Landtag von Baden-Württemberg **Drucksache 17 / 8681**

17. Wahlperiode **10.4.2025**

Antrag

**der Abg. Jochen Haußmann und
Daniel Karrais u. a. FDP/DVP**

und

Stellungnahme

**des Ministeriums des Inneren, für Digitalisierung
und Kommunen**

Förderung einer sicheren Medizindateninfrastruktur

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche baden-württembergischen Kliniken und Krankenhäuser wann an die Cloudplattform MEDI:CUS angeschlossen werden;

2. durch wen die Mitarbeitenden der Klinken und Krankenhäuser, die mit der Cloudplattform MEDI:CUS arbeiten werden, darin geschult werden;

3. wer für die Kosten dieser Schulungen aufkommt;

4. inwiefern die Cloudplattform MEDI:CUS in der Krankenhausplanung, in den Planungen der medizinischen Versorgungsregionen sowie für den Rettungsdienst eine Rolle spielt;

5. mit welchen Stakeholdern (unter Angabe des Ergebnisses der Beratungen) gesprochen wurde, damit die Cloudplattform MEDI:CUS nicht eine Insellösung für Baden-Württemberg bleibt, sondern auf andere regionale, nationale, europäische und internationale Ebenen erweitert werden kann;

6. inwieweit bei der Konzipierung und Implementierung auf die Expertise und Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zurückgegriffen wurde;

Eingegangen: 10.4.2025 / Ausgegeben: 8.5.2025

7. inwiefern das Projekt des Ministeriums für Wirtschaft, Arbeit und Tourismus, AIDA, mit dem Projekt MEDI:CUS vernetzt gedacht und geplant wurde, damit Synergien genutzt und Doppelstrukturen vermieden werden können und somit Fördermittel gezielt eingesetzt werden;

8. welche Cyberangriffe ihr auf Kliniken und Krankenhäuser, ambulante Gesundheitseinrichtungen sowie medizinische Dienstleister in Baden-Württemberg seit 2022 bekannt sind (unter Angabe des Ausmaßes, der Art des Angriffs, der Reaktionszeit und der daraus resultierenden Konsequenzen);

9. wie sie die aktuelle Gefährdungslage von Cyberangriffen auf Kliniken und Krankenhäuser, ambulante Gesundheitseinrichtungen sowie medizinische Dienstleister in Baden-Württemberg einschätzt;

10. wie sie die Medizindateninfrastruktur hinsichtlich deren Sicherheit und einer schnittstellenfreien sektorenübergreifenden Versorgung bewertet, vor dem Hintergrund der Einführung der elektronischen Patientenakte und des E-Rezepts sowie sektorenübergreifende Patientenversorgung (beispielsweise die Übermittlung von Entlassbriefen).

10.4.2025

Haußmann, Karrais, Reith, Fischer, Birnstock, Brauer,
Bonath, Fink-Trauschel, Haag, Hoher, Dr. Jung,
Dr. Timm Kern, Dr. Schweickert, Weinmann FDP/DVP

Begründung

Schon heute sind Krankenhäuser keine geschlossenen Systeme mehr. Sie müssen mit einer Vielzahl von anderen medizinischen Einrichtungen sensitive Daten austauschen. Am 20. März 2025 hat die Landesregierung Baden-Württemberg die Cloudplattform MEDI:CUS in Berlin vorgestellt. Die cloudbasierte Plattform vernetzt Universitätskliniken, Krankenhäuser sowie perspektivisch Arztpraxen und Patienten und bringt die medizinische Versorgung voran und soll damit auch die Forschung verbessern. Die Gesundheitscloud kann die Zusammenarbeit im Gesundheitswesen – von Universitätskliniken und Krankenhäusern über die gesamte Versorgungskette hinweg – vereinfachen und so die datengestützte Gesundheitsversorgung und Forschung der Zukunft weiter vorantreiben. Bis zum Jahr 2027 soll der Regelbetrieb etabliert sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt in seinem Abschlussbericht zum Projekt Sicherheitseigenschaften von Krankenhausinformationssystemen (SiKIS) vom 10. Februar 2025 zu der Erkenntnis, dass in den Krankenhausinformationssystemen seit langen Jahren kaum oder keine Sicherheitsmechanismen, wie Verschlüsselung oder Authentifizierung, definiert wurden.

Stellungnahme

Mit Schreiben vom 5. Mai 2025 Nr. IM4-0141.5-638/29/3 nimmt das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Wirtschaft, Arbeit und Tourismus und dem Ministerium für Soziales, Gesundheit und Integration zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche baden-württembergischen Kliniken und Krankenhäuser wann an die Cloudplattform MEDI:CUS angeschlossen werden;

Zu 1.:

Langfristig sollen alle ca. 200 baden-württembergischen Kliniken und Krankenhäuser sowie weitere Leistungserbringer des Gesundheitswesens, wie beispielsweise niedergelassene Arztpraxen, die Plattform MEDI:CUS (Medizindaten-Infrastruktur: cloudbasiert, universell, sicher) nutzen können. Gemäß Projektplanung wird die Plattform im ersten Schritt für die Universitätskliniken und Krankenhäuser des Landes und damit die stationäre Versorgung bereitstehen. Im nächsten Schritt folgt der Ausbau der Anbindung des ambulanten Sektors. Bei einem komplexen Digitalisierungsprojekt wie diesem muss die Umsetzung sukzessive erfolgen.

Bis Ende Juli 2025 soll der Grundaufbau der Plattform und die Dokumentation der technischen Voraussetzungen für die Anbindung der Einrichtungen abgeschlossen sein. Darauffolgend wird ein Proof of Concept sowie die Pilotierung erster Services bei ca. 10 bis 15 Kliniken und Krankenhäusern voraussichtlich ab dem 3. Quartal 2025 angestrebt. Die Kohorte der Piloteinrichtungen wird dabei Einrichtungen aus allen Regionen Baden-Württembergs sowie unterschiedlicher Einrichtungsgrößen – von Universitätsklinikum bis kleines Haus – abdecken, um einen realen Querschnitt unterschiedlicher technischer Grundvoraussetzungen abzubilden und so den Anbindungsprozess universell zu testen und für den Roll-Out optimal vorzubereiten. Die Auswahl erfolgt transparent und unter anderem in enger Abstimmung mit der Baden-Württembergischen Krankenhausgesellschaft e. V. (BWKG) als Landesverband. Nach der erfolgreichen Pilotierungsphase wird die flächendeckende Nutzung angestrebt.

2. durch wen die Mitarbeitenden der Klinken und Krankenhäuser, die mit der Cloudplattform MEDI:CUS arbeiten werden, darin geschult werden;

Zu 2.:

Der Schulungsbedarf der teilnehmenden Einrichtungen wird auf den jeweiligen klinischen Kontext und die Beschäftigten in den IT-Bereichen abgestimmt. Die Implementierungsbegleitung und die Schulungen werden je nach den konkreten Bedarfen und Konstellationen vom Projektkernteam (internes Projektteam mit strategischem und technischem Partner) angeboten und wenn notwendig durch servicespezifische Schulungen ergänzt. Servicespezifische Schulungen können beispielsweise für konkrete Applikationen wie Messenger oder Telemedizinlösungen direkt durch den jeweiligen Anbieter sinnvoll sein.

3. wer für die Kosten dieser Schulungen aufkommt;

Zu 3.:

Während der Projektphase bis Ende 2026 sind die Schulungskosten zur Implementierungsbegleitung der ersten Einrichtungen (vgl. Stellungnahme zu Ziffer 1 und 2) bereits im Projektbudget berücksichtigt.

4. inwiefern die Cloudplattform MEDI:CUS in der Krankenhausplanung, in den Planungen der medizinischen Versorgungsregionen sowie für den Rettungsdienst eine Rolle spielt;

Zu 4.:

Aufgrund der engen Mitarbeit des Ministeriums für Wissenschaft, Forschung und Kunst in seiner Zuständigkeit für die Universitätskliniken, des Ministeriums für Soziales, Gesundheit und Integration und der BWKG im Projekt werden die Krankenhausplanung und die Versorgungsregionen explizit mitberücksichtigt. So wird bei der Besetzung der Arbeitsgruppen sowie bei der Auswahl der Piloteinrichtungen jede Versorgungsregion einbezogen.

Rettungsdienste stehen derzeit ähnlich wie der ambulante Sektor zwar noch nicht im Fokus des Projektes, sind aber als Teil der Versorgungskette ebenso relevant. Es wurden auch hierzu bereits frühzeitig Gespräche mit verschiedenen Diensten geführt, um die Bedarfe und Besonderheiten zu verstehen und vorauszudenken.

5. mit welchen Stakeholdern (unter Angabe des Ergebnisses der Beratungen) gesprochen wurde, damit die Cloudplattform MEDI:CUS nicht eine Insellösung für Baden-Württemberg bleibt, sondern auf andere regionale, nationale, europäische und internationale Ebenen erweitert werden kann;

Zu 5.:

Eine wesentliche Prämisse des Projektes ist die Förderung von Standardisierung und Interoperabilität. Es bestehen daher Kontakte zu vielen Stakeholdern über Baden-Württemberg hinaus, die das Entstehen einer Insellösung verhindern.

Durch die Zusammenarbeit mit dem GovTech Campus Deutschland wird sichergestellt, dass die entwickelte Plattform in ihrem Grundaufbau unabhängig von Ländergrenzen adaptier- und erweiterbar ist. Austauschgespräche beispielsweise mit der API-Plattform (API = Programmierschnittstellen) des britischen National Health Service NHS oder dem finnischen Bürgerportal sowie der für den Europäischen Raum für Gesundheitsdaten (European Health Data Space – EHDS) zuständigen Stelle bei der EU dienten und dienen dem Vergleich auf internationaler Ebene. Die beiden erstgenannten Stakeholder sind stark im Bereich von standardisierten bzw. offenen Schnittstellen und Interoperabilität, so konnte als Ergebnis der Ansatz von MEDI:CUS, auf eben diese Prämissen zu setzen, gegen bereits funktionierende nicht begrenzte Ökosysteme abgeglichen und als zielführend bestätigt werden. Schließlich finden mit der gematik GmbH und dem Bundesministerium für Gesundheit anlassbezogen Gespräche statt, um die Kompatibilität zu nationalen Strukturen sicherzustellen und gegenseitig die Weiterentwicklungen zu teilen.

In mehreren Ländern gibt es darüber hinaus konkrete Initiativen und Lösungen, die sich mit MEDI:CUS sehr gut ergänzen, beispielsweise das Virtuelle Krankenhaus in Nordrhein-Westfalen und die klinikIT e. G. in Bayern, die spezialisierter, aber vom Grundgedanken ähnliche Ansätze verfolgen. Als Ergebnis finden operativ und strategisch intensive und regelmäßige Austausche statt, um mittelfristig alle Synergien aus den Initiativen zu heben, das heißt bestehende Lösungen zusammenzuführen und zukünftige Lösungen gemeinsam zu entwickeln bzw. zu nutzen.

6. inwieweit bei der Konzipierung und Implementierung auf die Expertise und Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zurückgegriffen wurde;

Zu 6.:

Die Vorgaben bzw. Handreichungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden berücksichtigt. Insbesondere die Cloud-Strategie des BSI und der Kriterienkatalog C5 haben Eingang in die konzeptionellen Arbeiten gefunden. Dies gilt für die Plattformarchitektur insgesamt und auch für die Serviceleistungen, die über MEDI:CUS zum Bezug bereitgestellt werden und die entsprechende Voraussetzungen erfüllen müssen. Ferner steht dem Projekt auch ein direkter Ansprechpartner im BSI zur Verfügung, der bei Erfordernis einbezogen wird.

7. inwiefern das Projekt des Ministeriums für Wirtschaft, Arbeit und Tourismus, AIDA, mit dem Projekt MEDI:CUS vernetzt gedacht und geplant wurde, damit Synergien genutzt und Doppelstrukturen vermieden werden können und somit Fördermittel gezielt eingesetzt werden;

Zu 7.:

Das Projekt PC3-AIDA wurde von Beginn an eng mit dem zentralen Infrastrukturprojekt MEDI:CUS vernetzt. Vertreter der Universitätskliniken sind in beiden Projekten vertreten. Ein Austausch mit den assoziierten Partnern von PC3-AIDA und dem MEDI:CUS-Projektmanagement findet statt. Bereits im Vorprojekt von MEDI:CUS (2023) wurde die Anschlussfähigkeit des standortübergreifenden Bilddatenaustausches, dessen Realisierung mit dem Projekt PC3-AIDA verfolgt wird, an die Gesundheitsdateninfrastruktur der Plattform MEDI:CUS berücksichtigt. Der im Projekt PC3-AIDA entwickelte Bilddatenaustausch wurde als UseCase von der MEDI:CUS-Projektleitung in einer fachlichen Arbeitsgruppe verankert. Dadurch wurden Fördermittel gezielt eingesetzt und die Grundlage für eine landesweit intersektoral interoperable, effiziente und datenschutzkonforme Gesundheitsdateninfrastruktur in Baden-Württemberg gelegt.

8. welche Cyberangriffe ihr auf Kliniken und Krankenhäuser, ambulante Gesundheitseinrichtungen sowie medizinische Dienstleister in Baden-Württemberg seit 2022 bekannt sind (unter Angabe des Ausmaßes, der Art des Angriffs, der Reaktionszeit und der daraus resultierenden Konsequenzen);

Zu 8.:

Eine spezielle Pflicht zur Meldung von Cyberangriffen auf Kliniken und Krankenhäuser sowie ambulante Gesundheitseinrichtungen und medizinische Dienstleister besteht in Baden-Württemberg weder im stationären noch im ambulanten Bereich, weshalb die Frage nur eingeschränkt beantwortet werden kann.

Zur konkreten Cybersicherheitslage kritischer Infrastrukturen wird darauf hingewiesen, dass nach § 8b Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) das BSI die zentrale Meldestelle für diese Stellen ist. Auch hat das BSI die Aufgabe, die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik in diesem Zusammenhang wesentlichen Informationen zu sammeln und auszuwerten. Eine Auswertung ist dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2024“ des BSI zu entnehmen. Gleichwohl beschäftigen sich sowohl die Cybersicherheitsagentur Baden-Württemberg (CSBW) im Bereich des Ministeriums des Inneren, für Digitalisierung und Kommunen als auch die BWKG und die Kassenärztliche Vereinigung Baden-Württemberg (KVBW) mit dem Thema Cybersicherheit im Gesundheitswesen in Baden-Württemberg.

Der CSBW bzw. dem bei ihr angesiedelten Computer Emergency Response Team (CERT BWL) wurden folgende Sicherheitsvorfälle sowie sicherheitsrelevante Ereignisse bei Einrichtungen des Gesundheitswesens bekannt:

Jahr	**Klinik/Krankenhaus**	**Ambulante Gesundheits-einrichtungen**	**Medizinische Dienstleister**
2022	2 Sicherheitsvorfälle – 2 Ransomware	0	0
2023	3 Sicherheitsvorfälle – 1 Hacking – 1 Fehlkonfiguration/Hardware defekt – 1 Phishing 1 Sicherheitsrelevantes Ereignis – 1 Schwachstelle	0	0
2024	1 Sicherheitsvorfall – 1 Fehlkonfiguration/Hardware defekt 2 Sicherheitsrelevante Ereignisse – 1 Fehlkonfiguration/Hardware defekt – 1 Passwort-Kompromittierung	0	1 Sicherheitsvorfall – 1 Fehlkonfiguration/Hardware defekt
2025	1 Sicherheitsrelevantes Ereignis – 1 Fehlkonfiguration/Hardware defekt	0	0
gesamt	**6 Sicherheitsvorfälle** **4 sicherheitsrelevante Ereignisse**	**0**	**1 Sicherheitsvorfall**

Bei fünf der CSBW im angefragten Zeitraum gemeldeten sieben Sicherheitsvorfällen und bei allen vier gemeldeten sicherheitsrelevanten Ereignissen war die CSBW unterstützend tätig.

Die BWKG und die KVBW teilen mit, über externe Kanäle bzw. öffentlich verfügbare Medien seit 2022 exemplarisch von folgenden Sicherheitsvorfällen Kenntnis erlangt zu haben:

– Cyberangriff auf Medizin Campus Bodensee vom Januar 2022 (vgl. kma Online): Der Klinikverbund war Ziel einer Cyberattacke. Betroffen waren die Kliniken in Friedrichshafen und Tettnang. Die Versorgung blieb gewährleistet.

– Klinikverbund Südwest (2022): Im Mai 2022 war der Klinikverbund Südwest von einem Cyberangriff betroffen, der zu Systemausfällen und Einschränkungen in der Patientenversorgung führte.

– Universitätsklinikum Tübingen (2023): Im Januar 2023 berichtete das Universitätsklinikum über einen Vorfall, bei dem die IT-Infrastruktur angegriffen wurde. Es wurden Vorkehrungen getroffen, um die Systeme zu sichern und die Versorgungsqualität aufrechtzuerhalten.

– Klinikum Esslingen vom 28. November 2023 (vgl. *Teckbote.de*). Dort stellte man am 28. November 2023 einen Angriff fest, der unter Ausnutzung einer Schwachstelle in der Kommunikationssoftware Citrix ausgeführt wurde. Laut Auskunft des Klinikums wurde „gezielt Schaden“ bei einigen Servern angerichtet. Bildgebende Systeme in der Radiologie, im Bereich Ultraschall und Endoskopie waren betroffen. In der Verwaltung seien unternehmensinterne Daten gelöscht worden, Patientendaten seien jedoch nicht abgeflossen.

– Kreiskliniken (2023): Mehrere Kreiskliniken in Baden-Württemberg meldeten im Laufe des Jahres 2023 Cyberattacken, die teilweise für kurzfristige Unterbrechungen der elektronischen Patientenakten sorgten.

Die KVBW gibt außerdem an, in ihrem Ticketsystem (HelpLine) seit dem Jahr 2022 zehn Fälle gefunden zu haben. Es lassen sich diesen Fällen auch Betriebsstättennummern (BSNRs) zuordnen, jedoch gehe aus den Tickets nicht immer eindeutig hervor, ob die Praxis selbst oder das Softwarehaus (es gab in dem angefragten Zeitraum Angriffe auf große Hersteller von informationstechnischen Systemen für den ambulanten Versorgungsbereich) betroffen war. In keinem der Fälle gab es die konkrete Meldung eines Cyberangriffs. Es besteht jedoch der Verdacht, dass einige dieser Vorfälle im Zusammenhang mit solchen Angriffen stehen könnten. Die meisten Vorfälle betreffen Fristverlängerungen bei der Abgabe von Abrechnungen, fehlende Software-Updates oder Honorarkürzungen im Zusammenhang mit der Telematikinfrastruktur (TI). Zwei Tickets stammen aus dem Jahr 2025, alle anderen waren aus dem Jahr 2022. In einem Fall handelte es sich um einen Härtefallantrag.

9. wie sie die aktuelle Gefährdungslage von Cyberangriffen auf Kliniken und Krankenhäuser, ambulante Gesundheitseinrichtungen sowie medizinische Dienstleister in Baden-Württemberg einschätzt;

Zu 9.:

Die Gefährdungslage ist ausweislich des Lageberichts des BSI zur IT-Sicherheit in Deutschland 2024 grundsätzlich als hoch einzuschätzen. (abrufbar unter: *https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html*)

Auch die Erkenntnisse und Erfahrungen der CSBW zeigen, dass Krankenhäuser immer wieder von Cyberangriffen betroffen sind. Solche Angriffe können erhebliche Auswirkungen auf den Krankenhausbetrieb haben. Daher unterstützt die CSBW im Einzelfall auch diese Stellen, insbesondere bei der forensischen Analyse als Grundlage für eine schnelle Wiederherstellung der Systeme nach einem Cyberangriff.

Durch einen Cyberangriff können die IT-Systeme und die IT-basierte Kommunikation vollständig oder teilweise eingeschränkt werden. Dies gilt für alle Gesundheitseinrichtungen gleichermaßen. Um sich vor Angriffen zu schützen, müssen unterschiedliche Maßnahmen ergriffen werden, wie beispielsweise redundante Kommunikationskanäle. Eine Notfallplanung zur Minimierung von Risiken ist daher empfehlenswert. Dadurch wird die Wahrscheinlichkeit erhöht, dass die Betriebsfähigkeit einer Einrichtung trotz eines Cyberangriffs möglichst uneingeschränkt aufrechterhalten werden kann. Ein vollständiger Überblick über die in Krankenhäusern und anderen Gesundheitseinrichtungen in Baden-Württemberg umgesetzten Lösungen und Konzepte zur Sicherstellung der Versorgung in unterschiedlichen Ausnahmelagen liegt nicht vor.

Der Gesetzgeber hat die Erforderlichkeit der Erhöhung der Cybersicherheit in der Gesundheitsversorgung jedoch erkannt. Insgesamt existieren für verschiedene Betriebsbereiche gesetzliche und untergesetzliche Regelungen sowie Normen, die die Funktions- und Handlungsfähigkeit für definierte Zeiträume sicherstellen und das Risiko von Datenverlust und Betriebsunterbrechungen verringern sollen:

Die Vorgaben des § 391 Sozialgesetzbuch Fünftes Buch (SGB V) sowie des § 8a BSI-Gesetz regeln übereinstimmend, dass Krankenhäuser dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen haben, die für die Funktionsfähigkeit des jeweiligen Krankenhauses (im Sinne des medizinischen Kernprozesse und der dafür notwendigen Unterstützungsprozesse) und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Neben KRITIS-Häusern finden alle Krankenhäuser im „B3S Krankenhaus“ (Branchenspezifischer Sicherheitsstandard) einen Rahmen, anhand dem die relevanten Bereiche identifiziert und die Risiken minimiert werden können.

Auch für den Bereich der vertragsärztlichen Versorgung wurden mit dem 2024 in Kraft getretenen Digitalgesetz neue IT-Sicherheitsvorgaben festgeschrieben (vgl.

§ 390 SGB V). Die Kassenärztliche Bundesvereinigung (KBV) wurde verpflichtet die Anforderungen zur Gewährleistung der IT-Sicherheit in einer Richtlinie festzulegen. Diese Richtlinie wurde erstellt und zuletzt zum 1. April 2025 aktualisiert. Darin beinhaltet sind klare Vorgaben, die dabei helfen, Patientendaten noch sicherer zu verwalten und Risiken wie Datenverlust oder Betriebsausfall zu minimieren. Beinhaltet sind auch Vorgaben für die Steigerung der Security-Awareness von Mitarbeiterinnen und Mitarbeitern. Die KBV zertifiziert im Einvernehmen mit dem BSI außerdem IT-Dienstleister (§ 390 Absatz 7 SGB V).

10. wie sie die Medizindateninfrastruktur hinsichtlich deren Sicherheit und einer schnittstellenfreien sektorenübergreifenden Versorgung bewertet, vor dem Hintergrund der Einführung der elektronischen Patientenakte und des E-Rezepts sowie sektorenübergreifende Patientenversorgung (beispielsweise die Übermittlung von Entlassbriefen).

Zu 10.:

Die digitale Vernetzung und der dafür notwendige Datenaustausch sind Grundbausteine für ein zeitgemäßes und zukunftsfähiges Gesundheitssystem sowie für eine gute Versorgung in Deutschland. Bislang hindern fehlende einheitliche Standards, Silohaltung sowie Bedenken im Hinblick auf die Sicherheit der Daten und Informationstechnik das Fortkommen bei der Digitalisierung des Gesundheitswesens. Diese Hürden zu überwinden und ein vernetztes Gesundheitswesen zu etablieren, ist das Ziel des Bundes sowie der gematik GmbH als Nationale Agentur für digitale Medizin (vormals Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) mit den entsprechenden Anwendungen der Telematikinfrastruktur (z. B. elektronische Patientenakte – ePA – und E-Rezept) als auch des Projekts MEDI:CUS.

Bei MEDI:CUS steht dabei jedoch, anders als bei der ePA oder dem E-Rezept, nicht der individuelle Behandlungskontext im Fokus. Betrachtet werden vielmehr die in ihrer Gesamtheit verfügbaren Daten einer Klinik bzw. einer Gesundheitseinrichtung. Diese können über die MEDI:CUS-Plattform mittels einer zentralen Datenaustauschplattform für verschiedene Anwendungen nutzbar gemacht werden. Dabei wird die syntaktische und semantische Interoperabilität der Daten sichergestellt. Eine solche Art der Aufbereitung ist Grundlage der reibungslosen Nutzung verschiedener Anwendungen, die wiederum über die MEDI:CUS-Plattform, vergleichbar eines „App-Stores“ bezogen werden können. Die geplante Multicloud-Architektur schafft die Voraussetzung dafür, dass sowohl Anbieter cloudbasierter Gesundheitsanwendungen als auch die Einrichtungen selbst flexibel auf neue Lösungen zugreifen und diese einfacher als bisher auch wieder wechseln können.

Dabei werden alle seitens des Bundesgesetzgebers bzw. der gematik GmbH vorgegebenen Standards eingehalten und auch eine Anschlussfähigkeit an den EHDS sichergestellt. So wird eine reibungslose Überführung der Daten z. B. in die ePA und den EHDS ermöglicht. Die Projektverantwortlichen sind im stetigen Austausch mit den Verantwortlichen bei der gematik GmbH, insbesondere beim Kompetenzzentrum für Interoperabilität im Gesundheitswesen (KIG).

Eigene Anwendungen, die in Konkurrenz zu den bereits verfügbaren Anwendungen der Telematikinfrastruktur stehen könnten, werden in MEDI:CUS nicht entwickelt oder auf den Markt gebracht.

Während die Telematikinfrastruktur mit Ihren Anwendungen vor allem im ambulanten Bereich gut vorankommt, nimmt MEDI:CUS außerdem zunächst die stationären Versorger in den Blick, bevor in der Zukunft auch niedergelassene Ärztinnen und Ärzte und weitere Gesundheitseinrichtungen von der Dateninfrastruktur profitieren können sollen.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen