen von Cyberangriffen abfließen. Über entsprechende Richtlinien kann klar definiert werden, wer mit welchen Berechtigungen auf welche Daten zugreifen kann und über welche Kanäle diese das Unternehmen verlassen dürfen. So kann über diese Lösung festgeschrieben werden, dass die Kommunikation von Patientendaten ausschließlich über KIM-Lösungen erfolgt. Bei Datenaustausch über Netzwerkgrenzen hinweg kann eine automatische Verschlüsselung der Daten veranlasst werden. Dieses Vorgehen könnte den in Rahmen von Ransomware-Attacken oft vorausgehenden Datendiebstahl begegnen.

6.4.1.8 Identity- and Access Management

SIEM- und DLP-Lösungen können zusätzlich um eine IAM-Anwendung ergänzt werden. Über eine entsprechende Lösung können unterschiedlichste Authentifizierungsdienste für Webdienste oder Dateisysteme zusammengeführt werden, so dass Benutzer über einen Single-Sign-on-Zugang auf alle für ihn autorisierten Dienste zugreifen kann. Hierdurch kann auch eines der häufigsten Probleme, die Verwendung von Standard- oder einfachen Passwörtern gelöst werden. Mit der Akzeptanz durch Bequemlichkeit wird damit ein hoher Anteil zur Security-Awareness geleistet. Unter Nutzung von Technologien wie Near Field Communication oder Spracherkennung könnten Clients automatisiert freigeben und gesperrt werden. In Verbindung mit einer Zutrittsmanagementlösung kann neben der logischen Zugriffsrechtevergabe und revisionssicheren Dokumentation von Freigabeprozessen auch der physische Zugang gesteuert werden.
Ein aktueller Anwendungsfall für eine zentrale IAM-Lösung ist die ePA, wo über den elektronischen Heilberufsausweis die Zugriffssteuerung auf Patientendaten in der TI gesteuert wird. Eine Ausweitung des Berechtigungsmanagements auf Krankenhaussysteme könnte daher in Erwägung gezogen werden.

6.4.1.9 Nutzung Künstliche Intelligenz

Die Zusammenführung der Systeme zur Überwachung der Infrastruktur kann nur unter Nutzung von automatisierten Überwachungsprozessen vollumfänglich gelingen. Die Erkennung von Abweichungen und die Einleitung von geeigneten Gegenmaßnahmen in Echtzeit liegen außerhalb der menschlichen Möglichkeiten.
Dabei ist zu beachten, dass die KI nicht selbst zum Einfallstor durch Cyberkriminelle genutzt wird, in dem diese manipuliert werden und mittels unerwarteten Verhaltens eine Täuschung der KI hervorrufen wird. Demonstriert wurde ein entsprechender Angriff auf ein mittels Deep Reinforcement Learning trainiertes neuronales Netz durch Forscher der University of California, Berkeley am Beispiel eines Elfmeterduells. Ein entsprechend trainierter Agent sollte bei einem immer gleich haltenden Torwart die Elfmeter verwandeln. Wenn sich der Torwart aber unerwartet verhielt, z.B. sich auf den Boden fallen ließ, war es dem Agenten nicht mehr möglich, ein Tor zu erzielen.[121] Auf Grund der zu erwartenden Kosten müsste ein entsprechendes Cybersecurity Operation Center zentral für die klinische Infrastruktur aufgebaut und für alle Teilnehmer bereitgestellt werden.

121 Vgl. Gleave et al. (25.05.2019).

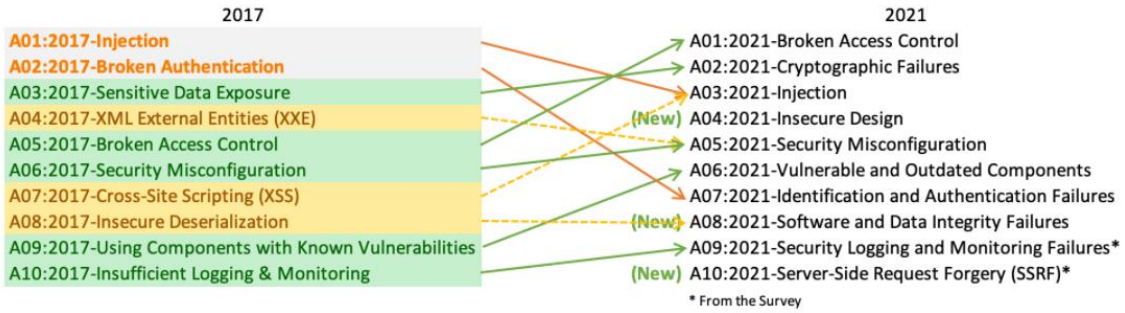
6.4.1.10 Backup & Replication

Zur Sicherstellung des Betriebs, aber auch aus Datenschutzgründen heraus, sind regelmäßige Backups der Daten und Systeme unabdingbar. Hierbei sollten möglichst mindestens zwei identische Backups erfolgen. Ein Backup zur schnellen Wiederherstellung der Daten und Systeme und ein weiteres zur Vorbeugung des Datenverlustes durch Verschlüsselung oder Kompromittierung. Hierbei sollte das zweite Backup über einen Medienbruch, z.B. über Bandlaufwerke, erstellt werden.

Als zweite Komponente sollte im Kontext einer Backupstrategie auch immer die Wiederherstellung mit betrachtet werden, um eine schnelle Wiederherstellung der Systeme zu ermöglichen. Im Rahmen der organisatorischen Maßnahmen müssen die Abläufe für die Wiederherstellung regelmäßig trainiert werden. Gleichzeitig wird dadurch die Nutzbarkeit der Backups überprüft.

6.4.1.11 Security by Design

Zur Vermeidung von Schwachstellen müssen bereits die Hersteller darauf achten, dass bei der Entwicklung der Anwendungen die Grundsätze der Software-Sicherheit berücksichtigt werden. Bei grundlegenden Neuentwicklungen ist eine Umsetzung der Empfehlungen des Open Web Application Security Project einfacher als dies bei Weiterentwicklungen der Fall ist. Insbesondere bei in der Vergangenheit individuell programmierten Anwendungen sollte sorgfältig geprüft werden, ob aus Sicherheitsgesichtspunkten eine Neuentwicklung oder die Beschaffung einer jetzt verfügbaren Standard-Anwendung einer Weiterentwicklung vorzuziehen ist. Das aus Kompatibilitätsgründen notwendigerweise Mitschleifen von alten Programmbibliotheken und abgekündigten Softwarebestandteilen erhöht deutlich die Anfälligkeit dieser Anwendungen gegenüber Cyberattacken, was sich auch in den durch die Open Web Application Security Project (OWASP) veröffentlichten Top-10-Schwachstellen von Software wiederspeigelt. Das von bekannten Schwachstellen und nicht mehr unterstützten Programmständen ausgehende Risiko ist im Vergleich zur Erhebung in 2017 um 3 Plätze von Rang 9 auf Platz 6 geklettert.



Quelle: OWASP, 2021

Abbildung 24: OSWAP Top 10 2021

Neben der Beachtung der grundlegend sicheren Programmierung der Lösungen ist auch die Akzeptanz durch nutzerfreundliche Anwendung, der Usability, bei Konzeption und Umsetzung zu beachten. Security-by-Design ist daher vielmehr als ganzheitlicher Ansatz zu verstehen und sollte sich nicht auf die Nutzung von aktuellen technischen Lösungen beschränken.

6.4.1.12 Weitere neue Technologien

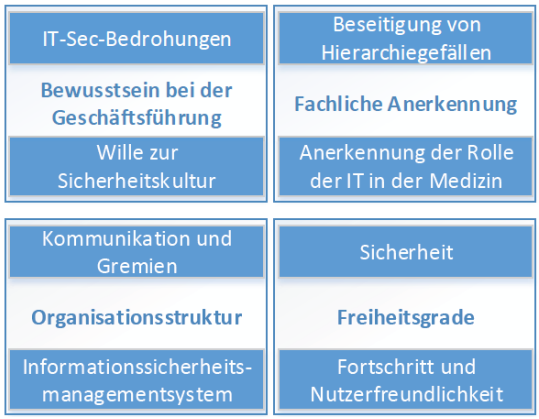
Die Entwicklung von neuen Technologien im Kampf gegen steigende Bedrohungen kommt einer besonderen Bedeutung zu. Eine vielversprechende Entwicklung könnte die Ransomware-Erkennungs- und Datenentwicklungstechnik SSD-Insider sein. Als Bestandteil der Firmware auf dem SSD-Controller laufen werden Ransomware-Angriffe auf Basis der Abweichung von Schreib-Lese-Algorithmen erkannt und verhindert über einen Wiederherstellungsalgorithmus die Verschlüsselung der Daten durch Ausnutzung der verzögerten Löschfunktion einer SSD. Die Entwickler gehen hierbei von einer nur geringen Verschlechterung der Zugriffszeiten auf das Speichermedium aus.[122] Auswirkungen auf bewusste Verschlüsselungen von Inhalten bei Nutzung dieser Technologie sind bisher nicht bekannt.

6.4.2 Organisatorische Maßnahmen

Technische Maßnahmen können nur unterstützend wirken. In erster Linie müssen organisatorische Maßnahmen zur sicheren Gestaltung der Digitalisierung getroffen werden. Über entsprechende Richtlinien, Handlungs- und Vorgehensanweisung muss deren richtige Anwendung sichergestellt werden. Bei nicht anwendungskonformer Implementierung und Nutzung können die technischen Lösungen nicht ihren Zweck erfüllen. Es müssen daher die entsprechenden Rahmenbedingungen zur Implementierung und Betrieb von sicheren Infrastrukturen geschaffen werden. Dies kann nur über das entsprechende Bewusstsein bei den Mitarbeitern gelingen. Dafür ist ein Vorangehen der Geschäftsführung notwendig. Zur Dokumentation der generellen (IT-)Sicherheits-Philosophie sind entsprechende übergeordneten Sicherheits-Policy geeignet, welche nicht nur eine interne, sondern auch eine entsprechende externe Außenwirkung haben und für Vertrauen stehen. Auf Basis dieser Policy können entsprechende Sicherheitsmaßnahmen entwickelt und implementiert werden. Oft ist allerdings der Geschäftsführung ihre Verantwortung für eine erfolgreiche Umsetzung der definierten Sicherheitsstrategie nicht bewusst. Im Klinikalltag steht zu oft ausschließlich die Versorgung der Patienten im Vordergrund und die notwendigen Maßnahmen

122 Vgl. Baek et al. (2020).

für die IT-Sicherheit werden durch die Mitarbeiter, insbesondere durch leitende Ärzte, hierfür als hinderlich empfunden. Dieses Hierarchiegefälle gilt es durch Anerkennung und Stärkung des nicht-medizinischen Personals aufzubrechen, was durch die Geschäftsleitung mit Förderung einer entsprechenden Unternehmenskultur maßgeblich beeinflusst werden kann.



Quelle: Michael Steinke, Laura Stojko, Siegfried Brunner, Volker Eiseler, Julia Hofmann, Marko Hofmann, Wolfgang Hommel, Uwe Langer, Jasmin Riedl, Juli 2021

Abbildung 25: Bausteine einer Sicherheitskultur im Krankenhaus

Zur Förderung der Anerkennung kann auch eine dahingehend aufgebaute Organisationsstruktur beitragen. Geeignet hierzu scheint der Etablierung eines unabhängigen Informationssicherheitsverantwortlichen, der direkt der Geschäftsleitung unterstellt ist.

Neben der Umsetzung und kontinuierlichen Weiterentwicklung der Sicherheitsstrategie, gemäß dem Plan-Do-Check-Act-Zyklus, gehört auch die Implementierung eines entsprechenden Notfallmanagements dazu. So sind neben den technischen Vorkehrungen auch organisatorische Maßnahmen zu planen. Diese Maßnahmen dienen zum einem zum Eindämmen der Auswirkungen, z.B. unverzügliches Trennen der Netzwerkverbindungen oder Aktivierung eines IT-Emergency-Response-Teams, als auch der Aufrechterhaltung des Klinikbetriebs. Der Ressourcenbedarf im Fall eines Angriffs ist ungleich höher als bei verfügbaren digitalen Prozessen. Regemäßiges Überprüfen und trainieren dieser Prozesse ist ebenso wichtig wie das Überprüfen von technischen Systemen selbst.

6.4.3 Personelle Maßnahmen

Personelle Maßnahmen wurden auf Grund ihrer Wichtigkeit für das Gelingen einer Sicherheitsstrategie aus den organisatorischen Maßnahmen herausgelöst. Neben der Gewinnung und Ausbildung des benötigten Personals für die IT-Abteilungen muss es gelingen, alle Mitarbeiter für (IT-)Sicherheit zu sensibilisieren.

Die Mitarbeiter als Human-Firewall tragen durch ihr Handeln einen maßgeblichen Teil zur Sicherheit bei. Dies kann über entsprechende Security-Awareness Maßnahmen wie

- Schulung und Training
- Periodische Newsletter
- offene Fehlerkultur
- interne Penetrationstests (z.B. über Phishing-E-Mails)
- Wissenstransfer/-festigung durch Quizspiele

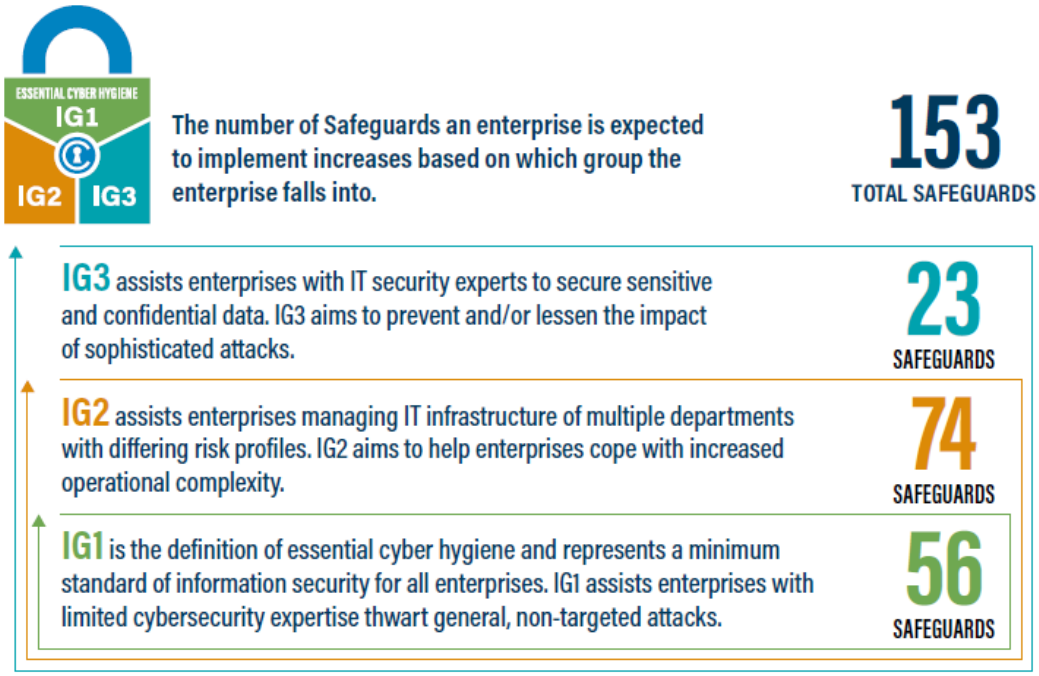
gelingen. Das gewünschte Verhalten der Mitarbeiter ausschließlich auf Basis von Richtlinien und Anweisung erreichen zu wollen, wird nur in geringem Maße den erhofften Erfolg bringen. Die Notwendigkeit des Vorhandenseins dieser Dokumente bleibt dabei unbestritten.
Begleitet werden sollten die personellen Maßnahmen als zentraler Bestandteil der Unternehmenskultur durch eine offene Feedback-Kultur und der Anerkennung von erbrachten Leistungen. Was in sozialen Medien heute bereits täglich gelebt wird, ist in vielen Unternehmen noch nicht angekommen. Die Erbringung der Arbeitsleistung wird als selbstverständlich verstanden. Jedoch erfährt im Zuge der Ressourcenknappheit der Mitarbeiterzufriedenheit als Key-Performance-Indicator wachsende Bedeutung. Gleichzeitig trägt eine hohe Zufriedenheit zur Risikoreduzierung in Bezug der Gefährdung durch Innentäter bei.

6.5 Umsetzung von Sicherheitsmaßnahme

Die Umsetzung der im vorhergehenden Kapitel aufgezeigten Maßnahmen sollte im Rahmen des PDAC Zyklus eines implementierten Informationssicherheitsmanagementsystems erfolgen. Sind entsprechenden Strukturen noch nicht installiert, sollte parallel zur Implementierung eines ISMS erste Sofortmaßnahmen ergriffen werden. Dies kann in Form der Durchführung einer Basis-Absicherung gemäß IT-Grundschutz erfolgen. Über die Basis-Absicherung wird ein grundlegendes Sicherheitsniveau angestrebt. Darauf aufbauend soll im nächsten Schritt mittels der Kern-Absicherung für die wichtigsten Systeme der Organisation ein höheres Schutzniveau erreicht werden. Im letzten Schritt kann über die Standard-Absicherung dann das Ziel verfolgt werden, die Lücke zwischen Basis- und Kern-Absicherung für die verbleibende Infrastruktur zu schließen. Problematisch bei der Vorgehensweise nach IT-Grundschutz und anderen daran angelehnten Frameworks ist die notwendige Definition des Gültigkeitsbereiches. Die Festlegung des Informationsverbunds erlaubt den Ausschluss von einzelnen Organisa-

tionseinheiten oder Infrastrukturen. Die hierdurch gewonnene Flexibilität zur Umsetzung von unterschiedlichen Sicherheitsniveaus steht die Gefahr einer Nichtberücksichtigung von Angriffsvektoren aus den nicht betrachteten Strukturen gegenüber. Insgesamt erfolgt diese Betrachtungsweise nicht aus Sicht möglicher Angriffsvektoren, sondern es werden technische und organisatorische Maßnahmen definiert, welche gegen Gefährdungen wirken. Die Implementierung auf Basis des IT-Grundschutze oder vergleichbarer Frameworks, wie ISO 27001, erfordert einen nicht unerheblichen Aufwand.

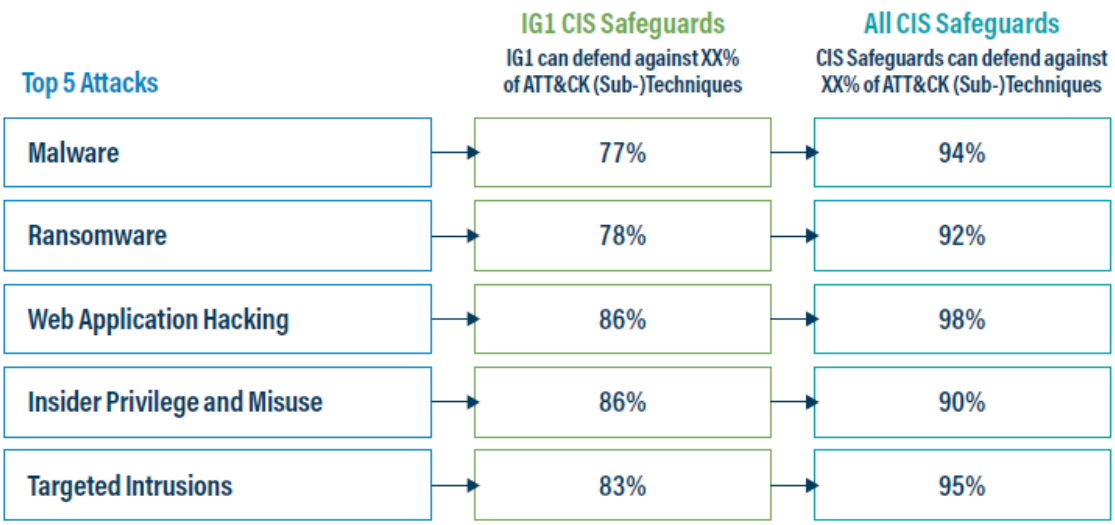
Mit einem Best-Practice-Ansatz versucht die gemeinnützige Organisation Center of Inernet Security die Sicherheit von IT-Systemen und Daten pragmatischer, kosteneffektiver und damit schneller zu gestalten. Die CIS Controls in der aktuellen Version 8 beschreiben dabei 18 Handlungsfelder mit insgesamt 153 konkreten Schutzmaßnahmen. Diese Staffelung des Niveaus der Absicherung ist hier ebenfalls in drei Stufen unterteilt. In der Implementation Gruppe 1, der Basisabsicherung, sind für die vollumfängliche Umsetzung dieser Stufe 56 Maßnahmen vorgesehen.



Quelle: Center for Internet Security, Mai 2021

Abbildung 26: Übersicht CIS Contols Implementation Groups

Das bereits mit dieser Absicherungsstufe ein gutes Sicherheitsniveau erreicht wird, zeigt das CIS Community Defense Model in der Version 2.0. Demnach weist bereits die Umsetzung der Maßnahmen der ersten Stufe eine hohe Wirksamkeit gegen die häufigsten Cyber-Angriffe auf.



Quelle: Valecia Stocchetti, 2021

Abbildung 27: Wirksamkeit CIS Controls gegen häufige Angriffsmustern [123]

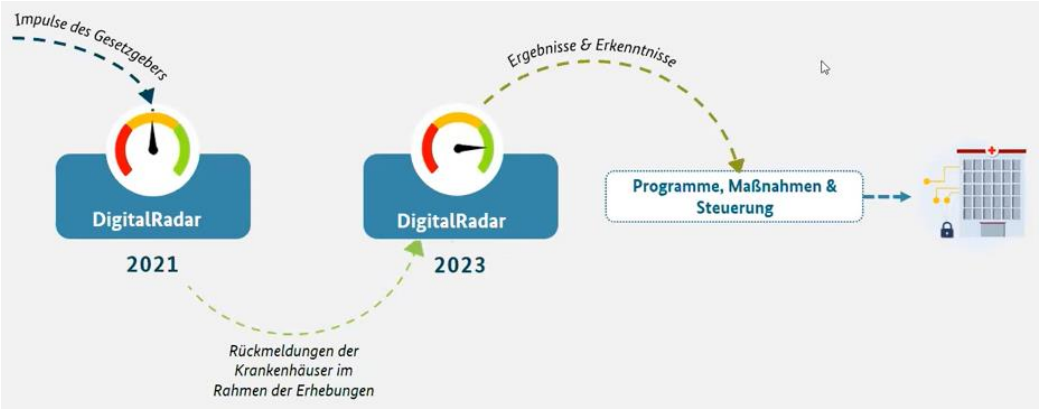
Zur Ermittlung der Wirksamkeit wurden verschiedene Angriffsvektoren und Techniken in den einzelnen Phasen eines Angriffs bewertet. Basis hierfür wurde das MITRE ATT&CK-Framework verwendet, worin derzeit mehr als 500 bekannte Angriffstechniken in Bezug auf die unterschiedlichen Phasen einer Attacke dokumentiert sind.[124] Diese Datenbank kann auch im späteren ISMS-Prozess zur Risikobewertung mit herangezogen werden, da zu der jeweiligen Angriffstechnik auch eine Bewertung zur möglichen Schadensbegrenzung und Angriffserkennung bzgl. diese Technik beschrieben wird. Diese Vorgehensweise erfasst allerdings nicht alle spezifischen Risiken im Gesundheitsumfeld, was auch nicht der Anspruch dieses Best-Practice-Ansatz ist, stellt aber einen gut und schnellen Einstiegt dar. Die branchenspezifischen Maßnahmen können anschließend darauf aufbauend ermittelt und umgesetzt werden. Für Einrichtungen, wie Arztpraxen, für welche derzeit die IT-Richtlinien der KVB gelten, würde eine Umsetzung der Maßnahmen der Implementierungsgruppe 1 einen Sicherheitsgewinn gegenüber dem aktuellen Status darstellen.

123 Alle Prozentsätze basieren auf ATT&CK-(Sub-)Techniken, die einer ATT&CK-Mitigation zugewiesen sind

124 Vgl. The MITRE Corporation (01.07.2021).

7 Zusammenfassung

Das deutsche dezentralisierte Gesundheitssystem, als eines der kostenintensivsten Gesundheitsversorgungssysteme weltweit, hat ein erhebliches Digitalisierungspotential. Welche Maßnahmen zur Verbesserung des Zustandes erforderlich sind und wie diese umgesetzt und finanziert werden können, darüber scheint es keine Erhebung zu geben. So erfolgt erst im Rahmen KHZG eine entsprechende Evaluierung in den Krankenhäusern.



Quelle: Dr. Nicolai Bodemer, 04. August 2021

Abbildung 28: Evaluierung von notwendigen Maßnahmen im Rahmen KHZG

Eine Evaluierung der konkreten Erfordernisse sollte der Gesetzgebung vorangestellt werden und nicht auf umgekehrtem Weg erfolgen. Eine kontinuierliche Messung und Bewertung der Maßnahmen ist dahingegen wie angestrebt als positiv zu bewerten. Bleibt die Hoffnung, dass dies im Gegensatz zum ITSiG auch erfolgt und Anpassungen nicht ohne eine entsprechende Erhebung und Evaluierung erfolgen. Die Gründe für die hohen Kosten in der Anzahl der Krankenhäuser zu suchen und ausschließlich durch Reduzierung dieser die notwendigen Kosteneinsparungen zu erzielen, führt mit anzunehmender hoher Wahrscheinlichkeit nicht zu dem gewünschten Ergebnis einer sicheren und effektiven Gesundheitsversorgung der Bevölkerung. Hierzu ist ein ganzheitliches, tragfähiges und von allen Akteuren akzeptiertes Konzept erforderlich. Folgt man dem Statement des Vorsitzenden der Kassenärztlichen Vereinigung Baden-Württemberg[125]

„Digitalisierung muss letztlich Mehrwerte für alle Akteure generieren.“

125 Vgl. Gesundheit wird digital (2021).

muss man konstatieren, dass was sich im ersten Moment gut anhört, an sich doch das größte Probleme darstellt, da die Mehrwerte für einzelne Akteure gegensätzlich gerichtet sind und sich daher gegenseitig ausschließen. So stehen erst einmal Gewinnmaximierung und Kosteneinsparung genauso im Wiederspruch wie Informationsfreiheit und Datenschutz und lassen sich schwer auflösen. Was bei Letzterem durch Übertragung der Daten-Ownerschaft auf jeden Einzelnen auflösen lässt, bedarf es für Ersteres eines Kompromiss', der sich im Gesundheitsbereich nicht alleinig durch marktwirtschaftliche Instrumente ergeben wird, sondern staatlicher Regelung bedarf.

Eine weitere maßgebliche Voraussetzung für das Gelingen der Digitalisierungsstrategie ist der Aufbau von Vertrauen in digitale Identitäten. Hierzu beitragen kann neben der sicheren Gestaltung der Prozesse auch die Förderung und Nutzung von einer nationalen unabhängigen Lösung. Abhängigkeiten von großen internationalen Technologiekonzernen stellt ein nicht unerhebliches Sicherheitsrisiko dar und wirkt auch nicht vertrauensbildend. So kann der von Marius von Spreti, Partner und Cyber Risk Leader bei Deloitte, geprägt Satz[126]

„Auch wenn eine komplette Risikoeliminierung niemals möglich ist,
beginnt der Schutz vor zunehmendem Datenmissbrauch ***in den Köpfen***
und an den Geräten ***der Nutzer****."*

insgesamt, nicht nur in Bezug auf die Gesundheitsdaten, wo dies schon immer höher ausgeprägt war, auf das zunehmende Sicherheitsbewusstsein der Bevölkerung in Bezug auf die eigenen Daten übertragen werden.

Wie bei der Digitalisierung, lässt sich auch in Bezug zur IT-Sicherheit keine durchgängige Strategie erkennen. Eine Verteilung der Verantwortlichkeiten auf verschiedene Organisationen ist diesem notwendigen Umstand dabei nicht zuträglich, sondern verstärkt vielmehr dessen Umstand. Die mit der Gesetzgebung angestrebten Stärkung und Erhöhung der Informationssicherheit basiert alleinig auf Druck ohne das Aufzeigen und der Bereitstellung von entsprechenden Lösungsansätzen, insbesondere fehlen für den sicheren Betrieb der jeweiligen Infrastrukturen entsprechende Konzepte. Über das KHZG bereitgestellte Mittel wurden wegen fehlender umsetzungsfähiger Lösungen und langwierigen Planungs- und Ausschreibungsphasen überwiegend pauschalisiert auf Basis der Größe der Einrichtungen verteilt.[127] Von einer bedarfsgerechten Nutzung kann daher nicht gesprochen werden. Auch berücksichtigt der Finanzierungsansatz auf Fördermittelbasis nicht die notwendigen Betriebskosten in der Folge. Über Schaffung einer IT-Security Awareness beim medizinischen Personal und Leitungsebene und der

126 Vgl. Deloitte Deutschland (August 2021).
127 Vgl. Julian Olk (05.02.2021).

Berücksichtigung von IT-Kosten in der Finanzierung des Gesundheitswesens lässt sich sicherlich mehr erreichen als über die Pönalisierung von fehlender Umsetzung vorgegebener Digitalisierungsmaßnahmen. Hier ist vielmehr zu befürchten, dass diese Mittel zu einer weiteren Einsparung im nicht medizinischen Bereich führen, da diese in der Wahrnehmung des Managements nicht zur Finanzierung des Krankenhauses beitragen.

Zurückkehrend zu der eingangs gestellten Frage, ob die über das KHZG bereitgestellten Mittel und die Form der Verteilung ausreichend ist, um die Digitalisierung signifikant und nachhaltig zu beeinflussen, muss man konstatieren, dass der erhoffte Effekt voraussichtlich nicht eintreten wird. Es werden durch die zusätzlich bereitgestellten Mittel sicherlich einige neue Projekte umgesetzt werden, größtenteils werden die Mittel aber in dringend benötigte Erneuerungen von Infrastrukturen fließen und damit nur im geringen Maße zur Erhöhung der Digitalisierung beitragen. Nachhaltige Wirkung wird es vor dem Hintergrund des Risikos der der Finanzierungslücke in Bezug der Betriebskosten nach dem Ende der Förderungen, wenn bis Ende 2024 der notwendige Strukturwandel vollzogen, zu mindestens aber begonnen wurde.

Auch die Änderungen des IT-Sicherheitsgesetzes werden nicht zur Erhöhung des Vertrauens in digitale Angebote beitragen können. In Bezug auf die Gesundheitsinfrastruktur ist dessen Möglichkeit der Einflussnahme zu gering, um die notwendigen Impulse für eine Erhöhung der IT-Sicherheit geben zu können. Durch Erhöhung der gesetzlichen Auflagen wird es zu keiner signifikanten Verbesserung der Sicherheitslage kommen. Hierfür muss vielmehr eine durchgehende Erhöhung des Sicherheitsbewusstseins bei allen Akteuren des Gesundheitswesens geschaffen werden. Parallel hierzu müssen klare Zuständigkeiten und eine Entflechtung der Gesetzgebung errichtet werden.

8 Literaturverzeichnis

ABDA – Bundesvereinigung Deutscher Apothekerverbände e. V. (Juni 2021): Die Aphotheke Zahlen. Daten. Fakten 2021. URL: https://www.abda.de/fileadmin/user_upload/assets/ZDF/ZDF21/ABDA_ZDF_2021_Broschuere.pdf.

Adhoc, A. (22.08.2021): Gematik-App: Kassen stoppen NFC-Bestellfunktion. URL: https://www.apotheke-adhoc.de/nachrichten/detail/e-rezept/gematik-app-kassen-stoppen-nfc-bestellfunktion/.

Adhoc, A. (08.10.2021): Gematik: Kasse kritisiert Geheimniskrämerei um E-Rezept. URL: https://www.apotheke-adhoc.de/nachrichten/detail/e-rezept/gematik-kasse-kritisiert-geheimniskraemerei-um-e-rezept/.

AerzteZeitung.de (2021): Ärzteschaft warnt vor zuviel Digitalisierung. URL: https://www.aerztezeitung.de/Kongresse/Aerzteschaft-warnt-vor-zuviel-Digitalisierung-419401.html.

Amt für Statistik Berlin-Brandenburg (2019): Krankenhaus und Rehabilitation. URL: https://www.statistik-berlin-brandenburg.de/krankenhaus-und-rehabilitation.

Antares Computer Verlag GmbH (15.08.2021): Krankenhauszukunftsfonds: Erst 244 Millionen Euro an Fördermitteln beantragt - Themen Digitalisierung - Publisher - Krankenhaus-IT Journal Online. URL: https://www.krankenhaus-it.de/modules/publisher/index.php/item.914/krankenhauszukunftsfonds%3A%20erst%20244%20millionen%20euro%20an%20f%C3%B6rdermitteln%20beantragt.html?keywords=Krankenhauszukunftsgesetz.

Apotheke Adhoc (30.07.202): TI-Nachzügler aufgeschreckt. URL: https://www.apotheke-adhoc.de/nachrichten/detail/apothekenpraxis/ti-nachzuegler-aufgeschreckt/.

Armin Gärtner: Aufgabenstellungen der novellierten MPBetreibV an Betreiber, Medizintechnik und IT für vernetzbare Medizinprodukte. URL: https://e-health-com.de/fileadmin/user_upload/dateien/Downloads/Gaertner_Anforderungen_der_MPBetreibV_an_vernetzbare_Medizinprodukte.pdf.

Ärzte Zeitung (24.11.2020): Zugunsten einer geriatrischen Reha-Klinik: Kleinste Klinik in Brandenburg schließt zum Jahreswechsel. In: Springer Medizin Verlag GmbH,

Avoxa – Mediengruppe Deutscher Apotheker GmbH (03.07.2021): DVPMG-Beschluss: Bundestag beschließt wichtige E-Rezept-Regelungen. URL:

https://www.pharmazeutische-zeitung.de/bundestag-beschliesst-wichtige-e-rezept-regelungen-125484/.

Baek, S./Jung, Y./Mohaisen, A./Lee, S. und Nyang, D. (2020): SSD-assisted Ransomware Detection and Data Recovery Techniques. In: IEEE Transactions on Computers 2020, S. 1.

Baeuerle (2021): Bekanntgabe Förderanteile Bundesländer ZF_Stand 01.02.2021 2021.

Barmer (03.07.2021): Gesetz zur digitalen Modernisierung von Versorgung und Pflege | BARMER. URL: https://www.barmer.de/politik/aktuelle-gesetzgebung/dvpmg-274278.

Berthold Wesseler (05.07.2021): Kaseya ist kein Einzelfall. URL: https://www.it-zoom.de/dv-dialog/e/kaseya-ist-kein-einzelfall-28418/?xing_share=news.

Bitkom e.V. (05. August 2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr. URL: https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr.

Bosch Global (19. Februar 2020): Ethische Leitlinien für Künstliche Intelligenz. Robert Bosch GmbH. URL: https://www.bosch.com/de/stories/ethische-leitlinien-fuer-kuenstliche-intelligenz/.

Bundesamt für Sicherheit in der Informationstechnik (2020a): KRITIS-Sektor Gesundheit: Informationssicherheit in Laboren Rahmenbedingungen, Status Quo, Handlungsfelder.

Bundesamt für Sicherheit in der Informationstechnik (11. 12. 2020): Cyber-Sicherheitsbetrachtung vernetzter Medizinprodukte. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.pdf;jsessionid=DD8761B4952DA3B482F85593476B9C70.internet462?__blob=publicationFile&v=1.

Bundesamt für Sicherheit in der Informationstechnik (07.01.2021): Internationale Anerkennung - Anerkennung von CC– Zertifikaten im Rahmen des CCRA. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Internationale-Anerkennung/CCRA_Anerkennung_dvl.html;jsessionid=17D566BBF608B1091923C57A35FF7066.internet082?nn=127374.

Bundesamt für Sicherheit in der Informationstechnik (01.07.2021): E-Rezept: BSI bestätigt Sicherheit. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210701_E-Rezept.html.

Bundesamt für Sicherheit in der Informationstechnik (16.07.2021a): Informationen für Hersteller. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/fuer-Hersteller/IT-SiK-fuer-hersteller_node.html.

Bundesamt für Sicherheit in der Informationstechnik (16.07.2021b): Informationen für Verbraucherinnen und Verbraucher. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html.

Bundesamt für Sicherheit in der Informationstechnik (16.07.2021c): Informationen für Verbraucherinnen und Verbraucher. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html.

Bundesamt für Sicherheit in der Informationstechnik (*BSI) (Oktober 2019)*: Die Lage der IT-Sicherheit in Deutschland 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=5B00F719FDAFE5A6633FCCB2B345C202.internet481?__blob=publicationFile&v=1.

Bundesamt für Sicherheit in der Informationstechnik (*BSI) (September 2020)*: Die Lage der IT-Sicherheit in Deutschland 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf;jsessionid=5B00F719FDAFE5A6633FCCB2B345C202.internet481?__blob=publicationFile&v=1.

Bundesärztekammer (31.12.2020): Ärztestatistik 31.12.2020.

Bundeskriminalamt (April 2021): Bundeslagebild | Cybercrime 2020. URL: www.bka.de/Lagebilder.

Bundesministerium für Gesundheit (2021): Digitales Gesundheitsamt: DEMIS. URL: https://gesundheitsamt-2025.de/angebote/demis.

Bundesverband Gesundheits-IT (21. Juni 2019): Eckpunktepapier-Kuenstliche-Intelligenz 21. Juni 2019.

Bundesverband Gesundheits-IT (01. Juni 2021): Gesundheit digital gestalten. bvitg Kernpositionen zur Bundestagswahl 2021 01. Juni 2021.

Bundesverband Medizintechnologie (1. Oktober 2020): Branchenbericht Medizintechnologien 2020. URL: https://www.bvmed.de/download/charts-med-tech-markt.pdf.

(Mai 2021): CIS Controls Version 8. URL: https://www.cisecurity.org/controls/v8/.

Daniel Sonnenberg (August 2019): Bevölkerungsfrage zum Thema Health. URL: https://www.bvdw.org/abfrageformular/bevoelkerungsfrage-zum-thema-health/10793/.

datenschutz cert GmbH (2020): https://www.doctolib.de - datenschutz cert GmbH. URL: https://ips.datenschutz-cert.de/doctolib.

Datenschutzkonferenz (3. April 2019): Hambacher Erklärung zur Künstlichen Intelligenz. In: Datenschutz und Datensicherheit - DuD, 43. Jg. 3. April 2019, H. 6, S. 375–376.

Deloitte Deutschland (August 2021): Cyber Security Report 2021. URL: https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (21.06.2021): Pressemitteilungen - Künstliche Intelligenz muss dem Menschen dienen. Pressemitteilung 12/2021. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. URL: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2021/12_K%C3%BCnstliche-Intelligenz-Menschen-dienen.html.

(24.05.2018): Der lange Weg eines Medizinproduktes von der Idee bis zur Anwendung am Patienten. URL: https://www.bvmed.de/de/versorgung/gesundheitspolitik/fortschritt-erleben/ferl201805-weg-eines-medizinproduktes.

Detlef Baer (31.07.2021): Die ePA kommt | IKK BB. 2020. URL: https://www.ikkbb.de/ueber-uns/unternehmen/positionen/epa.

Deutsche Krankenhausgesellschaft e. V. (14. Januar 2021): Stellungnahme der Deutschen Krankenhausgesellschaft zum Entwurf der Bundesregierung eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme. URL: https://www.dkgev.de/fileadmin/default/2021-02-24_Regierungsentwurf_IT-SiG_2.0_DKG-Stellungnahme.pdf.

Deutscher Ärzteverlag GmbH, Redaktion Deutsches Ärzteblatt (2021): Gesundheitsämter weiter zögerlich bei einheitlicher Software. URL: https://www.aerzteblatt.de/nachrichten/120842/Gesundheitsaemter-weiter-zoegerlich-bei-einheitlicher-Software.

(19.09.2021): Deutsches Krankenhaus Verzeichnis. URL: https://www.deutsches-krankenhaus-verzeichnis.de/app/suche.

Deutschlandfunk (2021): Corona-Bekämpfung in Behörden - Die verschleppte Digitalisierung. URL: https://www.deutschlandfunk.de/corona-bekaempfung-in-behoerden-die-verschleppte.724.de.html?dram:article_id=497446.

DeWiki (22.08.2021): Hilfsfrist. URL: https://dewiki.de/Lexikon/Hilfsfrist.

Dezernat Digitalisierung und IT (2021): FAQ - Richtlinie IT-Sicherheit in der Praxis - IT-Sicherheit in der Praxis. URL: https://hub.kbv.de/display/itsrl/FAQ.

Dieter Hallervorden (4. März 2021): Lockdown bis Ostern – weil Bund und Länder versagen? URL: https://www.zdf.de/politik/maybrit-illner/lockdown-bis-ostern-weil-bund-und-laender-versagen-sendung-vom-4-maerz-2021-100.html.

(03.07.2021): DiGA-Verzeichnis. URL: https://diga.bfarm.de/de/verzeichnis.

DMEA – Connecting Digital Health (15.09.2021): Künstliche Intelligenz durchdringt das Gesundheitswesen. URL: https://www.dmea.de/de/presse/news-blog/artikel/k%C3%BCnstliche-intelligenz-durchdringt-das-gesundheitswesen.html.

Dr. Astrid Bartels (03. Mai 2021): kv.dox – der KIM-Dienst des KV-Systems - kv.dox - Partnerportal der kv.digital GmbH. URL: https://partnerportal.kv-telematik.de/pages/viewpage.action?pageId=71079164.

Dr. Holger Schmidt (2016): Menschen vertrauen Robotern oft blind. URL: https://www.netzoekonom.de/2016/11/15/12236/.

Dr. Karl Blum (15.08.2021): Investitionsstau und Digitalisierungsprobleme in deutschen Krankenhäusern. URL: https://www.dki.de/pressemitteilung/pressemitteilung-investitionsstau-und-digitalisierungsprobleme-in-deutschen-krankenhaeusern.

Dr. Markus Schlobohm (28.09.2021): Der Versicherte im Mittelpunkt: Die Akte aus der Patientenperspektive. Online.

Dr. med. Petra Reis-Berkowicz (16.12.2020): Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit. URL: https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf.

Dr. Nicolai Bodemer (04. August 2021): KHZG: Deep Dive | Reifegradmessung der deutschen Krankenhäuser. Online.

Dr. Stefan Loos, Dr. Martin Albrecht, Karsten Zich (Juli 2019): Zukunftsfähige Krankenhausversorgung Juli 2019.

Dr. Steffen Hehner, Dr. Karl Liese, Gerald Loos, Dr. Manuel Möller, Dr. Stephanie Schiegnitz, Tobias Schneider, Dr. Mark Oellerich, Dr. Max Plischke, Anke Donath, Nadine Erk (September 2018): Digitalisierung in deutschen Krankenhäusern - Eine Chance mit Milliardenpotenzial für das Gesundheitssystem. URL: www.mckinsey.com.

Dr. Timo Braun, Patrick Winter (08. Dezember 2020): IT-Sicherheitsvorfälle in 2020. URL: https://www.curacon.de/neuigkeiten/neuigkeit/it-sicherheitsvorfaelle-in-2020.

(17.03.2021): Drucksache 19/27652. Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege. URL: www.betrifft-gesetze.de.

(29. Oktober 2015): E-HEALTH: ETHISCHE GRUNDSÄTZE. URL: https://www.abda.de/fileadmin/user_upload/assets/ehealth/E_Health_Ethische_Grundsaetze_ABDA_2015.pdf.

Ehneß, J. (16.08.2021): OVH-Großbrand hat gravierende Folgen. URL: https://www.storage-insider.de/ovh-grossbrand-hat-gravierende-folgen-a-1008399/.

Einhorn Apotheke am Stern (27.07.2021): Informationen zum Corona Impfzertifikat. URL: https://www.einhorn-apotheken.de/services/impfzertifikat.html.

endoflife.date (2021): Android OS. URL: https://endoflife.date/android.

Europäische Kommission (16.09.2021): Künstliche Intelligenz – ethische und rechtliche Anforderungen. URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Kunstliche-Intelligenz-ethische-und-rechtliche-Anforderungen/feedback_de?p_id=8242911.

gematik GmbH (Dezember 2020): Telematikinfrastruktur 2.0 - Arena für digitale MedizinWhitepaper. Berlin.

gematik GmbH (2021a): Dokumentensuche. URL: https://fachportal.gematik.de/dokumentensuche.

gematik GmbH (2021b): Elektronisches Rezept. URL: https://fachportal.gematik.de/anwendungen/elektronisches-rezept?tx_gemcharacteristics_productlist%5BformIdentifier%5D=form-3211&tx_gemcharacteristics_productlist%5Btype%5D=ProdT&tx_gemcharacteristics_productlist%5Bproducttype%5D=107&tx_gemcharacteristics_productlist%5Bproducttypeversion%5D=97#c3211.

gematik GmbH (2021c): FAQ. URL: https://www.gematik.de/anwendungen/e-patientenakte/faq/.

gematik GmbH (2021d): KIM. URL: https://www.gematik.de/anwendungen/kim/.

gematik GmbH (2021e): Kommunikation im Medizinwesen. URL: https://fachportal.gematik.de/anwendungen/kommunikation-im-medizinwesen.

gematik GmbH (2021f): Notfalldaten. URL: https://www.gematik.de/anwendungen/notfalldaten/.

gematik GmbH (26.06.2021): Weichenstellung für mehr Zusammenspiel im Gesundheitswesen. URL: https://www.gematik.de/news/news/weichenstellung-fuer-mehr-zusammenspiel-im-gesundheitswesen/.

gematik GmbH (21.07.2021): Konzeptpapier TI-Messenger. URL: https://fachportal.gematik.de/fileadmin/Fachportal/Anwendungen/TI-Messenger/gemKPT_TI_Messenger_V1.0.0.pdf.

Gerlof, H. (17.11.2020): Telematikinfrastruktur: Viertes Digitalisierungsgesetz soll Datenschutz-Problem abräumen. In: Springer Medizin Verlag GmbH, Ärzte Zeitung.

(2019): Germany: Country Health Profile 2019. Paris.

Gesundheit wird digital (2021): KVBW-Vorsitzender: "Digitalisierung muss letztlich Mehrwerte für alle Akteure generieren." - Gesundheit wird digital. URL: https://gesundheit-wird-digital.de/2021/04/26/digitalisierung-muss-letztlich-mehrwerte-fuer-alle-akteure-generieren/.

GKV-Spitzenverband (22.06.2021): Alle gesetzlichen Krankenkassen - GKV-Spitzenverband. URL: https://www.gkv-spitzenverband.de/krankenversicherung/kv_grundprinzipien/alle_gesetzlichen_krankenkassen/alle_gesetzlichen_krankenkassen.jsp.

GKV-Spitzenverband (28.09.2021a): Elektronische Arbeitsunfähigkeitsbescheinigung (eAU) - GKV-Spitzenverband. URL: https://www.gkv-spitzenverband.de/krankenversicherung/digitalisierung_und_innovation/eau/eau.jsp.

GKV-Spitzenverband (28.09.2021b): Meldung der Arbeitsunfähigkeitszeiten (eAU) - GKV-Datenaustausch. URL: https://www.gkv-datenaustausch.de/arbeitgeber/eau/eau.jsp.

Gleave, A./Dennis, M./Wild, C./Kant, N./Levine, S. und Russell, S. (25.05.2019): Adversarial Policies: Attacking Deep Reinforcement Learning.

Gunther Nolte (11.03.2021): Health-IT Talk Special: Krankenhauszukunftsgesetz. KHZG aus Sicht des BMG, eines Bundeslandes und einer Klinik. Online.

Guntram Doelfs (08.04.2021): Cyber-Attacken: IT-Sicherheit von Kliniken mangelhaft. URL: https://www.kma-online.de/aktuelles/it-digital-health/detail/it-sicherheit-von-kliniken-mangelhaft-a-45318.

Harald Czycholl (04.01.2021): Elektronische Krankmeldung: Das gilt ab Oktober 2021. In: Deutsche Handwerks Zeitung.

Healthcare Mittelhessen (2019): Trendbericht Virtual Reality: So hilft die virtuelle Realität der Medizin. URL: https://healthcare-mittelhessen.eu/virtual-reality-digitale-ausbildungshelfer-fuer-die-reale-medizin.

HIMSS Analytics - Europe (2019): Stage 6 & 7 Achievement. URL: https://www.himssanalytics.org/europe/stage-6-7-achievement.

https://www.helios-gesundheit.de/ (12.04.2019): Pilotprojekt setzt neue Maßstäbe beim Austausch von Behandlungsdaten. Helios Klinikum München West. URL: https://www.helios-gesundheit.de/kliniken/muenchen-west/unser-haus/aktuelles/detail/news/pilotprojekt-setzt-neue-massstaebe-beim-austausch-von-behandlungsdaten/.

https://www.helios-gesundheit.de/ (15.06.2021): Helios - das Unternehmen für Gesundheit. URL: https://www.helios-gesundheit.de/unternehmen/.

huawei (27.042021): Digitalisierung im Gesundheitswesen: Chancen durch KI & Co. URL: https://www.huawei.com/de/deu/magazin/e-health/analoge-klinik-oder-smart-hospital.

IGES Institut GmbH (07.09.2021): Simulation: 2030 eine von drei Kliniken in der Region Köln und Umgebung ausreichend. URL: https://www.iges.com/kunden/gesundheit/forschungsergebnisse/2019/krankenhaeuser/index_ger.html.

(06 August 2021): Input to the European Commission public consultation on the proposed 'Regulation laying down harmonized rules on artificial intelligence (AI Act)' by the Johner Institute. URL: https://ec.europa.eu/info/law/better-regulation/.

IT-Sicherheit-und-Recht.de (2017): Unterschreiten vom Stand der Technik - Comply or explain! | IT-Sicherheit-und-Recht.de. URL: https://it-sicherheit-und-recht.de/2017/08/29/unterschreiten-vom-stand-der-technik-comply-or-explain/.

J. Bolkart (09.08.2021): Cyberangriffe - Umfrage zum Täterkreis | Statista. URL: https://de.statista.com/statistik/daten/studie/1230319/umfrage/umfrage-unter-deutschen-unternehmen-zum-taeterkreis-von-cyberangriffen/.

Jennifer Hammel (25.06.2019a): BVDW_Grafik_HealthStudie_01.png (1200×630). URL: https://www.bvdw.org/der-bvdw/news/detail/artikel/bvdw-studie-hohe-akzeptanz-fuer-kuenstliche-intelligenz-und-digitale-anwendungen-im-gesundheitswesen/.

Jennifer Hammel (25.06.2019b): BVDW-Studie: Hohe Akzeptanz für künstliche Intelligenz und digitale Anwendungen im Gesundheitswesen. URL: https://www.bvdw.org/presse/detail/artikel/bvdw-studie-hohe-akzeptanz-fuer-kuenstliche-intelligenz-und-digitale-anwendungen-im-gesundheitswesen/.

Jörg Rauschenberger, Dr. Karl Blum, Prof. Dr. Volker Nürnberg, Dr. rer. pol. Matthias Offermanns (05. November 2019): Digitalisierung in deutschen Krankenhäusern bestenfalls noch in den Kinderschuhen. URL: https://www.bdo.de/de-de/insights-de/weitere-veroffentlichungen/studien/stand-der-digitalisierung-in-krankenhausern.

Julian Olk (05.02.2021): Länder wälzen Finanzierung ab oder verteilen per Gießkanne. URL: https://www.handelsblatt.com/inside/digital_health/milliarden-foerderung-laender-waelzen-finanzierung-auf-krankenhaeuser-ab-oder-verteilen-per-giesskanne/26889288.html?ticket=ST-1310614-GA305h6zfHjiJAQanEEL-ap2.

Jürgen Klauber, Max Geraedts, Jörg Friedrich, Jürgen Wasem Hrsg. (2019): Krankenhausreport 2019. Das digitale Krankenhaus.

Kaspersky (14. Juli 2021): Kaspersky_B2B_Healthcare_Report_07.2021 14. Juli 2021.

Klick, J./Koch, R. und Brandstetter, T. (20.01.2021): Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic.

(02.03.2020): Konzept Architektur der TI-Plattform. Version 2.10.0. gematik GmbH.

Krempl, S. (10.12.202): IT-Sicherheitsgesetz 2.0: "Mittelfinger ins Gesicht der Zivilgesellschaft&quot. Heise Medien. URL: https://www.heise.de/news/IT-Sicherheitsgesetz-2-0-Mittelfinger-ins-Gesicht-der-Zivilgesellschaft-4986032.html.

Krempl, S. (29.07.2021): IT-Sicherheitskennzeichen: BSI muss keine "Tiefenprüfung" durchführen. In: heise online.

(2020b): KRITIS-Sektor Gesundheit: Informationssicherheit in der stationären medizinischen Versorgung Rahmenbedingungen, Status Quo, Handlungsfelder. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_stationaere_med_Versorgung.pdf?__blob=publicationFile&v=3.

(2021): kv.digital – Digitalisierung im Gesundheitswesen. URL: https://www.kv.digital/.

Landesärztekammer Baden-Württemberg (31.07.2020): Elektronischer Medikationsplan (eMP). URL: https://www.aerztekammer-bw.de/10aerzte/45ae-health/ti-anwendungen/02-eMP/index.html.

Linus Neumann, Frank Rieger, Dirk Engling, Matthias Marx (01. März 2021): Sicherheit gestalten statt Unsicherheit verwalten 01. März 2021.

LogPoint (23.06.2015): Der Unterschied zwischen SIEM und EDR. URL: https://www.logpoint.com/de/blog/the-difference-between-siem-and-edr/.

Lossau, N. (02.01.2013): Hirnforschung: Digitale Demenz? Von wegen! In: WELT.

Luber, S. (26.06.2021): Was ist Digitalisierung? URL: https://www.bigdata-insider.de/was-ist-digitalisierung-a-626489/.

Maier, J. (04.05.2020): Die besten Gesundheitssysteme weltweit. In: praktischArzt.

Martin Lundbor, Pirmin Puhl, Annette Hillebrand, Sebastian Tenbrock, Julia Wielgosch (Januar 2020): Sichere Digitalisierung im Mittelstand. URL: https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Publikationen/it-sicherheitsstudie-kurzfassung.pdf?__blob=publicationFile&v=9.

Martin Peuker (28.09.2021): Datengetriebene Medizin. Online.

(Dezember 2019): MDCG 2019-16 - Leitlinien zur Cybersicherheit für Medizinprodukte. URL: https://ec.europa.eu/health/md_sector/new_regulations/guidance_en.

Medical Device Coordination Group (October 2019): md_mdcg_2021_mdsw_en October 2019.

(21 June 2017): Medienbrüche und Sicherheitslücken. URL: https://www.werbewoche.ch/en/digital/2017-06-21/schweizer-gesundheitswesen-steht-vor-einem-digitalisierungsschub/.

Michael Steinke, Laura Stojko, Siegfried Brunner, Volker Eiseler, Julia Hofmann, Marko Hofmann, Wolfgang Hommel, Uwe Langer, Jasmin Riedl (Juli 2021): Smart Hospitals: Neuauflage des Maßnahmenkatalogs zur Verbesserung der IT-Sicherheit in bayerischen Krankenhäusern. Universität der Bundeswehr München. URL: https://www.unibw.de/code/news/smart-hospitals-neuauflage-2021.

Michael Thoss (30. Mai 2020): Das regionale Krankenhaus am digitalen Finanzierungsabgrund: Warum kleine Krankenhäuser den Anforderungen der "Digitalisierung" kaum entsprechen können.

Ministerium für Wirtschaft, Arbeit und Gesundheit Mecklenburg-Vorpommern (Juni 2021): Krankenhauswesen - Regierungsportal M-V. URL: https://www.regierung-mv.de/Landesregierung/wm/gesundheit/Gesundheitsversorgung/Krankenhauswesen/.

Nürnberg, V. und Schneider, B. (2014): Kundenmanagement im Krankenhaus. Service, Qualität, Erreichbarkeit. Wiesbaden.

OWASP (2021): OWASP Top 10:2021 (ENTWURF FÜR PEER REVIEW). URL: https://owasp.org/Top10/.

PKV (22.06.2021): PKV: Mitglieder PKV-Verband. URL: https://www.pkv.de/verband/ueber-uns/mitglieder-pkv-verband/.

Prof. Dr. Dr. Thomas Schildhauer (2018): Schlüsselfaktoren der Digitalisierung. Institute of Electronic Business e. V. URL: https://www.schluesselfaktoren.de/Studie_Schluesselfaktoren.pdf.

Rene Schubert (08.10.2021): Startseite | Deutsches Krankenhaus Verzeichnis. URL: https://www.deutsches-krankenhaus-verzeichnis.de/app/suche.

Repschläger, Uwe/Schulte, Claudia und Osterkamp, Nicole (Hrsg.) (2019): BARMER Gesundheitswesen aktuell 2019. Beiträge und Analysen. Wuppertal.

Reuter, M. (26.05.2021): IT-Sicherheit: Schon wieder desaströse Sicherheitslücke in Luca App. URL: https://netzpolitik.org/2021/it-sicherheit-schon-wieder-desastroese-sicherheitsluecke-in-luca-app/.

S. Neumeier, T. O. (2016): Erreichbarkeit von Krankenhäusern mit Schwerpunkt- und/oder Maximalversorgung. Thünen-Erreichbarkeitsmodell 2019. URL: https://www.deutschlandatlas.bund.de/DE/Karten/Unsere-Gesundheitsversorgung/129-PKW-Krankenhaeuser-Maximalversorgung.html.

Schmidt, J. (06.07.2021): Kaseya VSA: Wie die Lieferketten-Angriffe abliefen und was sie für uns bedeuten. In: heise online.

(12.11.2020a): Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter. Version 1.3.0. gematik GmbH.

Statistisches Bundesamt (April 2021): Verzeichnis der Krankenhäuser und Vorsorge- oder Rehabilitationseinrichtungen. Stand 2019.

(08.10.2021): Strukturveränderung simulieren - GKV-Kliniksimulator. URL: https://www.gkv-kliniksimulator.de/start/.

SYNAGON (07.05.2021): Antragsverfahren im Überblick. URL: https://synagon.de/antragsverfahren-im-ueberblick/.

(12.11.2020b): Systemdesign der Telematikinfrastruktur. gematik GmbH.

t3n Magazin (2021): Datenschutz-Desaster bei Doctolib: Wundere dich nicht, wenn Facebook deinen Vasektomie-Termin kennt. URL: https://t3n.de/news/datenschutz-desaster-doctolib-1386492/.

The MITRE Corporation (01.07.2021): MITRE ATT&CK®. URL: https://attack.mitre.org/.

Tim Aschermann (11.12.2020): Alle Android-Versionen im Überblick. URL: https://praxistipps.chip.de/alle-android-versionen-im-ueberblick_40765.

(09.07.2021): Übergreifende Spezifikation Netzwerk. gemSpec_Ne.

Universität der Bundeswehr München (Juni 2019): Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser. Sichere Digitalisierung bayrischer Krankenhäuser. Universität der Bundeswehr München. URL: https://smart-hospitals.code.unibw-muenchen.de/#/.

(25.09.2017): Unsere Behörden und Einrichtungen. In: Bundesministerium des Innern, für Bau und Heimat.

Valecia Stocchetti (2021): CIS Community Defense Model Version 2.0. URL: https://www.cisecurity.org/blog/cis-community-defense-model-v2-0-coming-to-a-computer-near-you-summer-2021/.

Verband der Diagnostica-Industrie (2018): Kosten und Nutzen - VDGH - Verband der Diagnostica-Industrie e.V. URL: https://www.vdgh.de/nutzen-der-diagnostica/kosten-und-nutzen/worum-es-geht.

VFR Verlag für Rechtsjournalismus GmbH (11. August 2021): Elektronische Patientenakte – digitalisierte Gesundheitsdaten. In: Datenschutz.

Volker Mielke (28. September 2021): gematik TI 2.0 - Netzwerk: Beginn einer neuen Zeit. Online.

Welle, D. (01.08.2021): Gesundheitsämter: Mit Papier, Stift und Fax gegen Corona | DW | 26.01.2021. Deutsche Welle (www.dw.com). URL: https://www.dw.com/de/gesundheits%C3%A4mter-mit-papier-stift-und-fax-gegen-corona/a-56347106.

Wissen zu medizinischer Software (2019): MDR Regel 11 / Rule 11: Der Klassifizierungs-Albtraum? URL: https://www.johner-institut.de/blog/regulatory-affairs/mdr-regel-11/.

Wohlhüter, I. (21.01.2017): Was ist eigentlich… Digitale Demenz? In: WiPub - We publish!

(05. Oktober 2021): Zum X-ten Mal: Wir brauchen ein Zukunftsprogramm deutsches Krankenhaus! URL: https://www.vkd-online.de/?mnd_article=press-release3133725.

Anhang

Anhang A - Klinikverbünde

Kranken-haus-verbunds-ID	Krankenhausverbund	Standorte des Verbunds gesamt	Fälle				
			Betten	Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
004	Helios	110	27.589	3.386.528	1.164.675	23.547	2.196.565
005	Asklepios Kliniken Verwaltungsgesellschaft mbH	77	14.229	1.442.659	423.272	19.063	898.245
008	Sana Kliniken AG	40	8.489	1.113.525	369.430	8.908	705.204
016	Vivantes Klinikum	12	5.903	307.634	231.593	10.715	65.326
033	AGAPLESION	20	5.050	634.507	176.240	12.772	381.605
014	SRH Holding (SdbR)	12	3.752	415.291	149.718	2.705	262.868
030	AMEOS	29	6.698	239.269	141.609	3.772	93.888
032	Klinikum Region Hannover GmbH	10	2.953	663.860	124.273	1.311	538.276
027	UNIVERSITÄTSKLINIKUM Schleswig-Holstein	3	2.130	422.196	105.561	5.123	311.383
045	Klinikum Nürnberg	2	2.225	273.417	98.902	2.908	171.607
007	Malteser Hilfsdienst e.V.	11	2.536	237.317	86.547	1.971	128.887
018	Alexiander GmbH	11	3.098	268.628	79.296	3.481	156.367
023	Johannesstift Diakonie	8	1.798	212.469	78.840	640	132.989
044	Evangelisches Klinikum Bethel gGmbH	5	3.977	211.243	71.040	6.602	133.601
019	Immanuel-Krankenhaus GmbH	15	2.138	224.980	70.923	18.637	135.420
060	Gemeinnützige Gesellschaft der Franziskanerinnen zu Olpe mbH (GFO)	6	1.280	319.958	67.990	-	251.968
089	KMG Kliniken SE	10	1.725	208.924	67.219	653	141.052
041	Landschaftsverband Westfalen-Lippe	48	3.935	501.991	66.659	12.682	339.957
017	DRK Kliniken Berlin e.V.	4	1.351	206.650	62.481	411	143.758
024	Paracelsus Kliniken	15	2.214	183.221	60.340	679	97.803
039	Klinikum Dortmund	2	1.422	315.060	57.743	180	257.137
002	Städtisches Klinikum Dresden	3	1.473	186.149	55.848	2.332	127.969
049	Kliniken der Stadt Köln gGmbH	3	1.335	246.224	53.810	2	192.412
056	RoMed Kliniken	4	1.032	136.352	53.376	1.602	81.374

Kranken-haus-verbunds-ID	Krankenhausverbund	Standorte des Verbunds gesamt	Fälle				
			Betten	Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
031	DIAKOVERE gGmbH	3	1.074	143.974	52.639	159	91.176
052	Schwarzwald-Baar Klinikum	2	1.046	205.876	48.270	-	157.606
077	medius-kliniken	3	1.098	165.015	47.747	167	117.101
065	Gesundheitsverbund Landkreis Konstanz (GLKN) gemeinnützige GmbH	4	1.020	188.090	47.109	28	140.953
051	Klinikverbund Südwest	6	2.235	307.793	45.192	466	127.402
059	Klinikum Bamberg	3	1.013	105.200	44.535	1.695	58.970
003	Elblandkliniken	3	1.030	152.849	42.851	360	109.638
096		4	1.125	153.598	42.808	11.196	99.594
037	Landschaftsverband Rheinland (LVR)Dezernat 8 - Klinikverbund und Verbund Heilpädagogischer Hilfen	10	4.280	642.643	42.492	5.695	533.315
057	Kliniken Nordoberpfalz AG	6	989	108.058	41.037	619	61.786
083	Klinikum Mutterhaus der Borromäerinnen gGmbH	3	1.054	112.826	40.792	419	71.615
038	St. Vincenz-Krankenhaus GmbH	2	790	145.331	40.727	4.539	100.065
085	MEDICLIN Müritz-Klinikum	21	1.749	81.817	40.519	1.321	40.045
015	Heinrich-Braun-Klinikum gemeinnützige GmbH	2	930	83.567	38.997	2.167	42.403
058	Klinikum Bayreuth	2	1.048	78.598	38.492	1.330	38.776
055	Klinikum Passau	2	670	80.638	37.991	321	42.326
063	Ortenau Klinikum Offenburg	3	736	136.524	34.980	172	101.372
086	Vitos GmbH	46	2.615	228.861	34.906	4.819	188.783
035	Harzklinikum Dorothea Christiane Erxleben GmbH	7	1.054	115.092	34.407	1.889	78.796
061	Klinikum Oberberg	3	1.034	129.708	34.051	685	94.972
062	Kreiskliniken Reutlingen	2	678	126.801	32.747	-	94.054
072	Katholisches Klinikum Lünen/Werne GmbH	2	786	97.708	32.094	489	65.125
079	Kliniken-Südostbayern	2	624	67.919	31.651	3.146	33.122

Kranken-haus-verbunds-ID	Krankenhausverbund	Standorte des Verbunds gesamt	Fälle				
			Betten	Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
074	Klinikum Vest GmbH	2	703	106.666	30.746	64	75.856
036	Christophorus-Kliniken GmbH	3	620	81.869	30.315	244	51.310
011	Kreiskrankenhaus Delitzsch	3	689	67.693	30.205	512	36.976
090	THÜRINGEN-KLINIKEN "GEORGIUS AGRICOLA" GMBH	4	836	68.141	30.067	657	37.417
080	Diakonie in Südwestfalen gGmbH	3	786	78.401	28.988	-	49.413
040	Marien Hospital Herne	2	575	87.315	28.620	326	58.369
050	Katholisches Klinikum Mainz	2	624	57.148	27.712	-	29.436
068	DONAUISAR Klinikum	2	605	114.125	27.557	353	86.215
042	KEM | Evang. Kliniken Essen-Mitte gGmbH	3	926	106.607	27.271	3.290	76.046
088	Oberhavel Kliniken GmbH	4	790	87.464	26.721	21.194	39.549
087	Klinikum Hersfeld-Rotenburg GmbH	5	853	92.357	26.145	346	52.354
071	Landkreis Neumarkt i.d.OP	2	550	75.601	25.812	6.948	42.841
029	Ev.-luth. Diakonissenanstalt	5	491	85.603	24.708	895	60.000
081	Theresienkrankenhaus und St. Hedwig-Klinik GmbH Mannheim	2	580	61.100	24.324	-	36.776
069	Klinikum Kulmbach	2	525	88.382	24.238	31	64.113
053	Kliniken des Bezirks Oberbayern	25	2.485	121.833	24.132	4.769	92.932
047	Ruppiner Kliniken	3	765	55.546	23.947	1.005	30.437
020	Caritas-Klinik Berlin	3	612	57.240	23.503	22.652	11.085
076	Bürgerhospital und Clementine Kinderhospital gGmbH	2	412	89.519	23.483	547	65.489
066	Klinikum Garmisch-Partenkirchen	2	505	89.133	23.078	29	66.026
092	DRK-Landesverband Mecklenburg-Vorpommern e.V.	4	494	58.122	23.053	-	29.851
070	Stiftung Kreuznacher Diakonie	2	501	82.849	22.485	-	60.364
075	Cusanus träger Gesellschaft Trier mbH	2	511	64.651	22.260	122	42.269

Kranken-haus-verbunds-ID	Krankenhausverbund	Standorte des Verbunds gesamt	Fälle				
			Betten	Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
095	Krankenhausträger: Katholisches Krankenhaus Hagen gem. GmbH	3	649	71.651	21.630	177	48.875
046	Carl-von-Basedow-Klinikum Saalekreis gGmbH	3	725	52.112	21.465	1.016	29.631
064	Ortenau Klinikum Lahr-Ettenheim	2	488	87.203	21.393	10	65.800
028	Segeberger Kliniken	5	573	38.898	21.236	240	17.422
073	Klinikum Westmünsterland GmbH	2	566	77.816	21.180	-	45.524
006	Klinikum Oberlausitzer Bergland gemeinnützige GmbH	2	1.022	49.460	21.109	311	28.040
082	Klinikum Weimar	2	561	52.791	20.642	289	31.860
043	Evangelisches Krankenhaus Herne	2	445	52.164	19.937	32.227	-
010	Elbe-Elster Klinikum GmbH	3	488	19.625	19.446	179	-
048	Klinikum Bielefeld	2	479	19.214	19.214	-	-
021	Caritas-Klinik Saarland	3	806	121.031	18.757	162	102.112
012	Muldentalkliniken GmbH	2	355	38.992	18.556	-	20.436
094	VAMED Klinik Geesthacht GmbH	7	711	31.845	17.283	385	14.424
001	Diakonie Dresden	2	320	42.755	17.210	54	25.491
025	Kreiskrankenhaus Freiberg	2	350	43.720	17.175	-	26.545
026	DRK-Kliniken Nordhessen Gemeinnützige GmbH	3	490	51.175	15.966	415	34.794
093	DRK Krankenhausgesellschaft mbH Rheinland-Pfalz	2	323	39.955	14.735	201	25.019
034	AWO Landesverband Sachsen-Anhalt e.V.	4	1.098	30.088	13.878	1.663	14.547
009	Städtisches Krankenhaus Eisenhüttenstadt GmbH	3	1.062	25.420	10.776	799	13.845
054	Medizinische Einrichtungen des Bezirks Oberpfalz	5	678	183.101	10.665	836	163.056
078	Christophsbad GmbH & Co. Fachkrankenhaus KG	2	509	64.808	6.761	1.100	56.947
067	Bezirkskliniken Mittelfranken	3	528	141.864	5.916	608	135.340

Kranken-haus-verbunds-ID	Krankenhausverbund	Standorte des Verbunds gesamt	Fälle				
			Betten	Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
091	ACURA Kliniken	3	295	20.748	5.312	463	14.973
084	MEDIAN Kliniken	16	958	13.203	3.610	0	374
022	SCIVIAS Caritas gGmbH	2	115	9.602	1.569	151	7.882
013	Fachkrankenhaus Bethanien (AGAPLESION)	3	168	5.322	1.473	410	3.439
097		0	-	-	-	-	-
098		0	-	-	-	-	-
099		0	-	-	-	-	-
100		0	-	-	-	-	-

Quelle: Rene Schubert, 08.10.2021

Tabelle 4: Klinikverbünde

Anhang B - Zuordnung der Einrichtungen zu den Klinikenverbünden

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
001	Diakonissenkrankenhaus Dresden	Sachsen	220	30.017	13.124	0	16.893
001	Krankenhaus Emmaus Niesky	Sachsen	100	12.738	4.086	54	8.598
002	Städtisches Klinikum Dresden - Standort Friedrichstadt	Sachsen	943	131.185	34.475	2.059	94.651
002	Städtisches Klinikum Dresden - Standort Neustadt	Sachsen	358	47.667	16.948	0	30.719
002	Städtisches Klinikum Dresden - Standort Weißer Hirsch	Sachsen	172	7.297	4.425	273	2.599
003	ELBLANDKLINIKEN Stiftung; Co. KG, ELBLANDKLINIKUM Radebeul	Sachsen	345	41.721	11.828	170	29.723
003	ELBLANDKLINIKEN Stiftung; Co. KG, ELBLANDKLINIKUM Riesa	Sachsen	330	63.093	16.400	137	46.556
003	ELBLANDKLINIKEN Stiftung; Co. KG, ELBLANDKLINIKUM Meißen	Sachsen	355	48.035	14.623	53	33.359
004	Helios Klinikum Pforzheim GmbH	Baden-Württemberg	500	79.668	24.767		54.901
004	HELIOS Klinik für Herzchirurgie Karlsruhe	Baden-Württemberg	89	2.512	2.077		435
004	Helios Klinik Rottweil	Baden-Württemberg	275	27.998	10.743		17.255
004	HELIOS Rosmann Klinik Breisach	Baden-Württemberg	123	17.337	4.467		12.870
004	HELIOS Klinik Müllheim	Baden-Württemberg	150	26.121	7.232		18.889
004	HELIOS Klinik Titisee-Neustadt	Baden-Württemberg	151	26.294	7.647		18.647
004	Helios Spital Überlingen GmbH	Baden-Württemberg	170	31.126	8.709		22.417
004	HELIOS Klinik Miltenberg	Bayern	8	19	19		
004	Helios Klinik Erlenbach	Bayern	267	32.758	14.059		18.699
004	Helios Klinikum München West	Bayern	412	52.870	22.946		29.924
004	Helios Klinik München Perlach	Bayern	150	16.918	6.611		10.307
004	Helios Amper-Klinikum Dachau	Bayern	441	49.694	21.943	240	27.511
004	Helios Amper-Klinik Indersdorf	Bayern	35	5.998	709		5.289
004	HELIOS Kliniken Bad Grönenbach GmbH/ Akutpsychosomatik	Bayern	0	0			
004	Helios Frankenwaldklinik Kronach	Bayern	282	23.766	11.220		12.546
004	HELIOS Klinik Volkach	Bayern	32	2.758	2.552		206
004	Helios St. Elisabeth-Krankenhaus Bad Kissingen	Bayern	225	20.401	10.397		10.004

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
004	Helios OrthoClinic Hammelburg	Bayern	50	6.185	2.762		3.423
004	Helios Klinikum Berlin-Buch	Berlin	1096	164.612	51.394	1.462	111.756
004	HELIOS Klinikum Emil von Behring GmbH	Berlin	507	61.847	20.947	92	40.808
004	HELIOS Klinikum Bad Saarow	Brandenburg	583	62.795	29.360		33.435
004	HELIOS Mariahilf Klinik Hamburg	Hamburg	176	44.841	13.436		31.405
004	Helios ENDO-Klinik Hamburg	Hamburg	204	7.509	7.509		
004	Helios St. Elisabeth Klinik Hünfeld	Hessen	158	19.465	8.035		11.430
004	HELIOS Klinik Oberwald Grebenhain	Hessen	68	3.180	3.180		
004	DKD HELIOS Klinik Wiesbaden	Hessen	138	26.260	5.111	4.155	16.994
004	HELIOS Dr. Horst-Schmidt-Kliniken Wiesbaden	Hessen	55	367	236	107	24
004	HELIOS Aukamm-Klinik Wiesbaden GmbH	Hessen	54	1.741			
004	HELIOS Dr. Horst-Schmidt-Kliniken Wiesbaden	Hessen	1027	150.998	42.903	1.170	106.925
004	HELIOS Klinik Bad Schwalbach	Hessen	110	1.274	1.274		
004	HELIOS Klinik Idstein	Hessen	80	13.051	4.477		8.574
004	HELIOS Klinik für Kinder und Jugendpsychiatrie Psychotherapie und Psychosomatik Tagesklinik Greifswald	Mecklenburg-Vorpommern	13	64		64	
004	HELIOS Psychiatrische Tagesklinik und Institutsambulanz Ribnitz-Damgarten	Mecklenburg-Vorpommern	17	116		116	
004	Helios Hanseklinikum Stralsund	Mecklenburg-Vorpommern	467	52.038	21.798	1.604	28.636
004	HELIOS Hanseklinikum Stralsund	Mecklenburg-Vorpommern	198	2.733	2.733		
004	HELIOS Tagesklinik für Psychiatrie und Psychotherapie in der Innenstadt von Stralsund	Mecklenburg-Vorpommern	23	134		134	
004	HELIOS Tagesklinik und Institutsambulanz für Psychiatrie und Psychotherapie Grimmen	Mecklenburg-Vorpommern	15	98		98	
004	HELIOS Psychiatrische Tagesklinik und Institutsambulanz in Bergen	Mecklenburg-Vorpommern	22	132		132	
004	Helios Kliniken Schwerin	Mecklenburg-Vorpommern	1064	116.620	50.100	1.437	65.083
004	Helios Kliniken Schwerin - Psychiatrie	Mecklenburg-Vorpommern	468	16.478	4.031	990	11.457
004	Helios Klinik Leezen GmbH: Akutbereich, enthalten sind nur die Daten der Patientinnen/Patienten der besonderen Einrichtung, ohne Patientinnen/Patienten aus dem Reha-Bereich	Mecklenburg-Vorpommern	180	1.305	1.305		

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
004	Helios Kliniken Schwerin - Tagesklinik allgemeine Psychiatrie Ludwigslust	Mecklenburg-Vorpommern	16	107		107	
004	Helios Kliniken Schwerin Tagesklinik für Kinder - und Jugendpsychiatrie Ludwigslust	Mecklenburg-Vorpommern	0	59		59	
004	Helios Kliniken Schwerin - Tagesklinik für Psychiatrie Sternberg	Mecklenburg-Vorpommern	14	84		84	
004	Helios Kliniken Schwerin - Tagesklinik für Kinder- und Jugendpsychiatrie	Mecklenburg-Vorpommern	12	56		56	
004	Helios Klinik Wesermarsch	Niedersachsen	98	13.630	6.251		7.379
004	Helios Klinik Cuxhaven GmbH	Niedersachsen	196	34.046	10.731		23.315
004	HELIOS Seehospital Sahlenburg	Niedersachsen	65	13.678	3.049		10.629
004	Helios Klinik Wittingen GmbH	Niedersachsen	35	7.830	2.207		5.623
004	Helios Klinikum Uelzen GmbH	Niedersachsen	316	39.135	17.036		22.099
004	Helios Klinikum Hildesheim GmbH	Niedersachsen	579	106.534	26.758		79.776
004	Helios Lungenklinik Diekholzen	Niedersachsen	0	0			
004	Helios Kliniken Mittelweser	Niedersachsen	285	40.425	15.734		24.691
004	Helios Kliniken Mittelweser	Niedersachsen	63	3.285	1.904		1.381
004	HELIOS Albert-Schweitzer-Klinik Northeim	Niedersachsen	210	25.434	10.745		14.689
004	Helios Klinik Herzberg/Osterode	Niedersachsen	214	25.638	10.663		14.975
004	HELIOS Klinik Bad Gandersheim	Niedersachsen	93	7.609	2.807		4.802
004	Helios Klinikum Salzgitter GmbH	Niedersachsen	307	47.817	16.531		31.286
004	HELIOS St. Marienberg Klinik Helmstedt	Niedersachsen	315	33.252	15.178		18.074
004	HELIOS Klinikum Gifhorn GmbH	Niedersachsen	370	43.365	20.662		22.703
004	Helios Klinikum Warburg GmbH	Nordrhein-Westfalen	139	28.829	7.266		21.563
004	HELIOS Klinikum Wuppertal GmbH Herzzentrum, Standort Elberfeld	Nordrhein-Westfalen	150	12.289	6.795		5.494
004	HELIOS Universitätsklinikum Wuppertal GmbH	Nordrhein-Westfalen	923	174.256	45.506	364	128.386
004	Helios Universitätsklinikum Wuppertal -Schmerzklinik Bergisch Land	Nordrhein-Westfalen	5	478		376	102
004	Helios Klinikum Niederberg	Nordrhein-Westfalen	473	52.980	18.490	143	34.347
004	HELIOS St. Josefs-Hospital Bochum-Linden	Nordrhein-Westfalen	181	12.782	5.364	160	7.258
004	HELIOS St. Elisabeth Klinik Oberhausen	Nordrhein-Westfalen	199	37.179	10.035		27.144

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
004	Helios St. Vincenz Klinik	Nordrhein-Westfalen	0	0			
004	Helios Marien Klinik	Nordrhein-Westfalen	389	29.184	7.172	531	21.481
004	Helios St. Johannes Klinik	Nordrhein-Westfalen	645	106.214	25.155		81.059
004	Helios Klinikum Krefeld	Nordrhein-Westfalen	1002	152.706	51.118	2.807	98.781
004	Helios Cäcilien-Hospital Hüls	Nordrhein-Westfalen	170	9.231	5.578	170	3.483
004	HELIOS Klinik Lengerich	Nordrhein-Westfalen	171	30.660	8.132		22.528
004	Helios Klinik Wipperfürth	Nordrhein-Westfalen	131	20.050	7.430		12.620
004	HELIOS Klinikum Siegburg	Nordrhein-Westfalen	361	48.436	16.900		31.536
004	Helios Klinik Attendorn	Nordrhein-Westfalen	298	27.680	9.554	205	17.921
004	HELIOS Klinikum Schwelm	Nordrhein-Westfalen	401	57.817	17.646	250	39.921
004	Helios Weißeritztal Kliniken, Klinikum Freital	Sachsen	280	43.998	14.378	92	29.528
004	Helios Weißeritztal-Kliniken, Klinik Dippoldiswalde	Sachsen	60	12.394	2.320	0	10.074
004	Helios Klinikum Pirna	Sachsen	390	49.837	18.676	130	31.031
004	Helios Park-Klinikum Leipzig	Sachsen	796	63.792	14.087	549	49.156
004	HELIOS Klinik Schkeuditz GmbH	Sachsen	150	26.190	7.077		19.113
004	HELIOS Klinik Leisnig	Sachsen	175	26.012	9.172	291	16.549
004	Helios Klinikum Aue	Sachsen	580	66.505	27.258	1.130	38.117
004	Helios Vogtland-Klinikum Plauen	Sachsen	653	119.080	27.003	369	91.708
004	Helios Klinik Lutherstadt Eisleben	Sachsen-Anhalt	247	17.634	9.684	176	7.774
004	Helios Klinik Hettstedt	Sachsen-Anhalt	272	21.247	10.378	158	10.711
004	Helios Klinik Köthen GmbH	Sachsen-Anhalt	248	25.702	11.533		14.169
004	HELIOS Klinik Sangerhausen	Sachsen-Anhalt	268	40.519	13.710	125	26.684
004	HELIOS Fachklinik Vogelsang - Gommern	Sachsen-Anhalt	160	13.636	5.478		8.158
004	HELIOS Klinik Zerbst/Anhalt	Sachsen-Anhalt	160	14.191	8.618		5.573
004	HELIOS Klinik Jerichower Land	Sachsen-Anhalt	241	22.596	12.073	107	10.416
004	HELIOS Bördeklinik	Sachsen-Anhalt	184	15.983	10.035		5.948
004	Helios Agnes Karll Krankenhaus Bad Schwartau	Schleswig-Holstein	77	4.676	4.676		
004	HELIOS Klinik Kiel	Schleswig-Holstein	34	3.727	2.780		947
004	HELIOS Klinik Schleswig GmbH	Schleswig-Holstein	327	43.622	15.118	24	28.480

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
004	HELIOS Fachklinik, Klinik für Erwachsenenpsychiatrie und Psycho-somatische Medizin	Schleswig-Holstein	327	15.982	1.927	2	14.053
004	HELIOS Klinik für Kinder- und Jugendpsychiatrie und -Psychothe-rapie sowie Tagesklinik Baumhaus Schleswig	Schleswig-Holstein	307	1.166	1.126	40	
004	HELIOS Tagesklinik Psychiatrie (Erwachsene)	Schleswig-Holstein	20	128		128	
004	HELIOS Klinik für Kinder- und Jugendpsychiatrie und -Psychothe-rapie, Tagesklinik Baumhaus Husum	Schleswig-Holstein	25	36		36	
004	Helios Fachkliniken Hildburghausen/Psychiatrische Tagesklinik Sonneberg	Thüringen	21	2.580		134	2.446
004	Helios Fachkliniken Hildburghausen/Psychiatrische Tagesklinik Suhl	Thüringen	19	2.948		137	2.811
004	HELIOS Klinikum Meiningen	Thüringen	441	54.975	18.888	699	35.388
004	Helios Fachkliniken Hildburghausen/Psychiatrische Tagesklinik Meiningen	Thüringen	21	3.689		170	3.519
004	Helios Fachkliniken Hildburghausen	Thüringen	347	24.807	5.652	229	18.926
004	Helios Fachkliniken Hildburghausen/ Psychiatrische Tagesklinik Ilmenau	Thüringen	22	2.815		191	2.624
004	HELIOS Klinikum Erfurt	Thüringen	1261	169.633	54.091	1.220	114.322
004	HELIOS Klinik Blankenhain	Thüringen	125	12.290	6.811	95	5.384
004	HELIOS Klinik Bleicherode GmbH	Thüringen	101	8.107	3.066		5.041
004	Helios Klinikum Gotha	Thüringen	341	43.195	19.974	202	23.019
005	Asklepios Fachkliniken München-Gauting	Bayern	268	12.227	9.000	818	2.409
005	Asklepios Stadtklinik Bad Tölz	Bayern	270	34.337	11.664		22.673
005	Asklepios Klinik Lindau	Bayern	110	16.918	6.386		10.532
005	Asklepios Orthopädische Klinik Lindenlohe	Bayern	110	12.196	4.088		8.108
005	Asklepios Klinik Oberviechtach	Bayern	40	7.278	1.980		5.298
005	Asklepios Klinikum Bad Abbach GmbH	Bayern	200	27.337	7.302		20.035
005	Asklepios Klinik Burglengenfeld	Bayern	120	18.067	6.901		11.166
005	Asklepios Fachklinikum Lübben TK Cottbus	Brandenburg	19	366		100	266
005	Asklepios Fachklinikum Lübben TK Vetschau	Brandenburg	13	952		104	848
005	Asklepios Fachklinikum Teupitz TK Schönefeld - Waßmannsdorf	Brandenburg	10	1.372		74	1.298

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
005	Asklepios Fachklinikum Brandenburg TK Potsdam	Brandenburg	16	485		87	398
005	Asklepios Fachklinikum Brandenburg TK Teltow	Brandenburg	18	1.998		125	1.873
005	Asklepios Fachklinikum Brandenburg TK Werder	Brandenburg	18	2.051		114	1.937
005	Asklepios Fachklinikum Brandenburg TK Rathenow	Brandenburg	15	1.890		78	1.812
005	Asklepios Fachklinikum Brandenburg	Brandenburg	388	19.354	6.241	256	12.857
005	Asklepios Fachklinikum Brandenburg TK Brandenburg an der Ha-vel	Brandenburg	18	134		134	
005	Asklepios Fachklinikum Teupitz TK Ludwigsfelde	Brandenburg	18	1.084		100	984
005	Asklepios Fachklinikum Teupitz TK Königs Wusterhausen	Brandenburg	18	2.066		124	1.942
005	Asklepios Fachklinikum Lübben TK Königs Wusterhausen	Brandenburg	12	599		74	525
005	Asklepios Fachklinikum Teupitz	Brandenburg	239	8.428	4.822		3.606
005	Asklepios Fachklinikum Lübben	Brandenburg	233	6.585	3.198	128	3.259
005	Asklepios Klinikum Uckermark GmbH	Brandenburg	460	118.392	17.303	2.546	98.543
005	Asklepios Klinik Birkenwerder	Brandenburg	151	26.674	4.429		22.245
005	Asklepios Klinik St. Georg	Hamburg	695	77.670	26.268	3.250	48.152
005	Asklepios Klinik Nord - TK Alsteror	Hamburg	24	219		219	
005	Asklepios Klinikum Harburg	Hamburg	868	86.667	31.223	1.341	54.103
005	Asklepios Klinikum Harburg - Wilhelmsburg	Hamburg	0	2.074		124	1.950
005	Asklepios Klinikum Harburg - Neugraben	Hamburg	0	1.089		23	1.066
005	Asklepios Klinik Wandsbek	Hamburg	553	59.429	20.094	417	38.918
005	Asklepios Klinik Nord - Wandsbek	Hamburg	130	4.632	1.840	230	2.562
005	Asklepios Klinik Nord - TK Horn	Hamburg	25	1.834		297	1.537
005	Asklepios Klinik Barmbek	Hamburg	640	83.556	35.246	25	48.285
005	Asklepios Klinik Nord - TK Steilshoop	Hamburg	25	1.631		248	1.383
005	Asklepios Klinik Nord - TK Volksd.	Hamburg	30	2.224		283	1.941
005	Asklepios Klinik Nord - Heidberg	Hamburg	664	117.873	31.667	2.296	83.910
005	Asklepios Klinik Nord - Ochsenzoll	Hamburg	624	26.481	9.563	1.090	15.828
005	Asklepios Klinikum Harburg - Osdorf	Hamburg	0	456		44	412
005	Asklepios Westklinikum Hamburg GmbH	Hamburg	517	29.040	14.676	1.196	13.168

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
005	Asklepios Klinik Altona	Hamburg	657	79.963	34.372		45.591
005	Asklepios Schwalm-Eder-Kliniken GmbH, Klinikum Melsungen	Hessen	76	12.885	3.340	34	9.511
005	Asklepios Schwalm-Eder-Kliniken GmbH, Klinikum Schwalmstadt	Hessen	204	29.624	11.022	34	18.568
005	Asklepios Stadtklinik Bad Wildungen	Hessen	175	26.001	8.607		17.394
005	Asklepios Fachklinik Fürstenhof GmbH	Hessen	15	212	212		
005	Asklepios Klinik Lich GmbH	Hessen	244	61.320	12.852		48.468
005	Asklepios Neurologische Klinik Falkenstein	Hessen	50	313			
005	Asklepios Klinik Langen	Hessen	433	19.949			
005	Asklepios Klinik Seligenstadt	Hessen	265	23.496			
005	Asklepios Neurologische Klinik Bad Salzhausen	Hessen	96	2.355			
005	Asklepios Schlossberg Klinik	Hessen	110	493			
005	Asklepios Paulinen Klinik Wiesbaden	Hessen	314	29.267			
005	Asklepios Paulinen Klinik Wiesbaden TK Biebrich	Hessen	15	321			
005	Asklepios Paulinen Klinik Wiesbaden TK Rüdesheim	Hessen	45	750			
005	Asklepios Klinik Pasewalk	Mecklenburg-Vorpommern	222	22.654	11.899	149	10.606
005	AKG Klinik Parchim GmbH	Mecklenburg-Vorpommern	135	22.420	7.683		14.737
005	Asklepios Fachklinikum Göttingen	Niedersachsen	436	16.003	5.172	365	10.466
005	Asklepios Fachklinikum Göttingen - TK Friedländer Weg	Niedersachsen	20	161		161	
005	Asklepios Fachklinikum Tiefenbrunn	Niedersachsen	211	992	992		
005	Asklepios Harzklinik Goslar	Niedersachsen	269	36.905	15.152		21.753
005	Asklepios Harzklinik Bad Harzburg	Niedersachsen	66	12.646	2.418		10.228
005	Asklepios Harzklinik Clausthal-Zellerfeld	Niedersachsen	54	1.395	512		883
005	Asklepios Kliniken Schildautal	Niedersachsen	319	17.052	10.468		6.584
005	Asklepios Fachklinikum Göttingen - TK Seesen	Niedersachsen	16	112		112	
005	Asklepios Klinik Sankt Augustin GmbH	Nordrhein-Westfalen	206	64.473	7.206	693	56.574
005	Asklepios Südpfalzklinik Germersheim	Rheinland-Pfalz	128	13.600			
005	Asklepios Südpfalzklinik Kandel	Rheinland-Pfalz	188	11.535			
005	Asklepios-ASB Klinik Radeberg	Sachsen	145	18.056	5.776	0	12.280
005	Fachkrankenhaus Kreischa Neurologie	Sachsen	150	1.262	1.262	0	0

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
005	Neurologisches Fachkrankenhaus Zscheckwitz	Sachsen	15	8	8	0	0
005	Asklepios Orthopädische Klinik Hohwald	Sachsen	105	9.568	3.809	0	5.759
005	Asklepios Fachklinikum Wiesen	Sachsen	166	4.108	1.724	127	2.257
005	Asklepios Klinik Weißenfels	Sachsen-Anhalt	410	41.461	14.660		26.801
005	Asklepios Klinik Bad Oldesloe	Schleswig-Holstein	173	15.592	6.046	151	9.395
005	Asklepios Nordseeklinik Westerland/Sylt	Schleswig-Holstein	95	95		95	
005	Asklepios Fachklinikum Stadtroda TK Pößneck	Thüringen	31	5.365		229	5.136
005	Asklepios Fachklinikum Stadtroda TK Gera	Thüringen	19	1.998		76	1.922
005	Asklepios Fachklinikum Stadtroda	Thüringen	370	17.691	4.189	764	12.738
005	Asklepios Fachklinikum Stadtroda TK Greiz	Thüringen	22	4.893		128	4.765
006	Klinikum Oberlausitzer Bergland gemeinnützige GmbH	Sachsen	511	18.300	8.762	241	9.297
006	Klinikum Oberlausitzer Bergland gemeinnützige GmbH	Sachsen	511	31.160	12.347	70	18.743
007	Malteser Waldkrankenhaus St. Marien	Bayern	290	24.730	12.939		11.791
007	Malteser-Krankenhaus	Berlin	107	2.122	1.916	206	
007	Malteser Krankenhaus St. Johannes-Stift	Nordrhein-Westfalen	267	18.946	8.372	136	10.438
007	Malteser Krankenhaus St. Anna	Nordrhein-Westfalen	341	42.424	16.581		25.843
007	Malteser Krankenhaus St. Josefshospital Uerdingen	Nordrhein-Westfalen	262	18.732	9.324		9.408
007	Malteser Krankenhaus St. Hildegardis	Nordrhein-Westfalen	233	19.912			
007	Malteser Krankenhaus Seliger Gerhard Bonn/Rhein-Sieg	Nordrhein-Westfalen	381	58.635	12.607	160	45.868
007	Malteser Krankenhaus St. Johannes	Sachsen	160	18.021	7.529	91	10.401
007	Malteser Krankenhaus St. Carolus	Sachsen	120	13.594	5.356	670	7.568
007	Malteser Krankenhaus St. Franziskus-Hospital - Geriatrische Tagesklinik	Schleswig-Holstein	12	236		236	
007	Malteser Krankenhaus St. Franziskus-Hospital	Schleswig-Holstein	363	19.965	11.923	472	7.570
008	Sana Herzchirurgie Stuttgart GmbH	Baden-Württemberg	66	1.810	1.810		
008	Sana Klinik Bethesda Stuttgart gGmbH	Baden-Württemberg	150	9.864	4.792		5.072
008	Sana Klinikum Biberach	Baden-Württemberg	343	64.552	17.175		47.377
008	Sana Klinik Laupheim	Baden-Württemberg	78	20.573	3.034		17.539
008	Sana Klinik Riedlingen	Baden-Württemberg	54	13.895	2.498		11.397

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
008	Sana Kliniken Solln Sendling GmbH Umfirmierung im September 2018 in Sana Klinik München GmbH	Bayern	180	12.069	6.638		5.431
008	Sana Klinik Sendling GmbH	Bayern	58	1.701	1.701		
008	Sana-Klinik Nürnberg GmbH	Bayern	55	3.404	3.097		307
008	Sana Klinik Pegnitz GmbH	Bayern	117	11.449	5.952		5.497
008	Sana Kliniken des Landkreises Cham - Krankenhaus Cham	Bayern	200	37.873	12.940		24.933
008	Sana Kliniken des Landkreises Cham - Krankenhaus Roding	Bayern	90	10.686	4.258		6.428
008	Sana Kliniken des Landkreises Cham - Krankenhaus Bad Kötzting	Bayern	50	4.291	2.369		1.922
008	Sana Klinikum Hof	Bayern	465	49.449	23.022	347	26.080
008	Sana Klinikum Lichtenberg	Berlin	661	96.899	30.568	1.200	65.131
008	Sana-Herzzentrum Cottbus GmbH	Brandenburg	85	4.421	4.177		244
008	Sana Kliniken Sommerfeld	Brandenburg	263	8.170	7.498		672
008	Sana Krankenhaus Templin	Brandenburg	122	10.682	5.017		5.665
008	Sana Klinikum Offenbach GmbH	Hessen	926	119.910	38.683	463	80.764
008	Sana-Krankenhaus Rügen GmbH	Mecklenburg-Vorpommern	206	25.255	11.183		14.072
008	Sana HANSE-Klinikum Wismar- TK Gdb	Mecklenburg-Vorpommern	18	1.720		89	1.631
008	Sana HANSE-Klinikum Wismar- TK Gvm	Mecklenburg-Vorpommern	17	460		83	377
008	Sana HANSE-Klinikum Wismar GmbH	Mecklenburg-Vorpommern	419	46.243	18.402	469	27.372
008	Sana HANSE-Klinikum Wismar- TK Wis	Mecklenburg-Vorpommern	40	2.718		285	2.433
008	Gesundheitseinrichtungen Hameln-Pyrmont GmbH - Sana Klinikum Hameln-Pyrmont	Niedersachsen	402	63.469	22.257		41.212
008	Sana Kliniken Düsseldorf, Standort Benrath	Nordrhein-Westfalen	212	40.171	12.932		27.239
008	Sana Kliniken Düsseldorf, Standort Gerresheim	Nordrhein-Westfalen	278	47.039	11.269		35.770
008	Sana Krankenhaus Radevormwald	Nordrhein-Westfalen	140	17.836	4.848		12.988
008	Sana Fabricius-Klinik Remscheid GmbH	Nordrhein-Westfalen	105	2.651	2.169	121	361
008	Sana-Klinikum Remscheid GmbH	Nordrhein-Westfalen	531	70.388	23.795	507	46.086
008	Wedau Kliniken	Nordrhein-Westfalen	565	76.203	21.663	595	53.945
008	Sana-Krankenhaus Hürth	Nordrhein-Westfalen	140	16.716			
008	Sana Dreifaltigkeits-Krankenhaus Köln	Nordrhein-Westfalen	80	13.267			

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
008	Sana Kliniken Leipziger Land GmbH - Klinik Zwenkau	Sachsen	58	6.131	2.015	54	4.062
008	Sana Kliniken Leipziger Land GmbH - Klinikum Borna	Sachsen	422	97.024	25.023	719	71.282
008	Sana Kliniken Lübeck GmbH, Krankenhaus Süd	Schleswig-Holstein	389	41.016	17.840	3	23.173
008	Sana Kliniken Lübeck GmbH, Praxisklinik Travemünde	Schleswig-Holstein	28	1.238	1.196	42	
008	Sana Kliniken Ostholstein GmbH - Klinik Eutin	Schleswig-Holstein	197	34.021	11.190	3.186	19.645
008	Sana Kliniken Ostholstein GmbH, Klinik Middelburg	Schleswig-Holstein	100	1.689	1.387	302	
008	Sana Kliniken Ostholstein GmbH - Klinik Oldenburg	Schleswig-Holstein	151	19.402	6.011	443	12.948
008	Sana Kliniken Ostholstein GmbH - Inselklinik Fehmarn	Schleswig-Holstein	28	7.170	1.021		6.149
009	Städtisches Krankenhaus Eisenhüttenstadt GmbH	Brandenburg	354	218		218	
009	Städtisches Krankenhaus Eisenhüttenstadt GmbH	Brandenburg	354	1.051		166	885
009	Städtisches Krankenhaus Eisenhüttenstadt GmbH	Brandenburg	354	24.151	10.776	415	12.960
010	Elbe-Elster Klinikum GmbH Krankenhaus Finsterwalde	Brandenburg	188	5.488	5.440	48	
010	Elbe-Elster Klinikum GmbH Krankenhaus Elsterwerda	Brandenburg	147	5.839	5.708	131	
010	Elbe-Elster Klinikum GmbH Krankenhaus Herzberg	Brandenburg	153	8.298	8.298		
011	Kreiskrankenhaus Delitzsch GmbH - Standort Delitzsch	Sachsen	135	11.296	5.504		5.792
011	Kreiskrankenhaus Delitzsch GmbH - Standort Eilenburg	Sachsen	135	12.296	6.620		5.676
011	Klinikum Altenburger Land GmbH	Thüringen	419	44.101	18.081	512	25.508
012	Muldentalkliniken GmbH, Gemeinnützige Gesellschaft Standort Grimma	Sachsen	177	18.450	8.492		9.958
012	Muldentalkliniken GmbH, Gemeinnützige Gesellschaft Standort Wurzen	Sachsen	178	20.542	10.064		10.478
013	Tagesklinik Döbeln Fachkrankenhaus für Psychiatrie und Psycho-therapie Bethanien Hochweitzschen	Sachsen	22	186		186	
013	Fachkrankenhaus für Psychiatrie und Psychotherapie Bethanien Hochweitzschen	Sachsen	121	4.912	1.473		3.439
013	Tagesklinik Freiberg Fachkrankenhaus für Psychiatrie und Psycho-therapie Bethanien Hochweitzschen	Sachsen	25	224		224	
014	SRH Kurpfalzkrankenhaus Heidelberg GmbH	Baden-Württemberg	94	2.333	2.225	108	
014	SRH Krankenhaus Sigmaringen	Baden-Württemberg	380	55.319	15.930	88	39.301
014	SRH Fachkrankenhaus Neresheim GmbH	Baden-Württemberg	55	295	295		
014	SRH Klinikum Karlsbad-Langensteinbach GmbH	Baden-Württemberg	422	29.869	9.677	72	20.120

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
014	SRH Krankenhaus Oberndorf a.N.	Baden-Württemberg	120	24.764	6.129		18.635
014	SRH Krankenhaus Bad Saulgau	Baden-Württemberg	60	15.658	4.406	88	11.164
014	SRH Krankenhaus Pfullendorf	Baden-Württemberg	80	16.578	2.789	127	13.662
014	SRH Klinikum Burgenlandkreis GmbH, Standort Naumburg	Sachsen-Anhalt	458	36.811	14.778	345	21.688
014	SRH Klinikum Burgenlandkreis GmbH, Standort Zeitz	Sachsen-Anhalt	293	28.880	10.978	117	17.785
014	SRH Wald-Klinikum Gera GmbH	Thüringen	965	97.099	41.597	1.046	54.456
014	SRH Zentralklinikum Suhl GmbH	Thüringen	640	79.018	31.102	714	47.202
014	SRH Krankenhaus Waltershausen-Friedrichroda GmbH	Thüringen	185	28.667	9.812		18.855
015	Heinrich-Braun-Klinikum gemeinnützige GmbH, Standort Zwickau	Sachsen	825	75.120	34.808	2.167	38.145
015	Heinrich-Braun-Klinikum gemeinnützige GmbH, Standort Kirchberg	Sachsen	105	8.447	4.189		4.258
016	Vivantes Klinikum im Friedrichshain	Berlin	964	45.482	44.201	1.281	
016	Vivantes Klinikum im Friedrichshain - öB Fröbelstraße Prenzlauer Berg	Berlin	105	1.104	1.104		
016	Vivantes Klinikum Am Urban	Berlin	614	31.452	30.908	544	
016	Vivantes Wenckebach-Klinikum	Berlin	443	10.521	10.175	346	
016	Vivantes Auguste-Viktoria-Klinikum	Berlin	572	62.185	25.434	2.249	34.502
016	Vivantes Klinikum Neukölln	Berlin	1247	50.761	48.577	2.184	
016	Vivantes Ida-Wolff-Krankenhaus	Berlin	156	2.867	2.340	527	
016	Vivantes Klinikum Kaulsdorf	Berlin	434	16.821	16.271	550	
016	Vivantes Klinikum Kaulsdorf - ö.B. Mehrower Allee Mahrzahn	Berlin	20	2.963	2.485	478	
016	Vitanas Klinik & Tagesklinik für Geriatrie	Berlin	105	1.802	1.602	200	
016	Vivantes Humboldt-Klinikum	Berlin	640	26.960	26.169	791	
016	Vivantes Klinikum Spandau	Berlin	603	54.716	22.327	1.565	30.824
017	DRK Kliniken Berlin Köpenick	Berlin	525	66.804	22.664	179	43.961
017	DRK Kliniken Berlin Mitte	Berlin	259	34.821	10.893		23.928
017	DRK Kliniken Berlin Westend	Berlin	517	104.677	28.674	140	75.863
017	DRK Kliniken Berlin Wiegmann Klinik	Berlin	50	348	250	92	6
018	St. Hedwig-Krankenhaus Berlin	Berlin	427	41.368	13.336	706	27.326
018	Alexianer Krankenhaus Hedwigshöhe	Berlin	441	38.612	12.255	1.026	25.331

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
018	Alexianer St. Joseph-Krankenhaus Berlin-Weißensee	Berlin	361	17.703	4.404	939	12.360
018	Alexianer-Klinik Meerbusch GmbH	Nordrhein-Westfalen	14	5.494		191	5.303
018	Alexianer Krefeld GmbH - Krankenhaus Maria-Hilf	Nordrhein-Westfalen	554	37.188	15.984	476	20.728
018	Alexianer Tönisvorst GmbH - Krankenhaus Maria-Hilf	Nordrhein-Westfalen	62	11.925	2.697		9.228
018	Ludgerus-Kliniken Münster GmbH-Standort Raphaelsklinik	Nordrhein-Westfalen	275	28.371	11.942		16.429
018	Ludgerus-Kliniken Münster GmbH-Standort Clemenshospital	Nordrhein-Westfalen	405	50.638	17.525		33.113
018	Alexianer Krankenhaus Münster	Nordrhein-Westfalen	110	7.845	1.153	143	6.549
018	Alexianer Krankenhaus Köln	Nordrhein-Westfalen	189	14.668			
018	Alexianer Aachen GmbH	Nordrhein-Westfalen	260	14.816			
019	Immanuel Krankenhaus Berlin - Standort Buch	Berlin	85	24.300	2.235	42	22.023
019	Immanuel Krankenhaus Berlin - Standort Wannsee	Berlin	190	13.729	6.886	606	6.237
019	Tagesklinik Strausberg	Brandenburg	18	212		209	3
019	Tagesklinik Fürstenwalde	Brandenburg	20	267		267	
019	Immanuel Klinik Rüdersdorf	Brandenburg	414	37.856	12.430	359	25.067
019	Immanuel Klinikum Bernau Herzzentrum Brandenburg	Brandenburg	260	27.667	11.875	15.792	
019	Albertinen Krankenhaus	Hamburg	605	73.802	30.725		43.077
019	Albertinen Krankenhaus-Albertinen Haus	Hamburg	127	4.135	1.963	600	1.572
019	Alexius/Josef Krankenhaus - Tagesklinik St. Fabiola	Nordrhein-Westfalen	15	141		141	
019	Alexius/Josef Krankenhaus - Tagesklinik Benedikt	Nordrhein-Westfalen	15	216		216	
019	Alexius/Josef Krankenhaus/ Tagesklinik St. Anna	Nordrhein-Westfalen	12	91		91	
019	Alexius/Josef Krankenhaus	Nordrhein-Westfalen	333	42.250	4.809		37.441
019	Alexius/Josef Krankenhaus -Tagesklinik St. Bernhard	Nordrhein-Westfalen	20	123		123	
019	Alexius/Josef Krankenhaus / Tagesklinik St. Augustinus	Nordrhein-Westfalen	12	113		113	
019	Alexius/Josef Krankenhaus - Tagesklinik Luzia	Nordrhein-Westfalen	12	78		78	
020	Caritas-Klinik Maria Heimsuchung Berlin-Pankow	Berlin	245	36.352	14.196	22.156	
020	Caritas-Klinik Dominikus	Berlin	253	18.861	7.486	290	11.085
020	Caritas-Klinik St. Marien Brandenburg	Brandenburg	114	2.027	1.821	206	
021	CaritasKlinikum Saarbrücken Standort St. Theresia	Saarland	466	80.354	4.948	47	75.359
021	CaritasKlinikum Saarbrücken Standort St. Josef	Saarland	157	19.715	6.814	115	12.786

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
021	Caritas-Krankenhaus Lebach	Saarland	183	20.962	6.995		13.967
022	SCIVIAS Caritas gGmbH St. Valentinus Krankenhaus	Hessen	50	4.308	895		3.413
022	SCIVIAS Caritas gGmbH St. Valentinus-Krankenhaus	Hessen	65	5.294	674	151	4.469
023	Evangelische Elisabeth Klinik	Berlin	145	31.871	7.353		24.518
023	Evangelische Lungenklinik	Berlin	152	15.195	5.656		9.539
023	Evangelisches Geriatriezentrum Berlin gGmbH (EGZB)	Berlin	192	3.390	2.982	408	
023	Evangelisches Waldkrankenhaus Spandau	Berlin	493	83.751	21.141		62.610
023	Evangelisches Krankenhaus Hubertus	Berlin	200	20.007	6.457	154	13.396
023	Martin-Luther-Krankenhaus, Berlin	Berlin	260	16.284	14.918		1.366
023	Klinik Amsee GmbH	Mecklenburg-Vorpommern	50	3.026	3.026		
023	Paul Gerhardt Diakonie Krankenhaus und Pflege GmbH	Sachsen-Anhalt	306	38.945	17.307	78	21.560
024	Paracelsus Krankenhaus	Baden-Württemberg	65	2.804	2.005		799
024	Paracelsus Klinik München	Bayern	60	2.970	2.970		
024	Paracelsus-Klinik Bremen	Bremen	70	5.034	3.303		1.731
024	Paracelsus-Elena-Klinik	Hessen	120	2.701	2.281		420
024	Paracelsus-Nordseeklinik Helgoland	Niedersachsen	34	2.216	444		1.772
024	Paracelsus-Klinik am Silbersee	Niedersachsen	90	4.864	4.536		328
024	Paracelsus-Klinik Osnabrück	Niedersachsen	164	32.503	6.671		25.832
024	Paracelsus Klinik Düsseldorf Golzheim	Nordrhein-Westfalen	84	4.676	3.785		891
024	Klinikum Vest GmbH, Paracelsus-Klinik Marl	Nordrhein-Westfalen	343	38.366	11.525	64	26.777
024	Paracelsus-Klinik Hemer GmbH	Nordrhein-Westfalen	134	16.426			
024	Paracelsus-Klinik Bad Ems	Rheinland-Pfalz	140	7.973			
024	Paracelsus Klinik Zwickau	Sachsen	180	24.136	7.598	538	16.000
024	Paracelsus-Klinik Adorf/Schöneck -Standort Schöneck-	Sachsen	275	10.067	4.137		5.930
024	Paracelsus Klinik - Reichenbach	Sachsen	180	18.730	6.159	64	12.507
024	Paracelsus-Klinik Adorf/Schöneck -Standort Adorf -	Sachsen	275	9.755	4.926	13	4.816
025	Kreiskrankenhaus Freiberg	Sachsen	335	41.565	16.159		25.406
025	Kreiskrankenhaus Freiberg - Standort Mittweida	Sachsen	15	2.155	1.016		1.139

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
026	DRK-Kliniken Nordhessen Gemeinnützige GmbH Standort Wehl-heiden	Hessen	320	48.627	13.552	281	34.794
026	DRK-Kliniken Nordhessen Gemeinnützige GmbH Standort Betten-hausen	Hessen	70	1.251	1.251		
026	DRK-Kliniken Nordhessen Gemeinnützige GmbH Standort Kaufun-gen	Hessen	100	1.297	1.163	134	
027	UNIVERSITÄTSKLINIKUM Schleswig-Holstein, Campus Lübeck	Schleswig-Holstein	1035	205.114	54.733	1.360	149.021
027	UNIVERSITÄTSKLINIKUM Schleswig-Holstein, Campus Kiel	Schleswig-Holstein	1095	216.896	50.771	3.763	162.362
027	Tagesklinik für Psychiatrie und Psychosomatik	Schleswig-Holstein	0	186	57		
028	PRAXISKLINIK NORDERSTEDT	Schleswig-Holstein	19	1.375	1.213		162
028	SEGEBERGER KLINIKEN GMBH Am Kurpark	Schleswig-Holstein	230	11.840	8.006		3.834
028	AK SEGEBERGER KLINIKEN GMBH	Schleswig-Holstein	192	24.152	10.894	102	13.156
028	Neurologisches Zentrum	Schleswig-Holstein	101	1.393	1.123		270
028	Psychiatrisches Krankenhaus Rickling (TK Bad Segeberg)	Schleswig-Holstein	31	138		138	
029	Diakonissenkrankenhaus Flensburg	Schleswig-Holstein	400	84.828	24.708	120	60.000
029	Ev.-luth. Diakonissenanstalt Psychiatrische Tagesklinik für Ältere	Schleswig-Holstein	19	136		136	
029	Ev.-luth. Diakonissenanstalt Tagesklinik für Psychosomatik	Schleswig-Holstein	15	154		154	
029	Ev.-luth. Diakonissenanstalt Kinder- und Jugendpsychiatrie	Schleswig-Holstein	25	109		109	
029	Ev.-luth. Diakonissenanstalt Psychiatrische Tagesklinik	Schleswig-Holstein	32	376		376	
030	AMEOS Klinikum Kaiserstuhl	Baden-Württemberg	55	1.349	1.349		
030	AMEOS Klinikum Inntal	Bayern	60	493	493		
030	AMEOS Klinikum Mitte Bremerhaven	Bremen	182	7.676	7.676		
030	AMEOS Klinikum Am Bürgerpark Bremerhaven	Bremen	215	10.327	10.327		
030	AMEOS Klinikum Dr. Heines Bremen	Bremen	230	2.667	2.436	231	
030	AMEOS Tagesklinik für Psychiatrie und Psychotherapie	Mecklenburg-Vorpommern	14	76		76	
030	AMEOS Klinikum Ueckermünde	Mecklenburg-Vorpommern	217	7.278	7.194	84	
030	AMEOS Klinikum Anklam	Mecklenburg-Vorpommern	101	5.484	5.370	114	
030	AMEOS Klinikum Seepark Geestland	Niedersachsen	252	7.627	7.499		128
030	AMEOS Klinikum Alfeld	Niedersachsen	133	13.037	5.252		7.785
030	AMEOS Klinikum Hildesheim	Niedersachsen	475	5.844	5.226	618	

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
030	AMEOS Klinikum Hameln	Niedersachsen	53	456	318	138	
030	AMEOS Klinikum Osnabrück	Niedersachsen	420	13.009	6.041	321	6.647
030	AMEOS Klinikum Bad Salzuflen	Nordrhein-Westfalen	131	1.544	1.382	162	
030	AMEOS Klinikum Bernburg	Sachsen-Anhalt	245	19.566	10.668		8.898
030	AMEOS Klinikum Aschersleben-Staßfurt GmbH	Sachsen-Anhalt	250	25.917	13.148	257	12.512
030	AMEOS Klinikum Halberstadt	Sachsen-Anhalt	453	43.981	19.539		24.442
030	AMEOS Klinikum Schönebeck	Sachsen-Anhalt	245	21.007	13.381	213	7.413
030	AMEOS Klinikum Haldensleben	Sachsen-Anhalt	219	15.158	10.362		4.796
030	AMEOS Klinikum Haldensleben	Sachsen-Anhalt	170	2.369	2.020	349	
030	AMEOS Klinikum Staßfurt	Sachsen-Anhalt	90	3.118	2.256	332	530
030	AMEOS Klinikum Lübeck	Schleswig-Holstein	276	3.345	778	128	2.439
030	AMEOS Klinikum Eutin	Schleswig-Holstein	276	1.864		216	1.648
030	AMEOS Klinikum Neustadt	Schleswig-Holstein	276	5.432	1.981		3.451
030	AMEOS Klinikum Oldenburg	Schleswig-Holstein	332	1.585	1.121		464
030	AMEOS Klinikum Oldenburg	Schleswig-Holstein	332	1.111		83	1.028
030	AMEOS Klinikum Heiligenhafen	Schleswig-Holstein	332	13.434	4.456	307	8.671
030	AMEOS Klinikum Kiel	Schleswig-Holstein	332	2.052	598	11	1.443
030	AMEOS Klinikum Preetz	Schleswig-Holstein	332	2.463	738	132	1.593
031	DIAKOVERE Friederikenstift	Niedersachsen	428	55.162	24.800		30.362
031	DIAKOVERE Henriettenstift	Niedersachsen	485	49.579	21.483	159	27.937
031	DIAKOVERE Annastift	Niedersachsen	161	39.233	6.356		32.877
032	KRH Klinikum Nordstadt	Niedersachsen	428	65.751	18.667		47.084
032	KRH Klinikum Siloah	Niedersachsen	555	26.626	26.233	393	
032	KRH Psychiatrie Langenhagen	Niedersachsen	184	17.076	2.300	257	14.519
032	KRH Geriatrie Langenhagen (Akut-Geriatrie)	Niedersachsen	40	1.005	1.005		
032	KRH Klinikum Agnes Karll Laatzen	Niedersachsen	246	32.079	11.218	10	20.851
032	KRH Klinikum Großburgwedel	Niedersachsen	223	37.714	13.003		24.711
032	KRH Klinikum Robert Koch Gehrden	Niedersachsen	358	53.481	21.275		32.206
032	KRH Klinikum Lehrte	Niedersachsen	158	348.410	8.411		339.999

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
032	KRH Psychiatrie Wunstorf	Niedersachsen	486	36.556	4.377	651	31.528
032	KRH Klinikum Neustadt am Rübenberge	Niedersachsen	275	45.162	17.784		27.378
033	AGAPLESION BETHANIEN KRANKENHAUS HEIDELBERG	Baden-Württemberg	105	1.826	1.826		
033	AGAPLESION BETHESDA KLINIK ULM gGmbH Akademisches Krankenhaus der Universität	Baden-Württemberg	90	1.593	1.593		
033	AGAPLESION DIAKONIEKLINIKUM HAMBURG	Hamburg	388	48.397	19.120	271	29.006
033	AGAPLESION DIAKONIE KLINIKEN KASSEL	Hessen	304	29.336	15.692	129	13.515
033	AGAPLESION Evangelisches Krankenhaus Mittelhessen	Hessen	168	33.951	9.783		24.168
033	AGAPLESION Pneumologische Klinik Waldhof Elgershausen	Hessen	95	4.748	3.310		1.438
033	AGAPLESION BETHANIEN KRANKENHAUS	Hessen	243	13.402			
033	AGAPLESION MARKUS KRANKENHAUS	Hessen	650	58.010	22.627	1.072	34.311
033	AGAPLESION ELISABETHENSTIFT EVANGELISCHES KRANKENHAUS	Hessen	401	28.805			
033	AGAPLESION DIAKONIEKLINIKUM ROTENBURG gemeinnützige GmbH	Niedersachsen	714	230.415	30.903	451	199.061
033	AGAPLESION EV. KLINIKUM SCHAUMBURG gemeinnützige GmbH Standort Stadthagen	Niedersachsen	0	0			
033	AGAPLESION EV. KLINIKUM SCHAUMBURG gemeinnützige GmbH	Niedersachsen	0	0			
033	AGAPLESION EV. KLINIKUM SCHAUMBURG	Niedersachsen	437	41.388	18.071		23.317
033	AGAPLESION EV. KLINIKUM SCHAUMBURG gemeinnützige GmbH Standort Rinteln	Niedersachsen	0	0			
033	AGAPLESION EV. BATHILDISKRANKENHAUS gemeinnützige GmbH	Niedersachsen	243	23.040	12.648	10.392	
033	AGAPLESION KRANKENHAUS NEU BETHLEHEM gGmbH	Niedersachsen	100	9.585	9.128	457	
033	AGAPLESION EVANGELISCHES KRANKENHAUS HOLZMINDEN	Niedersachsen	183	23.745	8.889		14.856
033	AGAPLESION BETHESDA KRANKENHAUS WUPPERTAL gemeinnützige GmbH	Nordrhein-Westfalen	363	50.735	17.713		33.022
033	AGAPLESION ALLGEMEINES KRANKENHAUS HAGEN gem. GmbH	Nordrhein-Westfalen	454	21.683			
033	AGAPLESION DIAKONIEKRANKENHAUS SEEHAUSEN	Sachsen-Anhalt	112	13.848	4.937		8.911
034	AWO Psychiatriezentrum	Niedersachsen	705	19.639	7.919	850	10.870

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
034	AWO Psychiatriezentrum Halle GmbH	Sachsen-Anhalt	100	3.120	1.332	409	1.379
034	AWO Krankenhaus Calbe	Sachsen-Anhalt	108	2.698	2.698		
034	AWO Fachkrankenhaus Jerichow	Sachsen-Anhalt	185	4.631	1.929	404	2.298
035	Harzklinikum Dorothea Christiane Erxleben, Standort Quedlinburg	Sachsen-Anhalt	394	53.071	16.559	290	36.222
035	Harzklinikum Dorothea Christiane Erxleben, Standort Tagesklinik Psychiatrie Quedlinburg	Sachsen-Anhalt	20	99		99	
035	Harzklinikum Dorothea Christiane Erxleben, Standort Ballenstedt	Sachsen-Anhalt	80	2.008	466		1.542
035	Harzklinikum Dorothea Christiane Erxleben, Standort Wernigerode	Sachsen-Anhalt	349	51.309	14.354	1.363	35.592
035	Harzklinikum Dorothea Christiane Erxleben GmbH, Standort Kinderklinik Wernigerode	Sachsen-Anhalt	32	5.259	1.915		3.344
035	Harzklinikum Dorothea Christiane Erxleben GmbH, Standort Blankenburg	Sachsen-Anhalt	154	3.209	1.113		2.096
035	Harzklinikum Dorothea Christiane Erxleben GmbH, Standort Tagesklinik Psychiatrie Blankenburg	Sachsen-Anhalt	25	137		137	
036	Christophorus-Kliniken Coesfeld – Dülmen – Nottuln, Standort Dülmen	Nordrhein-Westfalen	194	23.023	8.495		14.528
036	Christophorus-Kliniken Coesfeld – Dülmen – Nottuln, Standort Nottuln	Nordrhein-Westfalen	101	3.179	2.548	244	387
036	Christophorus-Kliniken Coesfeld – Dülmen – Nottuln, Standort Coesfeld	Nordrhein-Westfalen	325	55.667	19.272		36.395
037	LVR-Klinikum Düsseldorf - Kliniken der Heinrich-Heine-Universität Düsseldorf	Nordrhein-Westfalen	639	91.394	8.192	1.415	81.787
037	LVR-Klinik Langenfeld	Nordrhein-Westfalen	463	82.802	5.805	562	76.435
037	LVR-Klinik Mönchengladbach	Nordrhein-Westfalen	226	7.416	2.436	417	4.563
037	LVR-Klinik Viersen	Nordrhein-Westfalen	446	76.563	4.814	555	71.194
037	LVR-Klinik für Orthopädie Viersen	Nordrhein-Westfalen	78	11.220	2.619		8.601
037	LVR-Klinikum Essen	Nordrhein-Westfalen	320	83.418	3.149	1.041	79.228
037	LVR-Klinik Bedburg-Hau	Nordrhein-Westfalen	371	115.652	5.838	471	109.343
037	LVR-Klinik Köln	Nordrhein-Westfalen	526	34.970			
037	LVR-Klinik Düren	Nordrhein-Westfalen	531	26.171			
037	LVR-Klinik Bonn	Nordrhein-Westfalen	680	113.037	9.639	1.234	102.164
038	St. Vincenz-Krankenhaus	Nordrhein-Westfalen	582	112.237	31.858	4.539	75.840

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
038	St. Josefs-Krankenhaus	Nordrhein-Westfalen	208	33.094	8.869		24.225
039	Klinikum Dortmund Mitte	Nordrhein-Westfalen	971	223.047	42.223	180	180.644
039	Klinikum Dortmund Nord	Nordrhein-Westfalen	451	92.013	15.520		76.493
040	Marien Hospital Herne, Klinikum der Ruhr-Universität Bochum	Nordrhein-Westfalen	535	72.172	26.400	326	45.446
040	Marien Hospital Herne, Klinikum der Ruhr-Univ. Bochum, Klinik f. Kinderchirurgie	Nordrhein-Westfalen	40	15.143	2.220		12.923
041	LWL-Klinik Paderborn - Standort Agathastraße	Nordrhein-Westfalen	230	15.999	2.863	71	13.065
041	LWL-Klinik Paderborn - Standort Leostraße	Nordrhein-Westfalen	18	142		142	
041	LWL-Klinik Paderborn - Standort Mallinckrodtstraße	Nordrhein-Westfalen	12	93		93	
041	LWL-Klinik Marsberg (Kinder- u. Jugendpsychiatrie) - Standort Paderborn	Nordrhein-Westfalen	10	61		61	
041	LWL-Klinik Paderborn - Standort Salzkotten	Nordrhein-Westfalen	20	2.084		108	1.976
041	LWL-Klinikum Gütersloh	Nordrhein-Westfalen	439	23.463	5.088	530	17.845
041	LWL-Universitätsklink Hamm/ Tagesklinik Gütersloh	Nordrhein-Westfalen	10	209		26	183
041	LWL-Klinikum Tagesklinik Gütersloh	Nordrhein-Westfalen	0	0			
041	LWL-Universitätsklink Hamm/ Tagesklinik Rheda-Wiedenbrück	Nordrhein-Westfalen	10	2.200		69	2.131
041	LWL-Klinikum Tagesklinik Halle	Nordrhein-Westfalen	22	1.417		155	1.262
041	LWL-Klinikum Tagesklinik Halle	Nordrhein-Westfalen	0	0			
041	LWL-Klinik Marsberg - Standort Marsberg	Nordrhein-Westfalen	130	63.465	1.793	113	61.559
041	LWL-Klinik Marsberg (Kinder- u. Jugendpsychiatrie)	Nordrhein-Westfalen	83	16.130	833	3	15.294
041	LWL-Klinik Marsberg (Kinder- u. Jugendpsychiatrie) - Standort Höxter	Nordrhein-Westfalen	10	60		60	
041	LWL-Tagesklinik Dortmund	Nordrhein-Westfalen	12	98		98	
041	LWL-Klinik Dortmund Psychiatrie - Psychotherapie - Psychosomatische Medizin - Rehabilitation - Prävention	Nordrhein-Westfalen	565	27.034	6.417	1.290	19.327
041	LWL Klinik Dortmund - Elisabeth-Klinik -	Nordrhein-Westfalen	35	2.091	374		1.717
041	LWL-Tagesklinik Dortmund	Nordrhein-Westfalen	45	7.707	6.417	1.290	
041	LWL-Tagesklinik Brackel	Nordrhein-Westfalen	0	7.707	6.417	1.290	
041	LWL-Tagesklinik Lünen	Nordrhein-Westfalen	0	7.707	6.417	1.290	
041	LWL Klinik Marl-Sinsen Tagesklinik Herne	Nordrhein-Westfalen	0	77		77	

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
041	LWL-Universitätsklinikum Bochum	Nordrhein-Westfalen	219	100.325	2.132	523	97.670
041	LWL Klinik Marl-Sinsen Tagesklinik Recklinghausen	Nordrhein-Westfalen	0	2.169		61	2.108
041	LWL-Klinik Herten	Nordrhein-Westfalen	226	76.213	2.360	468	73.385
041	LWL-Klinik Herten - Tagesklinik Haltern	Nordrhein-Westfalen	20	4.639		114	4.525
041	LWL-Klinik Marl-Sinsen, Haardklinik; Kinder- und Jugendpsychiatrie – Psychotherapie –Psychosomatik	Nordrhein-Westfalen	119	6.307	1.445	7	4.855
041	LWL Klinik Marl-Sinsen Tagesklinik Bottrop	Nordrhein-Westfalen	0	578		67	511
041	LWL-Klinik Herten - Tagesklinik Dorsten	Nordrhein-Westfalen	20	2.849		120	2.729
041	LWL Klinik Marl-Sinsen Tagesklinik Borken	Nordrhein-Westfalen	0	582		80	502
041	LWL-Klinik Münster	Nordrhein-Westfalen	376	24.771	4.852	606	19.313
041	LWL-Universitätsklinik Hamm/ Tagesklinik Warendorf	Nordrhein-Westfalen	12	731			
041	LWL-Klinik Lengerich Standort Rheine	Nordrhein-Westfalen	60	7.279			
041	LWL Klinik Marl-Sinsen Tagesklinik Gronau	Nordrhein-Westfalen	0	213			
041	LWL Klinik Marl-Sinsen Tagesklinik Coesfeld	Nordrhein-Westfalen	0	992			
041	LWL-Klinik Lengerich	Nordrhein-Westfalen	279	15.925			
041	LWL-Klinik Marsberg - Standort Schmallenberg-Fredeburg	Nordrhein-Westfalen	15	101			
041	LWL-Klinik Hemer- Hans-Prinzhorn Klinik	Nordrhein-Westfalen	362	2.922			
041	LWL-Universitätsklinik Hamm	Nordrhein-Westfalen	122	10.131			
041	LWL-Tagesklinik Bergkamen	Nordrhein-Westfalen	0	7.707	6.417	1.290	
041	LWL-Universitätsklinik Hamm/ Tagesklinik Bergkamen	Nordrhein-Westfalen	12	476			
041	LWL-Klinik Dependance Unna	Nordrhein-Westfalen	0	7.707	6.417	1.290	
041	LWL-Tagesklinik Unna	Nordrhein-Westfalen	0	7.707	6.417	1.290	
041	LWL-Universitätsklinik Hamm/ Tagesklinik Soest	Nordrhein-Westfalen	12	1.098			
041	LWL-Klinik Lippstadt/Tagesklinik Psychiatrie Soest	Nordrhein-Westfalen	0	151			
041	LWL-Klinik Lippstadt/Tagesklinik Psychiatrie Lippstadt	Nordrhein-Westfalen	0	156			
041	LWL-Klinik für Psychiatrie und Psychotherapie Lippstadt	Nordrhein-Westfalen	147	21.771			
041	LWL-Klinik für Psychiatrie und Psychotherapie Warstein	Nordrhein-Westfalen	273	20.690			
041	LWL-Klinik Marsberg (Kinder- u. Jugendpsychiatrie) - Standort Meschede	Nordrhein-Westfalen	10	57			

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
042	KEM | Evang. Kliniken Essen-Mitte gGmbH, Standort Evang. Huyssens-Stiftung Essen-Huttrop	Nordrhein-Westfalen	509	54.296	17.082	1.889	35.325
042	Evang. Kliniken Essen-Mitte gGmbH, Standort Evang. Krankenhaus Essen-Werden	Nordrhein-Westfalen	230	35.715	5.560	574	29.581
042	KEM | Evang. Kliniken Essen-Mitte gGmbH, Standort Evang. Krankenhaus Essen-Steele	Nordrhein-Westfalen	187	16.596	4.629	827	11.140
043	Evangelisches Krankenhaus Herne - Standort Herne-Mitte	Nordrhein-Westfalen	310	44.830	14.691	30.139	
043	Evangelisches Krankenhaus Herne - Standort Eickel	Nordrhein-Westfalen	135	7.334	5.246	2.088	
044	Evangelisches Krankenhaus Königin Elisabeth Herzberge gGmbH	Berlin	717	48.164	17.449	2.076	28.639
044	Friedrich von Bodelschwingh-Klinik	Berlin	163	4.286	1.715	406	2.165
044	Evangelisches Klinikum Bethel gGmbH - Standort Johannesstift	Nordrhein-Westfalen	1460	31.184	15.586	389	15.209
044	Evangelisches Klinikum Bethel gGmbH Standort Bethel	Nordrhein-Westfalen	1460	114.737	31.722	3.731	79.284
044	Krankenhaus Mara gGmbH	Nordrhein-Westfalen	177	12.872	4.568		8.304
045	Klinikum Nürnberg I Standort Nord	Bayern	1292	133.552	52.023	2.590	78.939
045	Klinikum Nürnberg I Standort Süd	Bayern	933	139.865	46.879	318	92.668
046	Carl-von-Basedow-Klinikum Saalekreis gGmbH	Sachsen-Anhalt	725	41.209	16.709	449	24.051
046	Carl-von-Basedow-Klinikum Saalekreis gGmbH	Sachsen-Anhalt	725	10.825	4.756	489	5.580
046	Carl-von-Basedow-Klinikum Saalekreis gGmbH	Sachsen-Anhalt	724	78		78	
047	Ruppiner Kliniken	Brandenburg	719	55.271	23.947	887	30.437
047	psychiatrische Tagesklinik Kyritz	Brandenburg	28	157			
047	psychiatrische Tagesklinik Wittstock	Brandenburg	18	118		118	
048	Klinikum Bielefeld, Standort Rosenhöhe	Nordrhein-Westfalen	309	12.643	12.643		
048	Klinikum Bielefeld gem. GmbH, Standort Halle/Westfalen	Nordrhein-Westfalen	170	6.571	6.571		
049	Kliniken Köln gGmbH - Kinderkrankenhaus Amsterdamer Straße	Nordrhein-Westfalen	204	60.814	9.982	2	50.830
049	Kliniken der Stadt Köln gGmbH - Krankenhaus Holweide	Nordrhein-Westfalen	407	85.568	19.463		66.105
049	Kliniken der Stadt Köln gGmbH - Krankenhaus Merheim	Nordrhein-Westfalen	724	99.842	24.365		75.477
050	Katholisches Klinikum Mainz	Rheinland-Pfalz	624	57.148	27.712		29.436
050	Katholisches Klinikum Mainz, Standort: St. Hildegardis Krankenhaus	Rheinland-Pfalz	0	0			
051	Kliniken Böblingen	Baden-Württemberg	710	72.505	18.446		54.059

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
051	Kliniken Sindelfingen	Baden-Württemberg	710	66.880	17.706	466	48.708
051	Krankenhaus Herrenberg	Baden-Württemberg	150	33.096			
051	Krankenhaus Leonberg	Baden-Württemberg	239	49.619			
051	Kliniken Nagold	Baden-Württemberg	227	52.018			
051	Kreiskliniken Calw	Baden-Württemberg	199	33.675	9.040		24.635
052	Schwarzwald-Baar Klinikum Villingen-Schwenningen GmbH	Baden-Württemberg	796	163.413	40.138		123.275
052	Schwarzwald-Baar Klinikum Villingen-Schwenningen GmbH	Baden-Württemberg	250	42.463	8.132		34.331
053	kbo-Isar-Amper-Klinikum Atriumhaus	Bayern	52	5.510	592	300	4.618
053	kbo-Isar-Amper-Klinikum München-Nord	Bayern	202	6.130	1.530	335	4.265
053	kbo-Kinderzentrum München	Bayern	45	12.051	783		11.268
053	kbo-Isar-Amper-Klinikum Tagesklinik für Psychiatrie am kbo-Kinderzentrum München	Bayern	8	315		67	248
053	kbo - Heckscher-Klinikum gGmbH München	Bayern	75	6.959	1.099	118	5.742
053	kbo-Tagesklinik München Berg am Laim	Bayern	30	87		87	
053	kbo-Isar-Amper-Klinikum Fürstenfeldbruck	Bayern	103	5.882	1.650	322	3.910
053	kbo - Heckscher-Klinikum gGmbH, Abteilung Rottmannshöhe	Bayern	42	1.809	141		1.668
053	kbo-Lech-Mangfall-Klinik Peißenberg	Bayern	0	3.842		140	3.702
053	kbo-Lech-Mangfall-Klinik Garmisch-Partenkirchen	Bayern	100	5.384	1.067	182	4.135
053	kbo - Heckscher-Klinikum gGmbH, Abteilung Rosenheim	Bayern	30	1.285	129	32	1.124
053	kbo-Inn-Salzach-Klinikum Rosenheim	Bayern	0	289		289	
053	kbo-Inn-Salzach-Klinikum Freilassing	Bayern	80	3.133	1.385	139	1.609
053	kbo-Inn-Salzach-Klinikum Wasserburg	Bayern	506	7.701	1.786	128	5.787
053	kbo - Heckscher-Klinikum gGmbH, Abteilung Wasserburg	Bayern	20	252		90	162
053	kbo-Lech-Mangfall-Klinik Agatharied	Bayern	108	4.727	1.675	150	2.902
053	kbo-Isar-Amper-Klinikum Taufkirchen (Vils)	Bayern	200	5.988	2.565	46	3.377
053	kbo-Inn-Salzach-Klinikum Altötting	Bayern	0	1.244		148	1.096
053	kbo-Heckscher-Klinikum gGmbH, Abteilung Ingolstadt	Bayern	0	1.189		28	1.161
053	kbo-Isar-Amper-Kinikum Taufkirchen Pychiatrische Tagklinik Freising	Bayern	0	1.289		157	1.132

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
053	kbo-Isar-Amper-Klinikum Dachau	Bayern	20	1.498		140	1.358
053	kbo-Isar-Amper-Klinikum München-Ost	Bayern	790	38.131	8.551	1.547	28.033
053	kbo-Inn-Salzach-Klinikum Ebersberg	Bayern	0	78		78	
053	kbo-Lech-Mangfall-Klinik Landsberg am Lech	Bayern	74	6.372	1.179	191	5.002
053	kbo-Heckscher-Klinikum gGmbH, Abteilung Landsberg am Lech	Bayern	0	688		55	633
054	Tagesklinik für Kinder- und Jugendpsychiatrie, Amberg	Bayern	0	7.006		41	6.965
054	Psychiatrische Tagesklinik Amberg	Bayern	0	2.518		76	2.442
054	Tagesklinik für Kinder- und Jugendpsychiatrie, Weiden	Bayern	0	8.544			
054	Bezirksklinikum Regensburg	Bayern	628	143.278	10.015	486	132.777
054	Zentrum für Psychiatrie Cham	Bayern	50	21.755	650	233	20.872
055	Klinikum Passau	Bayern	645	79.490	36.940	224	42.326
055	Privatklinik Dr. Hellge	Bayern	25	1.148	1.051	97	
056	RoMed Klinikum Rosenheim	Bayern	622	81.901	30.732	1.602	49.567
056	RoMed Klinik Bad Aibling	Bayern	140	17.673	8.017		9.656
056	RoMed Klinik Prien am Chiemsee	Bayern	140	19.083	6.922		12.161
056	RoMed Klinik Wasserburg	Bayern	130	17.695	7.705		9.990
057	Kliniken Nordoberpfalz AG - Klinikum Weiden	Bayern	649	77.074	29.335	619	47.120
057	Kliniken Nordoberpfalz AG - Krankenhaus Vohenstrauß	Bayern	40	1.184	1.184		
057	Kliniken Nordoberpfalz AG - Krankenhaus Neustadt a.d. Waldnaab	Bayern	10	338	338		
057	Kliniken Nordoberpfalz AG - Krankenhaus Kemnath	Bayern	100	11.986	5.023		6.963
057	Kliniken Nordoberpfalz AG - Krankenhaus Tirschenreuth	Bayern	145	12.860	5.157		7.703
057	Kliniken Nordoberpfalz AG - Krankenhaus Waldsassen	Bayern	45	4.616			
058	Klinikum Bayreuth	Bayern	712	56.913	28.704	854	27.355
058	Klinik Hohe Warte	Bayern	336	21.685	9.788	476	11.421
059	Klinikum Bamberg - Betriebsstätte am Heinrichsdamm	Bayern	20	957	900	57	
059	Klinikum Bamberg - Betriebsstätte am Bruderwald	Bayern	768	92.089	40.240	1.232	50.617
059	Klinikum Bamberg - Betriebsstätte am Michelsberg	Bayern	225	12.154	3.395	406	8.353
060	GFO Kliniken Bonn - Betriebstätte St. Marien-Hospital	Nordrhein-Westfalen	308	94.523	20.091		74.432
060	GFO Kliniken Bonn - Betriebstätte St. Franziskus	Nordrhein-Westfalen	40	171	171		

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
060	GFO Kliniken Bonn - Betriebstätte St. Josef	Nordrhein-Westfalen	210	85.808	12.498		73.310
060	GFO Kliniken Bonn - Betriebsstätte CURA Krankenhaus Bad Honnef	Nordrhein-Westfalen	178	16.103	7.737		8.366
060	GFO Kliniken Troisdorf, Betriebsstätte St. Josef Troisdorf	Nordrhein-Westfalen	324	62.937	15.612		47.325
060	GFO Kliniken Troisdorf	Nordrhein-Westfalen	220	60.416	11.881		48.535
061	Kreiskrankenhaus Waldbröl	Nordrhein-Westfalen	320	35.373	9.770	150	25.453
061	Kreiskrankenhaus Gummersbach	Nordrhein-Westfalen	537	84.181	21.348	353	62.480
061	Zentrum für Seelische Gesundheit Marienheide -Klinik Marien-heide-	Nordrhein-Westfalen	177	10.154	2.933	182	7.039
062	Ermstalklinik Bad Urach	Baden-Württemberg	132	12.976	3.188		9.788
062	Klinikum am Steinenberg	Baden-Württemberg	546	113.825	29.559		84.266
063	Ortenau Klinikum Offenburg-Gengenbach Standort Ebertplatz	Baden-Württemberg	461	98.333	26.753	154	71.426
063	Ortenau Klinikum Offenburg-Gengenbach Standort St. Josefsklinik	Baden-Württemberg	171	27.940	6.087	18	21.835
063	Ortenau Klinikum Offenburg-Gengenbach Standort Gengenbach	Baden-Württemberg	104	10.251	2.140		8.111
064	Ortenau Klinikum Lahr-Ettenheim Standort Lahr	Baden-Württemberg	411	74.800	19.190	10	55.600
064	Ortenau Klinikum Lahr-Ettenheim Standort Ettenheim	Baden-Württemberg	77	12.403	2.203		10.200
065	Hegau-Bodensee-Klinikum Singen	Baden-Württemberg	448	78.453	22.824	28	55.601
065	Hegau-Bodensee-Klinikum Radolfzell	Baden-Württemberg	147	21.456	4.986		16.470
065	Klinikum Konstanz	Baden-Württemberg	380	78.249	17.339		60.910
065	Hegau-Bodensee-Klinikum Stühlingen	Baden-Württemberg	45	9.932	1.960		7.972
066	Klinikum Garmisch-Partenkirchen Aussenstelle Murnau	Bayern	75	7.373	2.749	29	4.595
066	Klinikum Garmisch-Partenkirchen - Haupthaus	Bayern	430	81.760	20.329		61.431
067	Psychiatrische Tagesklinik und Institutsambulanz Fürth des Klini-kums am Europakanal Erlangen,	Bayern	20	19.347		203	19.144
067	Klinikum am Europakanal	Bayern	488	107.570	5.916	212	101.442
067	Psychiatrische Tagesklinik mit Institutsambulanz Neustadt/Aisch	Bayern	20	14.947		193	14.754
068	DONAUISAR Klinikum Landau	Bayern	125	17.447	3.153	51	14.243
068	DONAUISAR Klinikum Deggendorf	Bayern	480	96.678	24.404	302	71.972
069	Klinikum Kulmbach	Bayern	500	87.719	23.702	31	63.986
069	Fachklinik Stadtsteinach	Bayern	25	663	536		127

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
070	Diakonie Krankenhaus kreuznacher diakonie	Rheinland-Pfalz	392	69.910	19.059		50.851
070	Diakonie Krankenhaus Standort Kirn	Rheinland-Pfalz	109	12.939	3.426		9.513
071	Klinikum Neumarkt	Bayern	500	67.346	24.222	283	42.841
071	Klinik Parsberg	Bayern	50	8.255	1.590	6.665	
072	Katholisches Klinikum Lünen/Werne GmbH Klinikum Lünen St.-Marien-Hospital	Nordrhein-Westfalen	570	68.173	21.902	489	45.782
072	Katholisches Klinikum Lünen/Werne GmbH St. Christophorus-Krankenhaus	Nordrhein-Westfalen	216	29.535	10.192		19.343
073	Klinikum Westmünsterland St. Agnes-Hospital Bocholt	Nordrhein-Westfalen	441	66.704	21.180		45.524
073	Klinikum Westmünsterland St. Vinzenz-Hospital Rhede	Nordrhein-Westfalen	125	11.112			
074	Klinikum Vest GmbH	Nordrhein-Westfalen	422	68.300	19.221		49.079
074	Marien-Hospital Marl	Nordrhein-Westfalen	281	38.366	11.525	64	26.777
075	Cusanus Krankenhaus Bernkastel-Kues	Rheinland-Pfalz	121	3.876	3.580		296
075	St. Elisabeth Krankenhaus Wittlich	Rheinland-Pfalz	390	60.775	18.680	122	41.973
076	Bürgerhospital und Clementine Kinderhospital gGmbH	Hessen	76	25.414	3.046	547	21.821
076	Bürgerhospital und Clementine Kinderhospital gGmbH Standort: Bürgerhospital Frankfurt	Hessen	336	64.105	20.437		43.668
077	medius KLINIK NÜRTINGEN	Baden-Württemberg	331	63.266	16.190		47.076
077	medius KLINIK KIRCHHEIM	Baden-Württemberg	487	39.744	14.474	167	25.103
077	medius KLINIK OSTFILDERN-RUIT	Baden-Württemberg	280	62.005	17.083		44.922
078	Klinikum Christophsbad Göppingen	Baden-Württemberg	491	60.066	6.761	948	52.357
078	Psychiatrische Tagesklinik Geislingen	Baden-Württemberg	18	4.742		152	4.590
079	Klinikum Traunstein	Bayern	548	64.547	29.245	3.146	32.156
079	Kreisklinik Vinzentinum Ruhpolding	Bayern	76	3.372	2.406		966
080	Diakonie Klinikum Ev. Jung-Stilling-Krankenhaus	Nordrhein-Westfalen	503	59.030	21.471		37.559
080	Diakonie Klinikum Ev. Krankenhaus Kredenbach, Krankenhausbetrieb bis zum 28.02.2018	Nordrhein-Westfalen	100	979	183		796
080	Diakonie Klinikum Krankenhaus Bethesda	Nordrhein-Westfalen	183	18.392	7.334		11.058
081	St. Hedwig-Klinik	Baden-Württemberg	55	4.886	3.025		1.861
081	Theresienkrankenhaus Mannheim	Baden-Württemberg	525	56.214	21.299		34.915

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
082	Sophien- und Hufeland-Klinikum gGmbH	Thüringen	545	52.677	20.642	175	31.860
082	Sophien- u. Hufeland-Klinikum gGmbH, psychiatr.-psychotherap. Tagesklinik Apolda	Thüringen	16	114		114	
083	Klinikum Mutterhaus der Borromäerinnen - Standort Mitte	Rheinland-Pfalz	695	90.027	30.705	280	59.042
083	Klinikum Mutterhaus der Borromäerinnen gGmbH - Standort Nord	Rheinland-Pfalz	135	4.799	2.826	139	1.834
083	Klinikum Mutterhaus der Borromäerinnen gGmbH - Standort Ehr-ang	Rheinland-Pfalz	224	18.000	7.261		10.739
084	MEDIAN Klinik Gunzenbachhof Baden-Baden	Baden-Württemberg	68	3.358			
084	MEDIAN Franz-Alexander-Klinik Nordrach	Baden-Württemberg	34	343			
084	MEDIAN Achertal-Klinik Ottenhöfen	Baden-Württemberg	69	3.185			
084	MEDIAN Klinik St. Georg Bad Dürrheim	Baden-Württemberg	116	667			
084	MEDIAN Klinik Berlin Kladow	Berlin	35	190	190		
084	MEDIAN-Klinik Grünheide	Brandenburg	154	1.003	1.003		
084	MEDIAN Klinik Odenwald	Hessen	30	274			
084	MEDIAN Klinik NRZ Wiesbaden	Hessen	55	514			
084	MEDIAN Reha-Zentrum Gyhum GmbH & Co. KG	Niedersachsen	0	0			
084	MEDIAN Zentrum für Verhaltensmedizin Bad Pyrmont - Fachkran-kenhaus	Niedersachsen	73	590	590		
084	MEDIAN Klinik NRZ	Nordrhein-Westfalen	30	289	289		
084	MEDIAN Klinik Berus - Fachkrankenhaus	Saarland	32	287			
084	MEDIAN Klinik NRZ Magdeburg	Sachsen-Anhalt	100	580	580		
084	Median Klinik Lübeck	Schleswig-Holstein	27	897	523		374
084	MEDIAN Heinrich-Mann-Klinik	Thüringen	62	435	435		
084	MEDIAN Klinik Bad Tennstedt	Thüringen	73	591			
085	MediClin Reha Zentrum Gernsbach	Baden-Württemberg	27	278	286		
085	MediClin Klinik an der Lindenhöhe	Baden-Württemberg	173	8.931	1.534	218	7.179
085	MediClin Herzzentrum Lahr/Baden	Baden-Württemberg	75	4.831	3.643		1.188
085	MediClin Seidelklinik	Baden-Württemberg	63	2.825	1.721		1.104
085	MediClin Kliniken Bad Wildungen Fachklinik für Akutpsychosomatik	Hessen	75	606	552		54
085	MediClin Klinik Bad Orb	Hessen	15	167	149		

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
085	MediClin Müritz-Klinikum	Mecklenburg-Vorpommern	19	1.080		540	540
085	MediClin Müritz-Klinikum	Mecklenburg-Vorpommern	203	20.600	10.762		9.838
085	MediClin Müritz-Klinikum	Mecklenburg-Vorpommern	173	3.602	1.194	401	2.007
085	MediClin Krankenhaus am Crivitzer See	Mecklenburg-Vorpommern	74	14.331	3.799		10.532
085	MediClin Müritz-Klinikum	Mecklenburg-Vorpommern	18	1.465		89	1.376
085	MediClin Krankenhaus Plau am See	Mecklenburg-Vorpommern	192	9.456	5.789		3.667
085	MediClin Seepark Klinik	Niedersachsen	88	570	497	73	
085	MediClin Klinikum Soltau	Niedersachsen	59	1.434	578		856
085	MediClin Klinik für Akutpsychosomatik und Psychotherapie	Niedersachsen	49	341	399		
085	MediClin Hedon Klinik	Niedersachsen	105	765	662		
085	MediClin Klinik Reichshof	Nordrhein-Westfalen	20	138	130		
085	MediClin Robert Janker Klinik	Nordrhein-Westfalen	83	1.334	1.465		
085	MediClin Waldkrankenhaus Bad Düben	Sachsen	125	2.787	2.368		419
085	MediClin Klinik am Brunnenberg	Sachsen	0	75	75		
085	MediClin Herzzentrum Coswig	Sachsen-Anhalt	113	6.201	4.916		1.285
086	Vitos psychiatrische Tagesklinik Kassel	Hessen	0	8.309		368	7.941
086	Vitos Klinik Bad Wilhelmshöhe	Hessen	60	1.837	575	94	1.168
086	Vitos Orthopädische Klinik Kassel gemeinnützige GmbH	Hessen	137	22.090	5.090		17.000
086	Vitos Klinik für Psychiatrie und Psychotherapie Kassel	Hessen	110	1.074	1.060	14	
086	Vitos Klinik für Psychosomatik Kassel	Hessen	25	66	182		
086	Vitos psychiatrische Tagesklinik Melsungen	Hessen	0	1.501		82	1.419
086	Vitos Klinik für Psychiatrie und Psychotherapie Bad Emstal	Hessen	141	9.508	2.478	35	6.995
086	Vitos Klinik für Psychiatrie und Psychotherapie Hofgeismar	Hessen	22	1.032	259	38	735
086	Vitos kinder- und jungendpsychiatrische Tagesklinik Hofgeismar	Hessen	0	1.258		67	1.191
086	Vitos Klinik für Psychiatrie und Psychotherapie Standort Korbach	Hessen	15	97		97	
086	Vitos kinder- und jugendpsychiatrische Tagesklinik Korbach	Hessen	0	1.281		56	1.225
086	Vitos kinder- und jugendpsychiatrische Tagesklinik Wabern	Hessen	0	1.132		56	1.076
086	Vitos Klinikum Gießen-Marburg / Standort Marburg	Hessen	214	10.648	2.063	293	8.292
086	Vitos Klinik für Psychiatrie und Psychotherapie Standort Haina	Hessen	112	19.413	1.786	74	17.553

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
086	Vitos Psychiatrische Tagesklinik Martinshof	Hessen	0	445			
086	Vitos Klinikum Gießen-Marburg / Standort Gießen	Hessen	263	13.584	3.359	298	9.927
086	Vitos psychiatrische Tagesklinik Wetzlar und Vitos kinder- und jugendpsychiatrische Tagesklinik Wetzlar	Hessen	0	6.335		135	6.200
086	Vitos-Klinik Hasselborn	Hessen	14	338	314		
086	Vitos Klinikum Herborn	Hessen	304	12.429	3.102	211	9.116
086	Vitos psychiatrische Tagesklinik Weilburg der Vitos Klinik für Psychiatrie und Psychotherapie Weil-Lahn	Hessen	0	1.609		105	1.504
086	Vitos Klinikum Weil-Lahn, Standort Weilmünster	Hessen	204	7.643	3.428	87	4.128
086	Vitos Klinik Lahnhöhe Marburg / Tagesklinik Alsfeld	Hessen	12	2.243		48	2.195
086	Vitos kinder- und jungendpsychiatrische Tagesklinik Eschwege	Hessen	0	747		42	705
086	Vitos Klinik Bamberger Hof	Hessen	30	12.447		261	12.186
086	Vitos psychiatrische Tagesklinik Bad Homburg	Hessen	40	4.630		263	4.367
086	Vitos Waldkrankenhaus Köppern	Hessen	125	5.670	1.950	69	3.651
086	Vitos kinder- und jugendpsychiatrische Tagesklinik und Ambulanz Oberursel	Hessen	0	1.203		59	1.144
086	Vitos Klinik Hofheim Standort Dietzenbach	Hessen	0	1.771		52	1.719
086	Vitos kinder- und jugendpsychiatrische Tagesklinik Hanau	Hessen	0	3.312		102	3.210
086	Vitos Philippshospital Riedstadt Standort Gross-Gerau	Hessen	0	4.093		143	3.950
086	Vitos Klinikum Riedstadt Standort Riedstadt	Hessen	274	9.104	2.732	168	6.204
086	Vitos Klinikum Heppenheim Standort Bensheim	Hessen	0	855		138	717
086	Vitos Heppenheim	Hessen	206	13.535	2.822	233	10.480
086	Vitos Klinik Hofheim Standort Heppenheim	Hessen	0	3.938		57	3.881
086	Vitos Klinikum Heppenheim Standort Erbach	Hessen	0	0			
086	Vitos Klinik Hofheim Standort Höchst/Odenwald	Hessen	0	1.948		35	1.913
086	Vitos Klinikum Rheingau, Vitos psychiatrische Tagesklinik und Ambulanz Wiesbaden und Vitos kinder- und jugendpsychiatrische Tagesklinik und Ambulanz Wiesbaden	Hessen	0	8.011		214	7.797
086	Vitos Klinikum Rheingau, Eltville	Hessen	196	9.689	2.150	61	7.478
086	Vitos Philippshospital Riedstadt Standort Rüsselsheim	Hessen	0	3.610		231	3.379

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
086	Vitos Klinikum Rheingau, Vitos kinder- und jugendpsychiatrische Klinik Idstein	Hessen	18	2.104	73	14	2.017
086	Vitos Klinikum Rheingau, Vitos psychiatrische Tagesklinik und Ambulanz Idstein	Hessen	0	3.549		91	3.458
086	Vitos psychiatrische Tagesklinik Limburg der Vitos Klinik für Psychiatrie und Psychotherapie Hadamar	Hessen	0	3.002		86	2.916
086	Vitos kinder- und jugendpsychiatrische Tagesklinik Limburg	Hessen	0	1.832		63	1.769
086	Vitos Klinik für Psychiatrie und Psychotherapie Hadamar	Hessen	93	7.651	1.481	100	6.070
086	Vitos Klinikum Rheingau, Vitos kinder-und jugendpsychiatrische Tagesklinik und Ambulanz Kelkheim	Hessen	0	967	2	39	926
086	Vitos Klinikum Heppenheim Standort Lampertheim	Hessen	0	1.321		140	1.181
087	Herz-Kreislauf-Zentrum Klinikum Hersfeld-Rotenburg GmbH	Hessen	200	7.772			
087	Klinikum Bad Hersfeld	Hessen	568	78.845	26.145	346	52.354
087	Orthopädie Bad Hersfeld GmbH	Hessen	40	5.393			
087	Klinikum Bad Hersfeld - Klinik am Hainberg	Hessen	38	264			
087	Klinikum Bad Hersfeld - Vitalisklinik	Hessen	7	83			
088	Oberhavel Kliniken GmbH / Klinik Oranienburg	Brandenburg	237	29.617	9.238	20.379	
088	Oberhavel Kliniken GmbH / Klinik Hennigsdorf	Brandenburg	460	47.729	13.978	434	33.317
088	Oberhavel Klinik Gransee GmbH	Brandenburg	65	9.737	3.505		6.232
088	Oberhavel Kliniken GmbH / Tagesklinik Gransee	Brandenburg	28	381		381	
089	KMG Klinikum Luckenwalde	Brandenburg	253	37.136	10.136		27.000
089	KMG Klinikum Mitte GmbH Klinikum Kyritz	Brandenburg	165	33.587	7.359		26.228
089	KMG Klinikum Mitte GmbH, Klinikum Wittstock	Brandenburg	132	10.134	4.822		5.312
089	KMG Klinikum Pritzwalk	Brandenburg	133	10.803	4.170	135	6.498
089	KMG Klinikum Güstrow	Mecklenburg-Vorpommern	451	44.370	19.717	296	24.357
089	KMG Klinik Boizenburg GmbH	Mecklenburg-Vorpommern	54	3.854	2.329		1.525
089	KMG Manniske Klinik Bad Frankenhausen	Sachsen-Anhalt	128	8.197	2.359		5.838
089	KMG Klinikum Havelberg GmbH	Sachsen-Anhalt	80	3.295	1.447		1.848
089	KMG Klinikum Sömmerda	Thüringen	178	32.446	8.036		24.410
089	KMG Klinikum Sondershausen	Thüringen	151	25.102	6.844	222	18.036

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
090	Thüringen-Kliniken "Georgius Agricola", Standort Saalfeld	Thüringen	529	47.896	21.732	317	25.847
090	Thüringen-Kliniken "Georgius Agricola", Standort Pößneck	Thüringen	108	13.388	3.673		9.715
090	Thüringen-Kliniken "Georgius Agricola", Standort Rudolstadt	Thüringen	187	6.786	4.662	269	1.855
090	Thüringen-Kliniken "Georgius Agricola", Tagesklinik	Thüringen	12	71		71	
091	ACURA Kliniken Albstadt GmbH	Baden-Württemberg	55	9.712	1.588		8.124
091	ACURA Kliniken Baden-Baden GmbH	Baden-Württemberg	170	5.189	1.958	60	3.171
091	Acura Kliniken Rheinland-Pfalz GmbH Akutzentrum	Rheinland-Pfalz	70	5.847	1.766	403	3.678
092	DRK-Krankenhaus Teterow gGmbH	Mecklenburg-Vorpommern	95	16.588	5.384		11.204
092	DRK-Krankenhaus Mecklenburg-Strelitz gGmbH	Mecklenburg-Vorpommern	164	20.253	6.434		13.819
092	DRK-Krankenhaus Grimmen GmbH	Mecklenburg-Vorpommern	113	10.792	5.574		
092	DRK-Krankenhaus Grevesmühlen gGmbH	Mecklenburg-Vorpommern	122	10.489	5.661		4.828
093	DRK Krankenhaus Altenkirchen-Hachenburg (AK)	Rheinland-Pfalz	160	19.812	7.128	201	12.483
093	DRK Krankenhaus Altenkirchen-Hachenburg (HB)	Rheinland-Pfalz	163	20.143	7.607		12.536
094	VAMED Klinik Kipfenberg	Bayern	125	871	800		
094	VAMED Klinik Hohenstücken	Brandenburg	45	116	190		
094	VAMED Klinik Bad Berleburg GmbH	Nordrhein-Westfalen	127	14.690	6.111		8.579
094	VAMED Klinik Hagen Ambrock	Nordrhein-Westfalen	80	1.956	2.170		
094	VAMED Klinik Schloss Pulsnitz GmbH: Krankenhausbereich, enthalten sind nur die Daten der Patientinnen/Patienten der Besonderen Einrichtung, ohne Patientinnen/Patienten aus dem Reha-Bereich	Sachsen	100	951	951		
094	VAMED Klinik Geesthacht: Akutbereich, enthalten sind nur die Daten der Patientinnen/Patienten der besonderen Einrichtung, ohne Patientinnen/Patienten aus dem Reha-Bereich	Schleswig-Holstein	70	651	681		
094	VAMED Ostseeklinik Damp	Schleswig-Holstein	164	12.610	6.380	385	5.845
095	Katholisches Krankenhaus Hagen gem. GmbH -St. Josefs-Hospital-	Nordrhein-Westfalen	253	45.579	9.192		36.387
095	Katholisches Krankenhaus Hagen gem. GmbH -St. Johannes-Hospital-	Nordrhein-Westfalen	281	22.937	10.272	177	12.488
095	Katholisches Krankenhaus Hagen gem. GmbH -Katholisches Krankenhaus Elsey-	Nordrhein-Westfalen	115	3.135	2.166		

Kranken-haus-verbunds-ID	Einrichtung	Bundesland	Betten im Krankenhaus	Fälle			
				Gesamt	vollstationär 2018/2019	teilstationär 2018/2019	ambulant 2018/2019
096	Knappschaftskrankenhaus Dortmund, Klinikum Westfalen GmbH	Nordrhein-Westfalen	451	60.175	21.497		38.678
096	Klinik am Park Lünen, Klinikum Westfalen GmbH	Nordrhein-Westfalen	160	18.091	6.895	11.196	
096	Hellmig-Krankenhaus Kamen	Rheinland-Pfalz	188	31.335	7.959		23.376
096	Knappschaftskrankenhaus Lütgendortmund	Rheinland-Pfalz	326	43.997	6.457		37.540

Quelle: Rene Schubert, 08.10.2021

Tabelle 5: Zuordnung der Einrichtungen zu den Klinikverbünden

Anhang C - Dokumente zur Spezifikation der Telematikinfrastruktur

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0	-	V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Spezifikation KOM-LE-Clientmodul	1.11.1	20.04.2021	X								
Betriebskonzept Online-Produktivbetrieb	3.10.0	18.03.2021	X						3.8.0	3.8.0	3.9.0
Testkonzept der TI	2.8.2	02.09.2021	2.8.1	2.6.0	2.7.0	2.8.0		X	2.8.0	2.8.0	2.8.0
Produkttypsteckbrief Konnektor (Ausbaustufe VSDM)	1.1.0	19.01.2018									
Produkttypsteckbrief Konnektor	1.0.0	04.03.2020									
Produkttypsteckbrief Konnektor	1.0.0	08.01.2021									
Produkttypsteckbrief Konnektor	1.0.0	07.04.2021									
Produkttypsteckbrief Konnektor	1.0.0	14.07.2021									
Übergreifende Richtlinien zum Betrieb der TI	2.5.1	19.02.2021	X						X	2.5.0	X
Certificate Policy Gemeinsame Zertifizie-rungsrichtlinie für Teilnehmer der gematik-TSL	2.9.0	30.06.2021				X					2.7.0
S/MIME-Profil Kommunikation Leistungser-bringer	1.7.0	04.08.2021	X								
Spezifikation ePA Aktensystem	1.8.1	09.07.2021									
Spezifikation Authentisierung des Versicher-ten ePA	1.4.1	02.06.2021						X			
Spezifikation Basis- und KTR-Consumer	1.3.2	06.08.2021	X								

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0		V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Spezifikation KOM-LE-Clientmodul	1.12.0	04.08.2021	X								
Spezifikation des Card Operating System (COS)	3.13.1	01.11.2019		X							
Spezifikation CVC-Root	1.9.0	18.12.2018			X						
Spezifikation Trust Service Provider CVC	1.14.0	30.06.2021				X					
Datenmodell ePA	1.9.0	09.07.2021						X			
Spezifikation Datenmodell E-Rezept	1.2.0	19.02.2021							X	X	
Spezifikation ePA Dokumentenverwaltung	1.9.0	09.07.2021						X			
Spezifikation Datenschutzund Sicherheitsan-forderungen der TI an Anbieter	1.3.0	12.11.2020	X			X				X	X
Spezifikation Datenschutz- und Sicherheits-anforderungen der TI an Anbieter	1.3.0	12.11.2020	X	1.1.0	X	X		X	X	X	
Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.3.1	23.11.2016									
Speicherstrukturen der eGK für die Fachan-wendung AMTS	1.4.0	26.10.2018									
Speicherstrukturen der eGK für die Fachan-wendung NFDM	1.1.0	02.08.2017									
Speicherstrukturen der eGK für die Fachan-wendung VSDM	1.2.1	19.02.2021									X
Spezifikation der elektronischen Gesund-heitskarte eGK-Objektsystem	4.5.0	02.10.2019									
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	5.1.0	18.12.2017									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0		V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Die Spezifikation der elektronischen Gesund-heitskarte Äußere Gestaltung	3.10.0	02.10.2019									
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018									
Spezifikation ePA-Frontend des Versicherten	1.10.0	09.07.2021						X			
Spezifikation E-Rezept-Frontend des Versi-cherten	1.2.0	19.02.2021								X	
Spezifikation E-Rezept-Fachdienst	1.2.0	19.02.2021							X	X	
Spezifikation Fachdienst KOM-LE	1.14.0	04.08.2021									
Spezifikation Fachmodul AMTS	1.4.0	15.05.2019									
Spezifikation Fachmodul ePA	1.9.0	09.07.2021									
Spezifikation Fachmodul ePA im KTRConsumer	1.3.1	19.02.2021									
Spezifikation Fachmodul NFDM	1.6.0	28.06.2019									
Spezifikation Fachmodul VSDM	2.6.0	21.04.2017									
Spezifikation der gSMC-K Objektsystem	3.13.0	30.06.2021				3.9.0					
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018				X					
Übergreifende Spezifikation HSM-Proxy	1.0.0	15.05.2019	X								
Spezifikation Identity Provider-Dienst	1.3.0	14.06.2021									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0		V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Spezifikation Identity Provider – Nutzungs-spezifikation für Fachdienste	1.2.0	19.02.2021							X	X	
Spezifikation Identity Provider - Frontend	1.2.0	12.11.2020								1.1.0	
nformationsmodell eMP/AMTS-Datenma-nagement	1.5.0	02.10.2019									
Informationsmodell Notfalldaten-Management (NFDM)	1.6.0	02.03.2020									
Spezifikation Intermediär VSDM	1.12.0	02.03.2020									
Koordinierendes Informationssicherheitsma-nagement der Telematikinfrastruktur	1.4.1	23.11.2016									
Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0	24.08.2016				X					
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0	18.12.2017				X					
Spezifikation Konnektor	5.13.0	13.04.2021									
Ergänzung zur Spezifikation Konnektor (PTV4)	1.1.0	07.04.2021									
Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telema-tikinfrastruktur	2.20.0	02.09.2021	2.19.1	2.16.0	2.18.0	2.19.1		X	2.19.0	2.19.0	2.19.0
Spezifikation Konfigurationsdienst	2.5.0	02.03.2020				X					
Spezifikation eHealth-Kartenterminal	3.13.3	30.06.2021				X					
Spezifikation KTR-AdV	1.7.0	30.06.2020									
Spezifikation Mobiles Kartenterminal	2.14.0	26.06.2020									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0		V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Übergreifende Spezifikation Netzwerk	1.20.3	31.08.2021	1.20.2		1.19.0			X	1.20.0		1.20.1
Spezifikation Festlegung von OIDs	3.10.0	19.02.2021			3.9.0						
Übergreifende Spezifikation Operations und Maintenance	1.14.0	26.06.2020	X	1.13.0		X		X	X	X	X
Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0	14.06.2021				X			2.12.1		2.12.2
Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0	14.05.2018				X					
Spezifikation für Prüfkarten des Typs eGK	1.2.0	26.10.2018							X		
Übergreifende Spezifikation Spezifikation PKI	2.10.4	14.07.2021	X	2.8.0	2.10.0	2.10.2		2.10.3	2.10.2	2.10.2	
Spezifikation Service Monitoring	1.5.0	02.03.2020									
Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2	19.02.2021						X			
Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI	1.4.0	24.08.2016									
Spezifikation Datenschutz und Sicherheitsanforderungen	1.4.1	23.11.2016									
Spezifikation Signaturdienst	1.4.0	12.11.2020									
Spezifikation der Security Module Card SMC-B Objektsystem	5.0.0	10.09.2020									
Gemeinsame optische Merkmale der SMC	3.8.0	30.06.2020				X					
Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0	12.08.2016									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-tenversion	Basis-Consu-mer	Card Opera-ting System	CVC-Root/CVC-Root ECC	Komponenten & Dienste eHealth-Kar-tenterminal	ePA-Akten-system	Komponenten & Dienste ePA-Frontend des Versi-cherten	E-Rezept-Fachdienst	E-Rezept-Frontend des Versicherten	Fachdienste VSDM
Produktversion			V1.5.0-0	V4.6.0-0	V1.4.0-0	V1.7.1-0	_	V2.5.0-0	V1.2.0-0	V1.2.0-0	V1.7.0-0
Spezifikation Logdaten- und Betriebsdatener-fassung	1.2.0	30.06.2020							X		X
Schnittstellenspezifikation Primärsysteme VSDM	1.5.0	24.08.2016									
SchnittstellenspezifikationTransport VSDM	2.5.0	15.05.2019									X
Spezifikation Systemprozesse der dezentra-len TI	1.3.0	10.09.2020	X					X			
Übergreifende Spezifikation Tokenbasierte Authentisierung	1.4.0	14.05.2018									
Spezifikation TSL-Dienst	1.19.0	19.02.2021	X								X
Spezifikation VPN-Zugangsdienst	1.17.0	30.06.2021									
Spezifikation Verzeichnisdienst	1.13.1	20.04.2021									
Verfahrensbeschreibung Zulassung Anbieter ePA Aktensystem	2.4.0	03.07.2020					X				
Verfahrensbeschreibung Zulassung Betreiber ePA-Aktensystem	1.1.0	03.07.2020					X				
Verfahrensbeschreibung Bestätigung Sicher-heitsgutachten ePA-Aktensystem	1.7.0	08.02.2021					X				
Verfahrensbeschreibung Zulassung Produkt-typ ePA-Aktensystem	1.4.0	14.04.2021					X				
Antrag auf Zulassung als Anbieter operativer Betriebsleistungen	1.0.9	30.07.2020					X				
Zulassungsantrag Produkttyp ePA-Aktensys-tem	1.0.7	30.07.2020					X				

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Spezifikation KOM-LE-Clientmodul	1.11.1	20.04.2021				X							
Betriebskonzept Online-Produktivbetrieb	3.10.0	18.03.2021	X	X									
Testkonzept der TI	2.8.2	02.09.2021	2.8.0	2.8.0	2.8.0	2.8.1	2.8.1	2.7.0	1.10.0	2.1.0	2.6.1	2.6.1	2.8.1
Produkttypsteckbrief Konnektor (Ausbaustufe VSDM)	1.1.0	19.01.2018							X				
Produkttypsteckbrief Konnektor	1.0.0	04.03.2020								X			
Produkttypsteckbrief Konnektor	1.0.0	08.01.2021									X		
Produkttypsteckbrief Konnektor	1.0.0	07.04.2021										X	
Produkttypsteckbrief Konnektor	1.0.0	14.07.2021											X
Übergreifende Richtlinien zum Betrieb der TI	2.5.1	19.02.2021	X	X									
Certificate Policy Gemeinsame Zertifizie-rungsrichtlinie für Teilnehmer der gematik-TSL	2.9.0	30.06.2021			2.7.0		X	2.6.0	1.8.0	2.2.0	2.7.0	2.7.0	X
S/MIME-Profil Kommunikation Leistungser-bringer	1.7.0	04.08.2021				X							
Spezifikation ePA Aktensystem	1.8.1	09.07.2021											
Spezifikation Authentisierung des Versicher-ten ePA	1.4.1	02.06.2021											X
Spezifikation Basis- und KTR-Consumer	1.3.2	06.08.2021											
Spezifikation KOM-LE-Clientmodul	1.12.0	04.08.2021				X							

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Spezifikation des Card Operating System (COS)	3.13.1	01.11.2019											
Spezifikation CVC-Root	1.9.0	18.12.2018											
Spezifikation Trust Service Provider CVC	1.14.0	30.06.2021							1.8.1		1.13.0	1.13.0	X
Datenmodell ePA	1.9.0	09.07.2021									1.4.2	1.4.2	X
Spezifikation Datenmodell E-Rezept	1.2.0	19.02.2021											
Spezifikation ePA Dokumentenverwaltung	1.9.0	09.07.2021									1.4.2	1.4.2	X
Spezifikation Datenschutzund Sicherheitsan-forderungen der TI an Anbieter	1.3.0	12.11.2020	X	X	X		X	X				X	X
Spezifikation Datenschutz- und Sicherheits-anforderungen der TI an Anbieter	1.3.0	12.11.2020	X	X		X				1.0.0		X	X
Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.3.1	23.11.2016							X				
Speicherstrukturen der eGK für die Fachan-wendung AMTS	1.4.0	26.10.2018								1.2.0		X	1.2.0
Speicherstrukturen der eGK für die Fachan-wendung NFDM	1.1.0	02.08.2017								X			X
Speicherstrukturen der eGK für die Fachan-wendung VSDM	1.2.1	19.02.2021							1.2.0	1.2.0			X
Spezifikation der elektronischen Gesund-heitskarte eGK-Objektsystem	4.5.0	02.10.2019											
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	5.1.0	18.12.2017											
Die Spezifikation der elektronischen Gesund-heitskarte Äußere Gestaltung	3.10.0	02.10.2019											

Komponenten & Dienste / Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018											
Spezifikation ePA-Frontend des Versicherten	1.10.0	09.07.2021											
Spezifikation E-Rezept-Frontend des Versi-cherten	1.2.0	19.02.2021											
Spezifikation E-Rezept-Fachdienst	1.2.0	19.02.2021											
Spezifikation Fachdienst KOM-LE	1.14.0	04.08.2021					X						
Spezifikation Fachmodul AMTS	1.4.0	15.05.2019											X
Spezifikation Fachmodul ePA	1.9.0	09.07.2021										1.4.4	X
Spezifikation Fachmodul ePA im KTRConsumer	1.3.1	19.02.2021											
Spezifikation Fachmodul NFDM	1.6.0	28.06.2019										1.6.0	X
Spezifikation Fachmodul VSDM	2.6.0	21.04.2017							1.9.0			X	X
Spezifikation der gSMC-K Objektsystem	3.13.0	30.06.2021							3.10.0	3.11.1		3.12.0	X
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018											
Übergreifende Spezifikation HSM-Proxy	1.0.0	15.05.2019											
Spezifikation Identity Provider-Dienst	1.3.0	14.06.2021	X	X									
Spezifikation Identity Provider – Nutzungs-spezifikation für Fachdienste	1.2.0	19.02.2021											

Komponenten & Dienste / Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Spezifikation Identity Provider - Frontend	1.2.0	12.11.2020	X	X									
nformationsmodell eMP/AMTS-Datenma-nagement	1.5.0	02.10.2019								1.3.0		X	X
Informationsmodell Notfalldaten-Management (NFDM)	1.6.0	02.03.2020								1.4.0		X	X
Spezifikation Intermediär VSDM	1.12.0	02.03.2020		X	X								
Koordinierendes Informationssicherheitsma-nagement der Telematikinfrastruktur	1.4.1	23.11.2016							X				
Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0	24.08.2016											X
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0	18.12.2017										X	X
Spezifikation Konnektor	5.13.0	13.04.2021								1.4.0			X
Ergänzung zur Spezifikation Konnektor (PTV4)	1.1.0	07.04.2021										X	
Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telema-tikinfrastruktur	2.20.0	02.09.2021	2.19.0	2.19.0	2.19.0	2.19.1	2.19.1	2.18.0	2.8.0	2.11.0		2.16.2	2.19.1
Spezifikation Konfigurationsdienst	2.5.0	02.03.2020						X		2.2.0		X	X
Spezifikation eHealth-Kartenterminal	3.13.3	30.06.2021											
Spezifikation KTR-AdV	1.7.0	30.06.2020											
Spezifikation Mobiles Kartenterminal	2.14.0	26.06.2020											
Übergreifende Spezifikation Netzwerk	1.20.3	31.08.2021	1.20.1	1.20.1	1.20.0	1.20.2	1.20.2	1.19.0		1.14.0		1.17.2	1.20.2

Komponenten & Dienste / Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Spezifikation Festlegung von OIDs	3.10.0	19.02.2021											X
Übergreifende Spezifikation Operations und Maintenance	1.14.0	26.06.2020	X	X	X	X	X	X	1.8.0	1.10.0		X	
Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0	14.06.2021	X	X	2.12.1	X	X	2.12.0		2.5.0		2.10.1	X
Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0	14.05.2018							1.2.0	X		X	X
Spezifikation für Prüfkarten des Typs eGK	1.2.0	26.10.2018											
Übergreifende Spezifikation Spezifikation PKI	2.10.4	14.07.2021	2.10.2	2.10.2	2.10.2		2.10.2	2.10.0				2.8.1	X
Spezifikation Service Monitoring	1.5.0	02.03.2020			X		X	X					
Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2	19.02.2021										1.4.1	X
Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Pro-dukte der TI	1.4.0	24.08.2016							X				
Spezifikation Datenschutz und Sicherheitsan-forderungen	1.4.1	23.11.2016							X				
Spezifikation Signaturdienst	1.4.0	12.11.2020											
Spezifikation der Security Module Card SMC-B Objektsystem	5.0.0	10.09.2020											
Gemeinsame optische Merkmale der SMC	3.8.0	30.06.2020										3.7.0	X
Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0	12.08.2016							X	X		X	X
Spezifikation Logdaten- und Betriebsdatener-fassung	1.2.0	30.06.2020	X				X	X					

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	gematik Root-CA	Identity Provi-der	Intermediär	KIM-Client-modul	KIM-Fach-dienst	Konfigurati-onsdienst	Konnektor				
									PTV 1	PTV 3	PTV 4	PTV 4+	PTV 5
Produktversion			V2.2.0-0	V2.2.0-0	V1.6.4-0	V1.6.1-0	V1.6.1-0	V1.8.6-0					
Schnittstellenspezifikation Primärsysteme VSDM	1.5.0	24.08.2016							1.4.0	X		X	X
SchnittstellenspezifikationTransport VSDM	2.5.0	15.05.2019			X					2.4.0		X	X
Spezifikation Systemprozesse der dezentra-len TI	1.3.0	10.09.2020							1.12.0				
Übergreifende Spezifikation Tokenbasierte Authentisierung	1.4.0	14.05.2018								1.2.0		X	
Spezifikation TSL-Dienst	1.19.0	19.02.2021			X		X		1.11.0	1.13.0		1.18.0	X
Spezifikation VPN-Zugangsdienst	1.17.0	30.06.2021							1.9.0	1.12.0		1.15.0	X
Spezifikation Verzeichnisdienst	1.13.1	20.04.2021					X		1.5.0	1.6.0		1.9.1	X
Verfahrensbeschreibung Zulassung Anbieter ePA Aktensystem	2.4.0	03.07.2020											
Verfahrensbeschreibung Zulassung Betreiber ePA-Aktensystem	1.1.0	03.07.2020											
Verfahrensbeschreibung Bestätigung Sicher-heitsgutachten ePA-Aktensystem	1.7.0	08.02.2021											
Verfahrensbeschreibung Zulassung Produkt-typ ePA-Aktensystem	1.4.0	14.04.2021											
Antrag auf Zulassung als Anbieter operativer Betriebsleistungen	1.0.9	30.07.2020											
Zulassungsantrag Produkttyp ePA-Aktensys-tem	1.0.7	30.07.2020											

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion						V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Spezifikation KOM-LE-Clientmodul	1.11.1	20.04.2021									
Betriebskonzept Online-Produktivbetrieb	3.10.0	18.03.2021	3.9.0	X						X	
Testkonzept der TI	2.8.2	02.09.2021	2.8.0	2.8.1	2.6.1	2.8.0	2.8.0	2.7.0	2.8.0	2.8.0	2.7.0
Produkttypsteckbrief Konnektor (Ausbaustufe VSDM)	1.1.0	19.01.2018									
Produkttypsteckbrief Konnektor	1.0.0	04.03.2020									
Produkttypsteckbrief Konnektor	1.0.0	08.01.2021									
Produkttypsteckbrief Konnektor	1.0.0	07.04.2021									
Produkttypsteckbrief Konnektor	1.0.0	14.07.2021									
Übergreifende Richtlinien zum Betrieb der TI	2.5.1	19.02.2021	X	X						X	
Certificate Policy Gemeinsame Zertifizie-rungsrichtlinie für Teilnehmer der gematik-TSL	2.9.0	30.06.2021					2.7.0			X	
S/MIME-Profil Kommunikation Leistungser-bringer	1.7.0	04.08.2021		X							
Spezifikation ePA Aktensystem	1.8.1	09.07.2021		X							
Spezifikation Authentisierung des Versicher-ten ePA	1.4.1	02.06.2021									
Spezifikation Basis- und KTR-Consumer	1.3.2	06.08.2021		X							
Spezifikation KOM-LE-Clientmodul	1.12.0	04.08.2021		X							

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion						V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Spezifikation des Card Operating System (COS)	3.13.1	01.11.2019									
Spezifikation CVC-Root	1.9.0	18.12.2018									
Spezifikation Trust Service Provider CVC	1.14.0	30.06.2021									
Datenmodell ePA	1.9.0	09.07.2021		X							
Spezifikation Datenmodell E-Rezept	1.2.0	19.02.2021									
Spezifikation ePA Dokumentenverwaltung	1.9.0	09.07.2021		X							
Spezifikation Datenschutzund Sicherheitsan-forderungen der TI an Anbieter	1.3.0	12.11.2020	X			X	X	X	X	X	X
Spezifikation Datenschutz- und Sicherheits-anforderungen der TI an Anbieter	1.3.0	12.11.2020	X	X	1.2.0						
Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.3.1	23.11.2016									
Speicherstrukturen der eGK für die Fachan-wendung AMTS	1.4.0	26.10.2018									
Speicherstrukturen der eGK für die Fachan-wendung NFDM	1.1.0	02.08.2017									
Speicherstrukturen der eGK für die Fachan-wendung VSDM	1.2.1	19.02.2021	X		1.2.0						
Spezifikation der elektronischen Gesund-heitskarte eGK-Objektsystem	4.5.0	02.10.2019									
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	5.1.0	18.12.2017									
Die Spezifikation der elektronischen Gesund-heitskarte Äußere Gestaltung	3.10.0	02.10.2019									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion			-	-	-	V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018									
Spezifikation ePA-Frontend des Versicherten	1.10.0	09.07.2021									
Spezifikation E-Rezept-Frontend des Versi-cherten	1.2.0	19.02.2021									
Spezifikation E-Rezept-Fachdienst	1.2.0	19.02.2021									
Spezifikation Fachdienst KOM-LE	1.14.0	04.08.2021									
Spezifikation Fachmodul AMTS	1.4.0	15.05.2019									
Spezifikation Fachmodul ePA	1.9.0	09.07.2021									
Spezifikation Fachmodul ePA im KTRConsumer	1.3.1	19.02.2021		X							
Spezifikation Fachmodul NFDM	1.6.0	28.06.2019									
Spezifikation Fachmodul VSDM	2.6.0	21.04.2017									
Spezifikation der gSMC-K Objektsystem	3.13.0	30.06.2021									
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018									
Übergreifende Spezifikation HSM-Proxy	1.0.0	15.05.2019		X							
Spezifikation Identity Provider-Dienst	1.3.0	14.06.2021									
Spezifikation Identity Provider – Nutzungs-spezifikation für Fachdienste	1.2.0	19.02.2021									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion						V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Spezifikation Identity Provider - Frontend	1.2.0	12.11.2020									
nformationsmodell eMP/AMTS-Datenma-nagement	1.5.0	02.10.2019									
Informationsmodell Notfalldaten-Management (NFDM)	1.6.0	02.03.2020									
Spezifikation Intermediär VSDM	1.12.0	02.03.2020									
Koordinierendes Informationssicherheitsma-nagement der Telematikinfrastruktur	1.4.1	23.11.2016									
Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0	24.08.2016									
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0	18.12.2017									
Spezifikation Konnektor	5.13.0	13.04.2021									
Ergänzung zur Spezifikation Konnektor (PTV4)	1.1.0	07.04.2021									
Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telema-tikinfrastruktur	2.20.0	02.09.2021	2.19.0	2.19.1	2.16.0	2.19.1	2.19.0	2.18.0	2.19.0	2.19.1	2.18.0
Spezifikation Konfigurationsdienst	2.5.0	02.03.2020									
Spezifikation eHealth-Kartenterminal	3.13.3	30.06.2021									
Spezifikation KTR-AdV	1.7.0	30.06.2020	X								
Spezifikation Mobiles Kartenterminal	2.14.0	26.06.2020			X						
Übergreifende Spezifikation Netzwerk	1.20.3	31.08.2021	1.20.1	1.20.2				1.19.0	1.20.0	1.20.2	1.19.0

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion			-	-	-	V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Spezifikation Festlegung von OIDs	3.10.0	19.02.2021							X		
Übergreifende Spezifikation Operations und Maintenance	1.14.0	26.06.2020	X	X	X	X	X	X		X	X
Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0	14.06.2021	2.12.2			X	2.12.2	2.12.0	2.12.1	X	2.12.0
Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0	14.05.2018									
Spezifikation für Prüfkarten des Typs eGK	1.2.0	26.10.2018									
Übergreifende Spezifikation Spezifikation PKI	2.10.4	14.07.2021	2.10.2	X		2.10.2	2.10.2	2.10.0	2.10.2	2.10.2	2.10.0
Spezifikation Service Monitoring	1.5.0	02.03.2020				X	X	X	X	X	X
Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2	19.02.2021		X							
Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Pro-dukte der TI	1.4.0	24.08.2016									
Spezifikation Datenschutz und Sicherheitsan-forderungen	1.4.1	23.11.2016									
Spezifikation Signaturdienst	1.4.0	12.11.2020									
Spezifikation der Security Module Card SMC-B Objektsystem	5.0.0	10.09.2020									
Gemeinsame optische Merkmale der SMC	3.8.0	30.06.2020									
Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0	12.08.2016	X								
Spezifikation Logdaten- und Betriebsdatener-fassung	1.2.0	30.06.2020									

Komponenten & Dienste / Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	KTR-AdV	KTR-Consu-mer	Mobiles Kar-tenterminal	Zentrales Netz	Verzeichnis-dienst	Namens-dienst	TSL-Dienst	VPN-Zu-gangsdiens	Zeitdienst
Produktversion						V1.5.9-0	V1.6.0-0	V1.6.4-0	V2.2.0-0	V1.8.5-0	V1.5.7-0
Schnittstellenspezifikation Primärsysteme VSDM	1.5.0	24.08.2016	X								
SchnittstellenspezifikationTransport VSDM	2.5.0	15.05.2019	X								
Spezifikation Systemprozesse der dezentra-len TI	1.3.0	10.09.2020	X	X							
Übergreifende Spezifikation Tokenbasierte Authentisierung	1.4.0	14.05.2018									
Spezifikation TSL-Dienst	1.19.0	19.02.2021	X	X			X		X	X	
Spezifikation VPN-Zugangsdienst	1.17.0	30.06.2021								X	
Spezifikation Verzeichnisdienst	1.13.1	20.04.2021					X				
Verfahrensbeschreibung Zulassung Anbieter ePA Aktensystem	2.4.0	03.07.2020									
Verfahrensbeschreibung Zulassung Betreiber ePA-Aktensystem	1.1.0	03.07.2020									
Verfahrensbeschreibung Bestätigung Sicher-heitsgutachten ePA-Aktensystem	1.7.0	08.02.2021									
Verfahrensbeschreibung Zulassung Produkt-typ ePA-Aktensystem	1.4.0	14.04.2021									
Antrag auf Zulassung als Anbieter operativer Betriebsleistungen	1.0.9	30.07.2020									
Zulassungsantrag Produkttyp ePA-Aktensys-tem	1.0.7	30.07.2020									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Objektsystem					OCSP-Proxy	Schlüsselge-nerierungs-dienst ePA	Sicherheits-gateway Be-standsnetze	Signatur-dienst
			eGK Objektsystem	HBA-Objekt-system	SMC-B-Ob-jektsystem	gSMC Objekt-system	gSMC-KT-Ob-jektsystem				
Produktversion			V4.5.2-0	V4.7.1-1	V4.8.0-0	V4.5.0-0	V4.4.1-2	-	-	-	-
Spezifikation KOM-LE-Clientmodul	1.11.1	20.04.2021									
Betriebskonzept Online-Produktivbetrieb	3.10.0	18.03.2021							3.8.0		
Testkonzept der TI	2.8.2	02.09.2021	2.7.0	2.8.0	2.7.0	2.8.0	2.7.0	2.7.0	2.7.0	2.7.0	2.7.0
Produkttypsteckbrief Konnektor (Ausbaustufe VSDM)	1.1.0	19.01.2018									
Produkttypsteckbrief Konnektor	1.0.0	04.03.2020									
Produkttypsteckbrief Konnektor	1.0.0	08.01.2021									
Produkttypsteckbrief Konnektor	1.0.0	07.04.2021									
Produkttypsteckbrief Konnektor	1.0.0	14.07.2021									
Übergreifende Richtlinien zum Betrieb der TI	2.5.1	19.02.2021									
Certificate Policy Gemeinsame Zertifizie-rungsrichtlinie für Teilnehmer der gematik-TSL	2.9.0	30.06.2021									
S/MIME-Profil Kommunikation Leistungser-bringer	1.7.0	04.08.2021									
Spezifikation ePA Aktensystem	1.8.1	09.07.2021									
Spezifikation Authentisierung des Versicher-ten ePA	1.4.1	02.06.2021									
Spezifikation Basis- und KTR-Consumer	1.3.2	06.08.2021									
Spezifikation KOM-LE-Clientmodul	1.12.0	04.08.2021									

Spezifikation des Card Operating System (COS)	3.13.1	01.11.2019									
Spezifikation CVC-Root	1.9.0	18.12.2018									
Spezifikation Trust Service Provider CVC	1.14.0	30.06.2021									
Datenmodell ePA	1.9.0	09.07.2021									
Spezifikation Datenmodell E-Rezept	1.2.0	19.02.2021									
Spezifikation ePA Dokumentenverwaltung	1.9.0	09.07.2021									
Spezifikation Datenschutzund Sicherheitsanforderungen der TI an Anbieter	1.3.0	12.11.2020						X	X	X	X
Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.3.0	12.11.2020	X	X	1.2.0	X	X				
Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.3.1	23.11.2016									
Speicherstrukturen der eGK für die Fachanwendung AMTS	1.4.0	26.10.2018									
Speicherstrukturen der eGK für die Fachanwendung NFDM	1.1.0	02.08.2017									
Speicherstrukturen der eGK für die Fachanwendung VSDM	1.2.1	19.02.2021	1.2.0								
Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem	4.5.0	02.10.2019	X								
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	5.1.0	18.12.2017		X							
Die Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung	3.10.0	02.10.2019	X								
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018					X				
Spezifikation ePA-Frontend des Versicherten	1.10.0	09.07.2021									

Spezifikation E-Rezept-Frontend des Versicherten	1.2.0	19.02.2021									
Spezifikation E-Rezept-Fachdienst	1.2.0	19.02.2021									
Spezifikation Fachdienst KOM-LE	1.14.0	04.08.2021									
Spezifikation Fachmodul AMTS	1.4.0	15.05.2019									
Spezifikation Fachmodul ePA	1.9.0	09.07.2021									
Spezifikation Fachmodul ePA im KTRConsumer	1.3.1	19.02.2021									
Spezifikation Fachmodul NFDM	1.6.0	28.06.2019									
Spezifikation Fachmodul VSDM	2.6.0	21.04.2017									
Spezifikation der gSMC-K Objektsystem	3.13.0	30.06.2021				X					
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018									
Übergreifende Spezifikation HSM-Proxy	1.0.0	15.05.2019									
Spezifikation Identity Provider-Dienst	1.3.0	14.06.2021									
Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste	1.2.0	19.02.2021									
Spezifikation Identity Provider - Frontend	1.2.0	12.11.2020									
nformationsmodell eMP/AMTS-Datenmanagement	1.5.0	02.10.2019									
Informationsmodell Notfalldaten-Management (NFDM)	1.6.0	02.03.2020									
Spezifikation Intermediär VSDM	1.12.0	02.03.2020									

Koordinierendes Informationssicherheitsmanagement der Telematikinfrastruktur	1.4.1	23.11.2016									
Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0	24.08.2016				X					
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0	18.12.2017	X	X	X		X				
Spezifikation Konnektor	5.13.0	13.04.2021									
Ergänzung zur Spezifikation Konnektor (PTV4)	1.1.0	07.04.2021									
Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.20.0	02.09.2021	2.18.0		2.17.0	2.19.1	2.18.0	2.18.0	2.18.0	2.18.0	2.18.0
Spezifikation Konfigurationsdienst	2.5.0	02.03.2020									
Spezifikation eHealth-Kartenterminal	3.13.3	30.06.2021									
Spezifikation KTR-AdV	1.7.0	30.06.2020									
Spezifikation Mobiles Kartenterminal	2.14.0	26.06.2020									
Übergreifende Spezifikation Netzwerk	1.20.3	31.08.2021	1.19.0					1.19.0	1.19.0	1.19.0	1.19.0
Spezifikation Festlegung von OIDs	3.10.0	19.02.2021		X	3.8.0	X	3.6.0				
Übergreifende Spezifikation Operations und Maintenance	1.14.0	26.06.2020	X	X	X	X	X	X	X	X	X
Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0	14.06.2021	2.12.0		2.9.0			2.12.0	2.12.0	2.12.0	2.12.0
Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0	14.05.2018									
Spezifikation für Prüfkarten des Typs eGK	1.2.0	26.10.2018									
Übergreifende Spezifikation Spezifikation PKI	2.10.4	14.07.2021	2.10.0					2.10.0	2.10.0	2.10.0	2.10.0

Spezifikation Service Monitoring	1.5.0	02.03.2020	X					X		X	
Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2	19.02.2021							1.4.1		
Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI	1.4.0	24.08.2016									
Spezifikation Datenschutz und Sicherheitsanforderungen	1.4.1	23.11.2016									
Spezifikation Signaturdienst	1.4.0	12.11.2020									X
Spezifikation der Security Module Card SMC-B Objektsystem	5.0.0	10.09.2020			X						
Gemeinsame optische Merkmale der SMC	3.8.0	30.06.2020			X	X	X				
Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0	12.08.2016									
Spezifikation Logdaten- und Betriebsdatenerfassung	1.2.0	30.06.2020								X	X
Schnittstellenspezifikation Primärsysteme VSDM	1.5.0	24.08.2016									
SchnittstellenspezifikationTransport VSDM	2.5.0	15.05.2019									
Spezifikation Systemprozesse der dezentralen TI	1.3.0	10.09.2020									
Übergreifende Spezifikation Tokenbasierte Authentisierung	1.4.0	14.05.2018									
Spezifikation TSL-Dienst	1.19.0	19.02.2021							1.18.0		1.18.0
Spezifikation VPN-Zugangsdienst	1.17.0	30.06.2021									
Spezifikation Verzeichnisdienst	1.13.1	20.04.2021									
Verfahrensbeschreibung Zulassung Anbieter ePA Aktensystem	2.4.0	03.07.2020									

Verfahrensbeschreibung Zulassung Betreiber ePA-Aktensystem	1.1.0	03.07.2020									
Verfahrensbeschreibung Bestätigung Sicherheitsgutachten ePA-Aktensystem	1.7.0	08.02.2021									
Verfahrensbeschreibung Zulassung Produkttyp ePA-Aktensystem	1.4.0	14.04.2021									
Antrag auf Zulassung als Anbieter operativer Betriebsleistungen	1.0.9	30.07.2020									
Zulassungsantrag Produkttyp ePA-Aktensystem	1.0.7	30.07.2020									

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Spezifikation KOM-LE-Clientmodul	1.11.1	20.04.2021						
Betriebskonzept Online-Produktivbetrieb	3.10.0	18.03.2021		3.8.0				
Testkonzept der TI	2.8.2	02.09.2021	2.8.0	2.7.0	2.7.0	2.8.0	2.8.0	2.7.0
Produkttypsteckbrief Konnektor (Ausbaustufe VSDM)	1.1.0	19.01.2018						
Produkttypsteckbrief Konnektor	1.0.0	04.03.2020						
Produkttypsteckbrief Konnektor	1.0.0	08.01.2021						
Produkttypsteckbrief Konnektor	1.0.0	07.04.2021						
Produkttypsteckbrief Konnektor	1.0.0	14.07.2021						
Übergreifende Richtlinien zum Betrieb der TI	2.5.1	19.02.2021		2.5.0				
Certificate Policy Gemeinsame Zertifizie-rungsrichtlinie für Teilnehmer der gematik-TSL	2.9.0	30.06.2021		2.6.0	2.6.0	X	2.7.0	2.6.0
S/MIME-Profil Kommunikation Leistungser-bringer	1.7.0	04.08.2021						
Spezifikation ePA Aktensystem	1.8.1	09.07.2021						
Spezifikation Authentisierung des Versicher-ten ePA	1.4.1	02.06.2021						
Spezifikation Basis- und KTR-Consumer	1.3.2	06.08.2021						
Spezifikation KOM-LE-Clientmodul	1.12.0	04.08.2021						

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Spezifikation des Card Operating System (COS)	3.13.1	01.11.2019						
Spezifikation CVC-Root	1.9.0	18.12.2018						
Spezifikation Trust Service Provider CVC	1.14.0	30.06.2021	X					
Datenmodell ePA	1.9.0	09.07.2021						
Spezifikation Datenmodell E-Rezept	1.2.0	19.02.2021						
Spezifikation ePA Dokumentenverwaltung	1.9.0	09.07.2021						
Spezifikation Datenschutzund Sicherheitsan-forderungen der TI an Anbieter	1.3.0	12.11.2020	X	X	X	X	X	X
Spezifikation Datenschutz- und Sicherheits-anforderungen der TI an Anbieter	1.3.0	12.11.2020						
Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur	1.3.1	23.11.2016						
Speicherstrukturen der eGK für die Fachan-wendung AMTS	1.4.0	26.10.2018						
Speicherstrukturen der eGK für die Fachan-wendung NFDM	1.1.0	02.08.2017						
Speicherstrukturen der eGK für die Fachan-wendung VSDM	1.2.1	19.02.2021						
Spezifikation der elektronischen Gesund-heitskarte eGK-Objektsystem	4.5.0	02.10.2019						
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	5.1.0	18.12.2017						
Die Spezifikation der elektronischen Gesund-heitskarte Äußere Gestaltung	3.10.0	02.10.2019						

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018						
Spezifikation ePA-Frontend des Versicherten	1.10.0	09.07.2021						
Spezifikation E-Rezept-Frontend des Versi-cherten	1.2.0	19.02.2021						
Spezifikation E-Rezept-Fachdienst	1.2.0	19.02.2021						
Spezifikation Fachdienst KOM-LE	1.14.0	04.08.2021						
Spezifikation Fachmodul AMTS	1.4.0	15.05.2019						
Spezifikation Fachmodul ePA	1.9.0	09.07.2021						
Spezifikation Fachmodul ePA im KTRConsumer	1.3.1	19.02.2021						
Spezifikation Fachmodul NFDM	1.6.0	28.06.2019						
Spezifikation Fachmodul VSDM	2.6.0	21.04.2017						
Spezifikation der gSMC-K Objektsystem	3.13.0	30.06.2021						
Spezifikation der gSMC-KT Objektsystem	4.2.0	14.05.2018						
Übergreifende Spezifikation HSM-Proxy	1.0.0	15.05.2019						
Spezifikation Identity Provider-Dienst	1.3.0	14.06.2021						
Spezifikation Identity Provider – Nutzungs-spezifikation für Fachdienste	1.2.0	19.02.2021						

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Spezifikation Identity Provider - Frontend	1.2.0	12.11.2020						
nformationsmodell eMP/AMTS-Datenma-nagement	1.5.0	02.10.2019						
Informationsmodell Notfalldaten-Management (NFDM)	1.6.0	02.03.2020						
Spezifikation Intermediär VSDM	1.12.0	02.03.2020						
Koordinierendes Informationssicherheitsma-nagement der Telematikinfrastruktur	1.4.1	23.11.2016						
Befüllvorschriften für die Plattformanteile der Karten der TI	2.6.0	24.08.2016						
Befüllvorschriften für die Plattformanteile der Karten der TI der Generation G2.1	3.0.0	18.12.2017						
Spezifikation Konnektor	5.13.0	13.04.2021						
Ergänzung zur Spezifikation Konnektor (PTV4)	1.1.0	07.04.2021						
Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telema-tikinfrastruktur	2.20.0	02.09.2021	2.19.1	2.18.0	2.18.0	2.19.1	2.19.0	2.18.0
Spezifikation Konfigurationsdienst	2.5.0	02.03.2020						
Spezifikation eHealth-Kartenterminal	3.13.3	30.06.2021						
Spezifikation KTR-AdV	1.7.0	30.06.2020						
Spezifikation Mobiles Kartenterminal	2.14.0	26.06.2020						
Übergreifende Spezifikation Netzwerk	1.20.3	31.08.2021		1.19.0	1.19.0		1.20.0	1.19.0

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Spezifikation Festlegung von OIDs	3.10.0	19.02.2021	X	3.9.0	3.9.0	X	X	3.9.0
Übergreifende Spezifikation Operations und Maintenance	1.14.0	26.06.2020	X	X	X	X	X	X
Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0	14.06.2021		2.12.0	2.12.0	X	2.12.1	2.12.0
Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur	1.3.0	14.05.2018						
Spezifikation für Prüfkarten des Typs eGK	1.2.0	26.10.2018						
Übergreifende Spezifikation Spezifikation PKI	2.10.4	14.07.2021	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.0
Spezifikation Service Monitoring	1.5.0	02.03.2020		X	X	X	X	X
Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2	19.02.2021						
Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Pro-dukte der TI	1.4.0	24.08.2016						
Spezifikation Datenschutz und Sicherheitsan-forderungen	1.4.1	23.11.2016						
Spezifikation Signaturdienst	1.4.0	12.11.2020						
Spezifikation der Security Module Card SMC-B Objektsystem	5.0.0	10.09.2020						
Gemeinsame optische Merkmale der SMC	3.8.0	30.06.2020						
Schnittstellenspezifikation Fachdienste (UFS/VSDD/CMS)	1.6.0	12.08.2016						
Spezifikation Logdaten- und Betriebsdatener-fassung	1.2.0	30.06.2020						

Komponenten & Dienste Dokumente	Version	Änderungs-datum der aktuellen Dokumen-ten-version	Trust Service Provider CVC	Trust Service Provider X.509 (nonQES) – eGK	Trust Service Provider X.509 (nonQES) – HBA	Trust Service Provider X.509 (nonQES) – Komp	Trust Service Provider X.509 (nonQES) – SMC-B	Trust Service Provider X.509 QES
Produktversion			-	-	-	-	-	-
Schnittstellenspezifikation Primärsysteme VSDM	1.5.0	24.08.2016						
SchnittstellenspezifikationTransport VSDM	2.5.0	15.05.2019						
Spezifikation Systemprozesse der dezentra-len TI	1.3.0	10.09.2020						
Übergreifende Spezifikation Tokenbasierte Authentisierung	1.4.0	14.05.2018						
Spezifikation TSL-Dienst	1.19.0	19.02.2021						
Spezifikation VPN-Zugangsdienst	1.17.0	30.06.2021						
Spezifikation Verzeichnisdienst	1.13.1	20.04.2021						
Verfahrensbeschreibung Zulassung Anbieter ePA Aktensystem	2.4.0	03.07.2020						
Verfahrensbeschreibung Zulassung Betreiber ePA-Aktensystem	1.1.0	03.07.2020						
Verfahrensbeschreibung Bestätigung Sicher-heitsgutachten ePA-Aktensystem	1.7.0	08.02.2021						
Verfahrensbeschreibung Zulassung Produkt-typ ePA-Aktensystem	1.4.0	14.04.2021						
Antrag auf Zulassung als Anbieter operativer Betriebsleistungen	1.0.9	30.07.2020						
Zulassungsantrag Produkttyp ePA-Aktensys-tem	1.0.7	30.07.2020						

Quelle: gematik GmbH, 2021a

Tabelle 6: Dokumente zur Spezifikation der Telematikinfrastruktur

Anhang D - Ergebnisse Datenanalyse zu Auswirkungen von Krankenhausausfällen

Auswertung für das Bundesland Berlin

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
BLN29	Alexianer St. Hedwig	Große Hamburger Strasse 5-11	10115	Berlin	freigemeinnützig	3.657.074	3120,7	5,7	5,8	37	0	Plankrankenhaus
	Alexianer St. Joseph-Krankenhaus	Gartenstrasse 1	13088	Berlin	freigemeinnützig							Plankrankenhaus
	ARGORA Klinik Berlin	Carmerstr. 2	10623	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Arona klinik füe Altersmedizin	Blumberger Damm 2G	12683	Berlin	privater Träger							Khs. mit Versorgungsvertrag
	Augenklinik am Wittenbergplatz	Kleiststrasse 23-26	10787	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Augenklinik Berlin-Marzahn	Brebacher Weg 15	12683	Berlin	privater Träger							Plankrankenhaus
	Augenklinik im Ringcenter	Bayreuther Straße 36	10789	Berlin	privater Träger							Plankrankenhaus
	Avicenna Klinik	Paulsborner Strasse 2	10709	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Berlin Klinik Leipziger Platz	Leipziger Platz 3	10117	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN32	BG Klinikum Unfallkrankenhaus	Warener Strasse 7	12683	Berlin	freigemeinnützig	2.976.123	3458,2	5,7	5,8	30	0	Plankrankenhaus
BLN01	Bundeswehrkrankenhaus Berlin	Scharnhorststrasse 13	10115	Berlin	öffentlich	3.746.480	2764,7	5,7	5,7	40	0	Bundeswehrkrankenhaus
	Casa Dentalis	Ringstraße 81	12203	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN05	Charité - Universitätsmedizin	Charitéplatz 1	10117	Berlin	öffentlich	3.681.097	3058	5,7	5,7	39	0	Hochschulklinik
	Chirurgia Ästhetica - Dr. Kümpel	Hundekehlestr. 32	14199	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Chirurgische Privatklinik am	Hohenzollerndamm 28a	10713	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Count Down-	Frankfurter Allee 40	10247	Berlin	freigemeinnützig							Khs. mit Versorgungsvertrag
BLN06	Deutsches Herzzentrum Berlin	Augustenburger Platz 1	13353	Berlin	freigemeinnützig	3.794.369	2390	5,8	5,8	42	0	Plankrankenhaus
BLN02	Dominikus-Krankenhaus Berlin	Kurhausstrasse 30	13467	Berlin	freigemeinnützig	2.910.462	2610,1	5,2	5,3	34	0	Plankrankenhaus
	DRK Kliniken Berlin	Spandauer Damm 130	14050	Berlin	freigemeinnützig							Plankrankenhaus
BLN09	DRK Kliniken Berlin Köpenick	Salvador-Allende-Strasse 2-8	12559	Berlin	freigemeinnützig	2.193.035	2629,2	6,0	6,4	19	0	Plankrankenhaus
BLN07	DRK Kliniken Berlin Mitte	Drontheimer Strasse 39-40	13359	Berlin	freigemeinnützig	3.855.777	2494,1	5,8	5,8	43	0	Plankrankenhaus
BLN08	DRK Kliniken Berlin Westend	Spandauer Damm 130	14050	Berlin	freigemeinnützig	3.929.833	1870,6	5,9	6,0	43	0	Plankrankenhaus
	EuroEyes AugenLaserZentrum	Bellevuestrasse 5	10785	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN10	Evangelische Elisabeth Klinik	Lützowstrasse 24-26	10785	Berlin	freigemeinnützig	3.995.159	2473,7	6,0	6,0	41	0	Plankrankenhaus
BLN11	Evangelische Lungenklinik Berlin	Lindenberger Weg 27 Haus 205	13125	Berlin	freigemeinnützig	1.997.879	1295,3	6,8	6,9	18	0	Plankrankenhaus
	Evangelisches Geriatriezentrum	Reinickendorfer Strasse 61	13347	Berlin	freigemeinnützig							Plankrankenhaus

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
	Evangelisches Johannesstift	Schönwalder Allee 26	13587	Berlin	freigemeinnützig							Plankrankenhaus
BLN12	Evangelisches Krankenhaus	Spanische Allee 10-14	14129	Berlin	freigemeinnützig	3.450.785	1980,2	5,7	5,7	36	0	Plankrankenhaus
BLN13	Evangelisches Krankenhaus	Herzbergstrasse 79	10365	Berlin	freigemeinnützig	3.037.349	4056,8	5,6	5,6	29	0	Plankrankenhaus
BLN14	Evangelisches Waldkrankenhaus	Stadtrandstrasse 555-561	13589	Berlin	freigemeinnützig	1.097.595	1683,8	5,8	6,2	12	0	Plankrankenhaus
	Fliedner Klinik Berlin	Charlottenstraße 65 / EG, 5. OG	10117	Berlin	freigemeinnützig							Khs.ohne Versorgungsvertrag
BLN15	Franziskus-Krankenhaus	Budapester Strasse 15-19	10787	Berlin	freigemeinnützig	3.795.086	2690,9	5,8	5,8	40	0	Plankrankenhaus
	Friedrich von Bodelschwingh	Landhausstrasse 33-35	10717	Berlin	freigemeinnützig							Plankrankenhaus
BLN16	Gemeinschaftskrankenhaus	Kladower Damm 221	14089	Berlin	freigemeinnützig	715.956	1976	5,9	6,4	8	0	Plankrankenhaus
	Havelklinik	Gatower Strasse 191	13595	Berlin	privater Träger							Plankrankenhaus
BLN17	Helios Klinikum Berlin-Buch	Schwanebecker Chaussee 50	13125	Berlin	privater Träger	1.865.901	1294,5	6,8	6,8	18	0	Plankrankenhaus
BLN18	Helios Klinikum Emil von Behring	Walterhöferstrasse 11	14165	Berlin	privater Träger	2.960.971	2451,8	5,4	5,4	31	0	Plankrankenhaus
	HELIOS Privatkliniken,	Schwanebecker Chaussee 50	13125	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	HELIOS Privatkliniken,	Walterhöferstrasse 11	14165	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Ida-Wolff-Krankenhaus	Juchaczweg 21	12351	Berlin	öffentlich							Plankrankenhaus
BLN19	Immanuel-Krankenhaus	Königstrasse 63	14109	Berlin	freigemeinnützig	3.327.383	1962,3	5,7	5,7	36	0	Plankrankenhaus
BLN20	Jüdisches Krankenhaus Berlin	Heinz-Galinski-Strasse 1	13347	Berlin	freigemeinnützig	3.824.346	2533	5,8	5,8	43	0	Plankrankenhaus
	Klinik "Helle Mitte"	Alice-Salomon-Platz 2	12627	Berlin	privater Träger							Plankrankenhaus
	Klinik am Kurfürstendamm	Kurfürstendamm 41	10719	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Klinik am Schlosspark Biesdorf	Elsterwerdaer Platz 1	12683	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Klinik Dr. Mertz	Kurfürstendamm 177	10707	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Klinik für	Kurstrasse 11	14129	Berlin	privater Träger							Khs. mit Versorgungsvertrag
	Klinik Pacelliallee	Pacelliallee 6	14195	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Klinik Schöneberg	Fuggerstrasse 23	10777	Berlin	privater Träger							Plankrankenhaus
	Kliniken im	Potsdamer Chaussee 69	14129	Berlin	privater Träger							Plankrankenhaus
BLN21	Krankenhaus Bethel Berlin	Promenadenstrasse 3-5	12207	Berlin	freigemeinnützig	3.127.870	2881,3	5,4	5,4	30	0	Plankrankenhaus
BLN22	Krankenhaus Waldfriede	Argentinische Allee 40	14163	Berlin	freigemeinnützig	3.332.665	2348,5	5,5	5,6	36	0	Plankrankenhaus
	M1 Med Beauty Schlossklinik	Grünauer Straße 5	12557	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Malteser-Krankenhaus	Pillkaller Allee 1	14055	Berlin	freigemeinnützig							Plankrankenhaus
BLN03	Maria Heimsuchung	Breite Strasse 46/47	13187	Berlin	freigemeinnützig	3.492.666	2403,9	5,8	5,9	37	0	Plankrankenhaus

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
BLN23	Martin-Luther-Krankenhaus	Caspar-Theyß-Strasse 27-29	14193	Berlin	freigemeinnützig	4.024.277	1807	6,0	6,1	45	0	Plankrankenhaus
	MedizinZentrum	Frankfurter Allee 231 A	10365	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	MEOCLINIC	Friedrichstrasse 71	10117	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Panorama Klinik Berlin	Badensche Straße 18	10715	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Park-Klinik Sophie-Charlotte	Heubnerweg 2 a	14059	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN24	Park-Klinik Weißensee	Schönstrasse 80	13086	Berlin	privater Träger	3.393.103	2844	5,7	5,8	32	0	Plankrankenhaus
	Paulinenkrankenhaus	Dickensweg 25-39	14055	Berlin	freigemeinnützig							Plankrankenhaus
	Plastethics GmbH	Schlüterstraße 40	10707	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Privatklinik Nikolassee	Von-Luck-Strasse 3	14129	Berlin	freigemeinnützig							Khs.ohne Versorgungsvertrag
	Privatklinik Schloßstrasse	Schloßstrasse 38-40	12165	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Privatklinik Spandau PKS GmbH	Gatower Strasse 191	13595	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN25	Sana Klinikum Lichtenberg	Fanningerstrasse 32	10365	Berlin	privater Träger	3.490.856	3250,6	5,8	5,9	36	0	Plankrankenhaus
BLN26	Sankt Gertrauden-Krankenhaus	Paretzer Strasse 12	10713	Berlin	freigemeinnützig	4.010.692	1901,2	6,0	6,1	44	0	Plankrankenhaus
	SBW Schmerzklinik Berlin	Schmolstraße 24	13086	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN27	Schloßpark-Klinik	Heubnerweg 2	14059	Berlin	privater Träger	3.841.948	1932,9	5,9	5,9	42	0	Plankrankenhaus
BLN30	St. Joseph-Krankenhaus	Wüsthoffstrasse 15	12101	Berlin	freigemeinnützig	3.968.117	2425	6,0	6,1	41	0	Plankrankenhaus
BLN31	St. Marien-Krankenhaus	Gallwitzallee 123-143	12249	Berlin	freigemeinnützig	2.931.665	2569,6	5,4	5,4	29	0	Plankrankenhaus
	Vitanas Krankenhaus für Geriatrie	Senftenberger Ring 51	13435	Berlin	privater Träger							Plankrankenhaus
	Vivantes Komfortklinik GmbH	Oranienburger Strasse 285	13437	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Vivantes Netzwerk für Gesundheit	Oranienburger Strasse 285	13437	Berlin	öffentlich							Plankrankenhaus
	West-Klinik Dahlem	Clayallee 225 b	14195	Berlin	privater Träger							Plankrankenhaus
	Zahnklinik MEDECO	Prinzenallee 89-90	13357	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Zahnklinik MEDECO	Stresemannstrasse 121	10963	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Zahnklinik MEDECO	Klosterstrasse 17-18	13581	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Zahnklinik MEDECO	Königin-Luise-Platz 1	14195	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Zahnklinik MEDECO	Mariendorfer Damm 19-21	12109	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
	Zahnklinik MEDECO Berlin-Neukölln	Karl-Marx-Strasse 27	12043	Berlin	privater Träger							Khs.ohne Versorgungsvertrag
BLN35	Vivantes Klinikum Spandau	Neue Bergstraße 6	13585	Berlin	öffentlich	2.161.492	3117,1	5,1	5,4	26	0	Plankrankenhaus
BLN28	Alexianer St. Hedwig-Kliniken Berlin	Höhensteig 1	12526	Berlin	freigemeinnützig	3.010.796	1881,4	5,7	5,8	31	0	Plankrankenhaus
BLN33	Vivantes Klinikum Kaulsdorf	Myslowitzer Str. 45	12621	Berlin	öffentlich	2.924.752	3112,6	5,8	5,9	30	0	Plankrankenhaus

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
BLN04	Campus Benjamin Franklin	Hindenburgdamm 30	12203	Berlin	öffentlich	3.597.318	2566,2	5,6	5,7	39	0	Plankrankenhaus
BLN34	Vivantes Klinikum Neukölln	Rudower Straße 48	12351	Berlin	öffentlich	3.776.200	2138,2	5,9	6,2	41	0	Plankrankenhaus
Mittelwert							**2456,4**	**5,8**	**5,9**	**34**	**0**	

Quelle: GKV-Spitzenverband, 08.10.2021

Tabelle 7: Auswirkungen von Krankenhausausfällen im Bundesland Berlin

Auswertung für das Bundesland Mecklenburg-Vorpommern

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
MV01	AMEOS Klinikum Ueckermünde	Ravensteinstr. 23	17373	Ueckermünde	privater Träger	29.142	66	18,9	38,3	0	18.154	Plankrankenhaus
MV02	Asklepios Klinik Pasewalk	Prenzlauer Chaussee 30	17309	Pasewalk	privater Träger	70.417	49,2	15,6	23,7	1	20.516	Plankrankenhaus
	BDH- Klinik Greifswald gGmbH	Karl-Liebknecht-Ring 26a	17491	Greifswald	freigemeinnützig							Plankrankenhaus
MV03	Bodden-Kliniken Ribnitz-Damgarten	Sandhufe 2	18311	Ribnitz-Damgarten	öffentlich	44.560	65,4	17,6	41,8	0	37.409	Plankrankenhaus
MV04	Dietrich-Bonhoeffer-Klinikum	Salvador-Allende-Str. 30	17036	Neubrandenburg	freigemeinnützig	106.578	95,8	13,3	31,0	0	71.597	Plankrankenhaus
MV05	DRK Krankenhaus Grimmen GmbH	Dorfstr. 39	18516	Süderholz	freigemeinnützig	72.603	77	15,1	20,2	0	19.029	Plankrankenhaus
MV06	DRK Krankenhaus Teterow gGmbH	Goethestr. 14	17166	Teterow	freigemeinnützig	36.873	35,8	11,7	20,0	1	5.875	Plankrankenhaus
MV07	DRK-Krankenhaus	Penzliner Straße 56	17235	Neustrelitz	freigemeinnützig	62.411	68,2	13,2	24,4	0	29.125	Plankrankenhaus
MV08	DRK-Krankenhaus Grevesmühlen	Klützer Str. 13-15	23936	Grevesmühlen	freigemeinnützig	111.645	105,8	13,1	17,2	1	15.549	Plankrankenhaus
	Evangelisches Krankenhaus	Gützkower Landstr. 69	17489	Greifswald	freigemeinnützig							Plankrankenhaus
	Fachklinik Waldeck	Dr.-Friedrich-Dittmann-Weg 1	18258	Schwaan	privater Träger							Plankrankenhaus
MV09	HELIOS Hanseklinikum	Große Parower Str. 47-53	18435	Stralsund	privater Träger	86.434	148,9	11,0	30,4	0	45.445	Plankrankenhaus
	HELIOS Klinik Leezen GmbH	Wittgensteiner Platz 1	19067	Leezen	privater Träger							Plankrankenhaus
MV10	Helios Kliniken Schwerin	Wismarsche Str. 393-397	19049	Schwerin	privater Träger	144.570	152,4	14,6	28,2	0	69.778	Plankrankenhaus
	Klinik Amsee GmbH	Amsee 6	17192	Waren (Müritz)	privater Träger							Plankrankenhaus

Kennzahlen und Schließungseffekte im Radius von 30 Pkw-Fahrzeitminuten

Zuordnungs-ID	Krankenhaus	Straße	PLZ	Ort	Träger	Einwohner	Einwohnerdichte (Einwohner je km²)	Durchschnittliche Pkw-Fahrzeitminuten zum nächsten Grundversorger		Anzahl Versorger im Umkreis	Einwohner, die durch die Schließung des Krankenhauses länger als 30 Pkw-Fahrzeitminuten benötigen würden, um ein Krankenhaus der Grundversorgung zu erreichen	Einrichtungstyp
								Status quo	bei Schließung			
	Klinikum Karlsburg	Greifswalder Str. 11	17495	Karlsburg	privater Träger							Plankrankenhaus
MV11	Klinikum Südstadt Rostock	Südring 81	18059	Rostock	öffentlich	285.791	293,3	13,5	14,0	2	3.015	Plankrankenhaus
MV12	KMG Klinik Boizenburg	Vor dem Mühlentor 3	19258	Boizenburg/Elbe	privater Träger	51.528	72,5	16,0	27,7	0	22.347	Plankrankenhaus
MV13	KMG Klinikum Güstrow GmbH	Friedrich-Trendelenburg-Allee 1	18273	Güstrow	privater Träger	83.146	86,3	13,9	23,5	1	14.543	Plankrankenhaus
MV14	Kreiskrankenhaus Demmin GmbH	Wollweberstr.21	17109	Demmin	öffentlich	37.654	37,7	15,6	34,4	0	25.936	Plankrankenhaus
MV15	Kreiskrankenhaus Wolgast	Chausseestr. 46	17438	Wolgast	öffentlich	45.498	73	13,9	37,7	0	33.338	Plankrankenhaus
MV16	MediClin Krankenhaus	Quetziner Str. 88	19395	Plau am See	privater Träger	34.097	41,4	20,3	33,9	0	24.215	Plankrankenhaus
MV17	Mediclin Krankenhaus am Crivitzer	Amtsstr. 1	19087	Crivitz	privater Träger	73.251	82,4	16,7	20,1	0	7.865	Plankrankenhaus
MV18	MediClin Müritz Klinikum	Weinbergstr.19	17192	Waren (Müritz)	privater Träger	35.981	44,1	12,4	37,0	0	30.845	Plankrankenhaus
MV20	Sana Hanse-Klinikum Wismar	Störtebekerstraße 6	23966	Wismar	privater Träger	101.452	102,7	13,0	23,0	1	11.672	Plankrankenhaus
MC21	Sana Krankenhaus Bad Doberan GmbH	Am Waldrand 1	18209	Hohenfelde	privater Träger	208.408	274,9	12,3	16,2	2	23.328	Plankrankenhaus
MC22	SANA Krankenhaus Rügen GmbH	Calandstr. 7/8	18528	Bergen auf Rügen	privater Träger	58.108	86,2	15,9	39,9	0	47.699	Plankrankenhaus
	Short Care Klinik Greifswald GmbH	Pappelallee 1	17489	Greifswald	privater Träger							Plankrankenhaus
	Tagesklinik für Psychiatrie/	Clara-Zetkin-Straße 16	18069	Rostock	privater Träger							Plankrankenhaus
MV23	Universitätsmedizin Greifswald	Fleischmannstr. 8	17475	Greifswald	öffentlich	84.668	129,2	10,3	31,2	1	61.995	Hochschulklinik
MV24	Universitätsmedizin Rostock	Schillingallee 35	18055	Rostock	öffentlich	279.142	379,6	12,8	14,3	2	690	Hochschulklinik
MV25	Warnow-Klinik Bützow gGmbH	Am Forsthof 3	18246	Bützow	freigemeinnützig	59.016	63,5	12,7	18,3	1	9.414	Plankrankenhaus
MV26	Westmecklenburg Klinikum	Parkstraße 12	19230	Hagenow	öffentlich	54.188	53,1	17,4	28,5	0	26.319	Plankrankenhaus
Mittelwert							**107,4**	**14,4**	**27,0**	**0,5**	**27.028**	

Quelle: GKV-Spitzenverband, 08.10.2021

Tabelle 8: Auswirkungen von Krankenhausausfällen im Bundesland Mecklenburg-Vorpommern

Anhang E - Wirkung von Gesetzen auf Akteure des Gesundheitswesens

Akteure / gesetzliche Grundlagen	Änderungs-Datum	Krankenhäuser	Vorsorge oder Rehabilitations-Einrichtungen	Medizinische Versorgungszentren	niedergelassene		Labore	Krankenkassen	Apotheke	gematik GmbH	Dienstleister	Hersteller		
					Ärzte	Zahnärzte						Von Medizinprodukten	Anwendungen der TI	Sonstige
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik	23.06.2021	X					X		X		X[1]	X[1]	X[1]	X[1]
Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz	06.09.2021	§6 und Anhang 5					§6 und Anhang 5		§6 und Anhang 5					§6 und Anhang 5
Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt	19.06.2020										X	X		X
Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik	Entwurf 28.07.2021											X	X	X
DIN EN 80001-1		X[2]	X[2]	X[2]	X[2]	X[2]								
Übergreifende Spezifikation Netzwerk	31.08.2021	X								X		X	X	
Spezifikation Datenschutz und Sicherheitsanforderungen der TI an Anbieter	12.11.2020										X			
Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	12.11.2020											X	X	
Richtlinie nach § 75b SGB V über die Anforder-ungen zur Gewährleistung der IT-Sicherheit	22.01.2021			X	X	X								
§ 75c - IT-Sicherheit in Krankenhäusern	20.08.2021	X[3]												
Medical Device Regulation	05.05.2017													

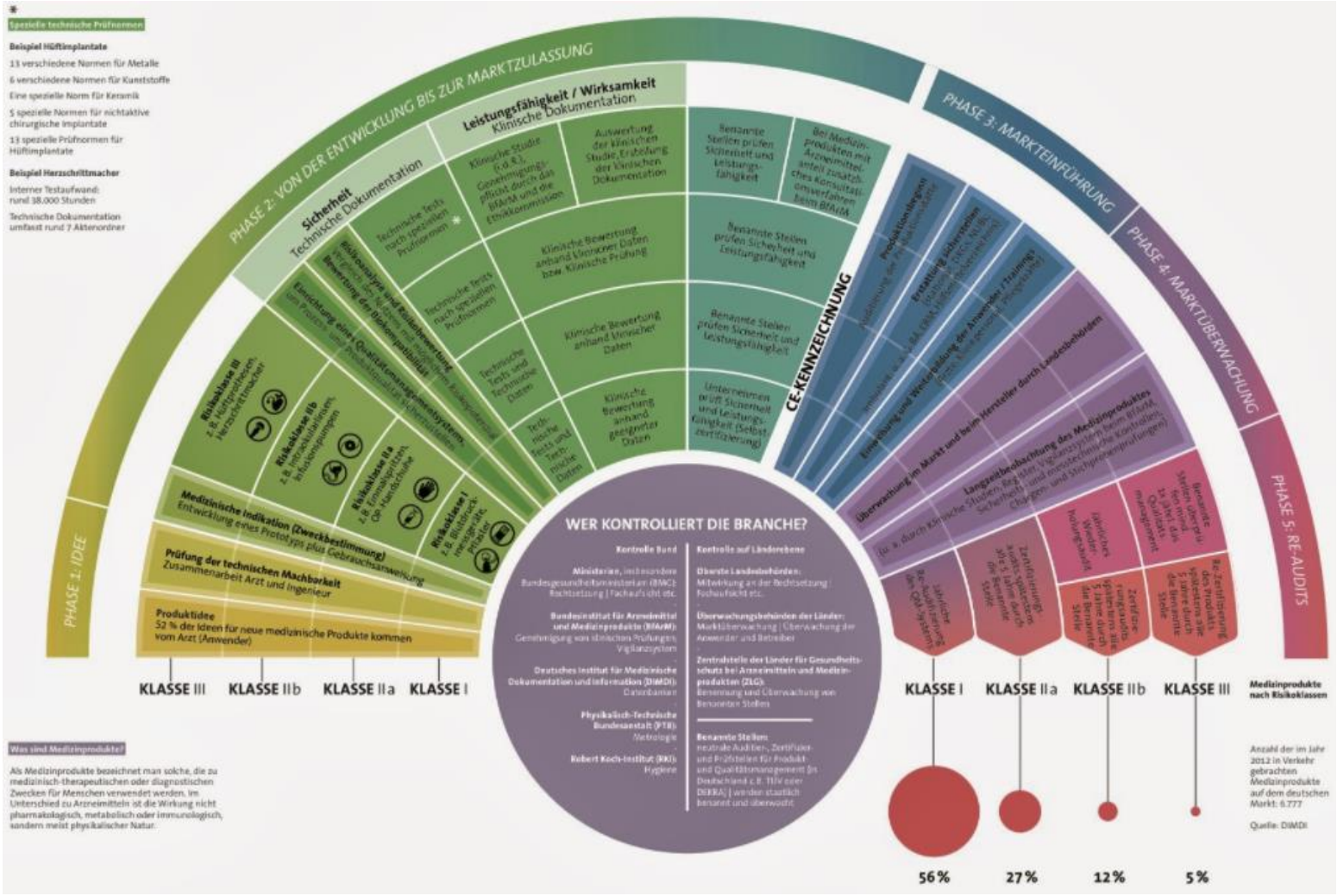
X[1] zutreffend, wenn Einstufung als Kritische Infrastruktur auf Basis §2 Absatz 10 Satz 2 BSIG

Akteure / gesetzliche Grundlagen	Änderungs-Datum	Krankenhäuser	Vorsorge oder Rehabilitations-Einrichtungen	Medizinische Versorgungszentren	niedergelassene		Labore	Krankenkassen	Apotheke	gematik GmbH	Dienstleister	Hersteller		
					Ärzte	Zahnärzte						Von Medizinprodukten	Anwendungen der TI	Sonstige
In-vitro-Diagnostika	März 20							0						
Guidance on cybersecurity for medical devices	Dezember 19	X	X	X	X	X					X[4]	X	X	
Qualification and classification of software	Oktober 19											X	X	
Datenschutzgrundverordnung	04.03.2021	X	X	X	X	X	X	X	X	X	X	X	X	X
Bundesdatenschutzgesetz	25. Mai 2018	X	X	X	X	X	X	X	X	X	X	X	X	X
Patientendatenschutzgesetz	20.10.2020	X	X	X	X	X	X	X	X	X	X			
Verordnung über künstliche Intelligenz	Entwurf 21.04.2021	X	X	X	X	X	X	X	X	X	X	X	X	X

Tabelle 9: Wirkung von Gesetzen auf Akteure des Gesundheitswesens

X[1] zutreffend, wenn Einstufung als Kritische Infrastruktur auf Basis §2 Absatz 10 Satz 2 BSIG

Anhang F - Anforderungen an Medizinprodukteklassen innerhalb des Produktentwicklungszyklus



Quelle: BVMed - Bundesverband Medizintechnologie e.V., 24.05.2018

Abbildung 29: Anforderungen an Medizinprodukteklassen innerhalb des Produktentwicklungszyklus

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt wurde.

Brandenburg, 18. Oktober 2021
Ort, Datum

Unterschrift
(Torsten Otto)