WHITEPAPER

STIFTUNG MÜNCH

MIGRATION IN DIE CLOUD ODER ON-PREMISES-BETRIEB

– worauf Krankenhäuser bei der Entscheidung achten sollten

INHALT

Management Summary 3

Einleitung 5

Warum On-Premises-Lösungen (noch immer) einen hohen Stellenwert haben 6

Cloud-Computing im Gesundheitswesen – Status quo, Potenziale, Entwicklungen 10

Welche Anforderungen eine sichere Cloud-Computing-Strategie erfüllen muss 16

Gemeinsame Vision für den Gesundheitssektor 18

Unterzeichnende des Whitepapers 19

MANAGEMENT SUMMARY

Die Digitalisierung im deutschen Krankenhaus liegt hinter dem europäischen Durchschnitt. Sie schreitet jedoch voran und verspricht viele Vorteile für Mitarbeitende, Patient:innen und das Gesundheitssystem insgesamt. Dabei stellt sich oftmals die Frage, welche Technologie für welchen Zweck geeignet ist. Bei der Adaption moderner Technologien hinkt das Gesundheitswesen im Vergleich zu anderen Branchen deutlich hinterher.[1] Das gilt auch für den Einsatz von Cloud-Diensten, also Diensten, bei denen die Datenverarbeitung und -speicherung ganz oder teilweise auf externen IT-Ressourcen basiert und die bspw. im Banken- und Versicherungswesen schon heute zur gängigen Praxis gehören.[2]

Ursachen der teils mühseligen Adaption neuer Technologien, insbesondere von Cloud-Computing, sind u. a. unscharfe und fehlende Regularien sowie mangelnde Kenntnisse über das Potenzial von Cloud-Technologien und Vorurteile. Das Verständnis von Zuverlässigkeit und Transparenz der Datenverarbeitung, Datenschutz und -sicherheit sowie Rechtskonformität sind Themen, die Krankenhäuser beim Thema Cloud beschäftigen.

Neben der Aufklärung dieser Fragen werden auch Potenziale von Cloud-Computing für Krankenhäuser im Detail aufgeführt:

1. **Entlastung des IT-Personals.** Die Wartung, das Einspielen von Updates sowie das Release-Management führen die Cloud-Anbieter selbst durch. Durch einen zusätzlichen geräte-, zeit- und ortsunabhängigen Zugriff kann der Support der Anbieter im Bedarfsfall auch kurzfristig unterstützen.
2. **Verlässliche IT-Sicherheit und umfassender Datenschutz.** IT-Sicherheit gehört für Cloud-Anbieter zum Kerngeschäft. Denn um von Kund:innen in Betracht gezogen zu werden, müssen sie die Konformität zu wichtigen Regularien und „Best Practices" bspw. durch externe Auditoren bestätigen lassen.
3. **Reduktion von Kosten.** Laut einer aktuellen McKinsey-Studie lassen sich durch die Digitalisierung im Gesundheitswesen jährlich 42 Mrd. Euro einsparen, ein Großteil der adressierten Potenziale basiert auf Cloud-Lösungen.[3]
4. **Empowerment der Patient:innen durch Datenbereitstellung.** Patient:innen möchten immer mehr Herr über ihre eigenen Daten sein und als Kommunikationspartner:innen der Ärzt:innen wahrgenommen werden. Laut Self Tracking Report nutzen bereits jetzt knapp 40 % der Patient:innen digitale Gesundheitstracker, rund 80 % der Befragten würden zudem ihre Daten für die medizinische Forschung bereitstellen.[4]
5. **Datenbereitstellung für Forschung und künstliche Intelligenz.** Über Cloud-Computing können Machine-Learning-Modelle Zugriff auf verschlüsselte Daten beteiligter medizinischer Einrichtungen erhalten, während dies anderen Parteien, z. B. dem Cloud-Provider, sicher verwehrt bleibt.[5]

1 Deutsches Ärzteblatt (zuletzt abgerufen am 16.08.2022)
2 Detecon Consulting.(zuletzt abgerufen am 25.08.2022)
3 McKinsey (zuletzt abgerufen am 25.08.2022)
4 Nexus AG (zuletzt abgerufen am 17.08.2022)
5 Cloud Computing (zuletzt abgerufen am 17.08.202)

Jedes 2. Krankenhaus in Deutschland nutzt bereits eine Cloud-Lösung in der Verwaltung, z. B. zur Archivierung.[6] Rund 80 % könnten sich vorstellen, mindestens einen Prozess oder Dienst aus der Cloud zu beziehen.

Damit Krankenhäuser Cloud-Lösungen erfolgreich einsetzen, müssen mögliche Bedenken aufgelöst werden. Softwareanbieter erreichen Vertrauen und Überzeugung durch offene Kommunikation über Verantwortlichkeiten und Risiken, aber auch durch ein vollständiges Change-Management-Konzept sowie effektive Interoperabilität.

Eine ausführliche Checkliste soll Krankenhäusern rechtliche und technische Sicherheit zum Cloud-Dienst geben, u. a. durch:

- Gewährleistung von DSGVO-Konformität
- Datenspeicherung in zertifizierten Datenzentren
- Erfüllung von BSI-Vorgaben
- Sicherheit bei Produktentwicklung
- Durchführung von Penetrationstests
- Zertifizierungen als Must-have
- E2E-Verschlüsselung medizinischer Dokumente
- Verschlüsselte Daten und Datenverbindungen
- Benutzerauthentifizierung

Gemeinsame Vision

Die Stakeholder im Gesundheitswesen müssen Hand in Hand an einer gemeinsamen Vision für die Zukunft arbeiten. Hierbei sollte nicht im Fokus der Diskussion stehen, ob die Wahl auf Cloud- oder On-Premises-Lösungen fällt. Entscheidend müssen der funktionelle Umfang sowie die Sicherheit und Zukunftsfähigkeit der Lösungen sein. Wichtig ist zudem, dass die Patient:innen im Mittelpunkt stehen, denn eine gute Patientenversorgung sowie eine Entlastung für das medizinische Personal können ohne die Ermächtigung von Patient:innen, ihre eigenen Gesundheitsdaten zu managen, nur schwer gelingen.

6 Healthcare Information and Management Systems Society (zuletzt abgerufen am 16.08.2022)

EINLEITUNG

Die Digitalisierung des Gesundheitswesens hat das Potenzial, eine nachhaltige Transformation einzuleiten, die Krankenhäusern, Mitarbeitenden und Patient:innen zugutekommen wird. Vor dem Hintergrund der COVID-19-Pandemie, einer alternden Bevölkerung und eines zunehmenden Manges an medizinischen Fachkräften benötigen Krankenhäuser intelligente digitale Lösungen, die personelle Ressourcen freisetzen. Damit sollen Mitarbeitende entlastet und Kosten gesenkt werden und eine Patientenversorgung auf höchstem Niveau erfolgen.

Schon heute unterstützen zahlreiche digitale Lösungen Krankenhäuser bei der Modernisierung und Optimierung interner Abläufe, medizinischer Leistungen, Dokumentationen sowie in der Interaktion mit Patient:innen. Der Schutz von sensiblen Patientendaten ist dabei essenziell und muss auf dem höchsten Niveau stattfinden, weshalb die Frage nach dem Betriebs- und Storage-Modell der Anwendungen und Daten kontrovers diskutiert wird. Hierbei unterscheidet man in der Regel zwischen On-Premises-Betrieb – die Daten werden lokal vor Ort auf Servern gespeichert und verarbeitet – sowie dem Betrieb in einer Public-Cloud-Lösung – hier erfolgt die Datenspeicherung und –-verarbeitung in der Regel bei einem externen Cloud-Dienstleister. Darüber hinaus gibt es hybride Modelle, die eine Kombination aus On-Premises- und Cloud-Betrieb darstellen.

Im deutschen Gesundheitswesen ist die Cloud derzeit noch kein standardmäßig eingesetztes Werkzeug. Einerseits erschweren rechtliche Hürden den Aufbau einer Cloud-Infrastruktur, andererseits halten sich gewisse Vorurteile, wie bspw. die Sorge vor unberechtigtem Datenzugriff. Auch das Thema Cloud-Computing – die Datenverarbeitung und Nutzung von Software in der Cloud – gewinnt derzeit an Bedeutung, da es ein Schwerpunktthema im Krankenhauszukunftsgesetz (KHZG) der Bundesregierung darstellt.[7] Mit dem Förderprogramm des Bundes stehen insgesamt 4,3 Mrd. Euro für die Digitalisierung der Krankenhäuser bereit. Das KHZG führt dabei die Nutzung von Cloud-Computing explizit als Möglichkeit zur Digitalisierung von Prozessen auf.

Aktuelle Nutzung von Cloud-Lösungen in deutschen Krankenhäusern

Laut einer Studie von HIMSS, dem weltweit größten Verband für IT im Gesundheitswesen, nutzt bereits jedes 2. Krankenhaus in Deutschland eine Cloud-Lösung in der Verwaltung, z. B. zur Archivierung.[8] Cloud-Lösungen werden derzeit am häufigsten für Bildspeicher (Patienten-Archivierungs- und Kommunikations-Systeme) und Verwaltungssoftware wie Microsoft Office 365 genutzt.

Etwa 80 % der Befragten konnten sich vorstellen, mindestens einen Prozess oder Dienst aus der Cloud zu beziehen.

Bei 30 % belief sich diese Zahl sogar auf 3 bis 4 Prozesse bzw. Dienste.

7 Bundesamt für soziale Sicherung (zuletzt abgerufen am 19.08.2022)

8 Healthcare Information and Management Systems Society (zuletzt abgerufen am 16.08.2022)

Warum On-Premises-Lösungen (noch immer) einen hohen Stellenwert haben

In anderen Branchen, wie etwa dem Versicherungs- und Bankenwesen, gehört Cloud-Computing bereits zum Standard. Rund 80 % aller Banken in Deutschland setzen bereits auf Cloud-Dienste, bspw. für Zahlungsdienstleistungen oder das Kundenbeziehungsmanagement.[9] Das deutsche Gesundheitswesen hinkt bei der Adaption moderner Technologien im Vergleich zu anderen Branchen und auch europäischen Ländern deutlich hinterher.[10] Auch der EMRAM-Score – ein Modell, das den Digitalisierungsgrad von Krankenhäusern auf einer Skala von 0–7 bewertet – zeigt den Nachholbedarf. Der EMRAM-Score für Deutschland lag 2019 mit einem Wert von 2,3 unter dem europäischen Durchschnitt von 3,6.[11] Die teils mühselige Adaption neuer Technologien ist unter anderem mit dem stark regulierten und komplexen Umfeld der Gesundheitsbranche zu begründen.[12] Ein weiterer Punkt ist zudem die mangelnde Kenntnis über das Potenzial der Technologien und damit verbundene Vorurteile.

Die Bedenken gegenüber Cloud-Lösungen im Gesundheitswesen drehen sich u. a. um die Zuverlässigkeit und Transparenz der Datenverarbeitung und die dauerhafte Verfügbarkeit der Daten. Eine wichtige Rolle spielen zudem die Sicherheit der Daten, die Gewährleistung des Datenschutzes sowie das Thema Datenhoheit, worauf im Folgenden noch tiefer eingegangen wird. Hinzu kommt, dass der Krankenhausmarkt stark von Legacy-Herstellern geprägt wird, sprich von Herstellern, die Produkte bereits vor einem längeren Zeitraum auf den Markt gebracht haben und deshalb von längeren Betriebszeiten ihrer Software profitieren. Nicht alle Legacy-Hersteller sind hier auf den Zug der Innovation mit aufgesprungen, wodurch potenzielle Nachteile für die Krankenhäuser entstehen können.[13]

Dr. med. Ilias Tsimpoulis,
Chief Medical Officer, Doctolib

„Wir verbauen uns wertvolle Chancen, von denen besonders Krankenhäuser profitieren könnten, wenn wir im Gesundheitsbereich eine Technologie ablehnen, die in allen sonstigen Bereichen des Lebens bereits erfolgreich zum Einsatz kommt."

9 PWC (zuletzt abgerufen am 25.08.2022)

10 Deutsches Ärzteblatt (zuletzt abgerufen am 16.08.2022)

11 Detecon Consulting (zuletzt abgerufen am 25.08.2022)

12 Europäisches Parlament (zuletzt abgerufen am 16.08.2022)

13 Devicemed (zuletzt abgerufen am 16.08.2022)

Transparenz der Datenbearbeitung und dauerhafte Verfügbarkeit der Daten

Der Fokus auf On-Premises-Lösungen resultiert oftmals aus dem Wunsch einer Gesundheitseinrichtung, die Autonomie über die eigenen Daten zu wahren und sicherzustellen, dass sie einerseits für das eigene Personal jederzeit zugänglich sind und andererseits bei Bedarf auch endgültig gelöscht werden können. Als Teil der kritischen Infrastruktur in Deutschland müssen Krankenhäuser ihre IT-Lösungen in Bezug auf Zuverlässigkeit und Leistungsfähigkeit besonders absichern.[14] Während im herkömmlichen Industriebereich eine Unterbrechung des Service unter Umständen zwar Produktionsausfälle und damit Umsatzeinbußen zur Folge haben kann, können Beeinträchtigungen, bspw. aufgrund von Internetausfall, in Gesundheitseinrichtungen zu Behandlungsausfällen oder gar Behandlungsfehlern führen.[15]

Dr. med. Jens Deerberg-Wittram, CEO, RoMed Kliniken des Landkreises Rosenheim

„In Krankenhäusern, die zur kritischen Infrastruktur gehören, werden sich Cloud-Lösungen dann durchsetzen, wenn die Hersteller die berechtigten Sicherheitsbedenken z. B. bei einem Netzausfall ernst nehmen und praktikable Lösungen anbieten. Dies setzt voraus, dass sie die Regularien und Sicherheitsvorgaben von KRITIS-Häusern im Detail kennen."

Gewährleistung des Datenschutzes und Schrems II

In kaum einer anderen Branche liegen Daten vor, die so sensibel sind wie die Gesundheitsdaten der Menschen. Das Missbrauchspotenzial dieser Daten ist groß, und die Daten sind daher besonders zu schützen. Über die Frage, ob Cloud-Computing gegenüber On-Premises-Lösungen ein besonderes Sicherheitsrisiko im Gesundheitsbereich darstellt oder ob die Daten unter Umständen durch die Nutzung cloudbasierter Infrastruktur und Technologien nicht sogar besser geschützt sind, gehen die Meinungen auseinander.

Das Urteil des Europäischen Gerichtshofes vom 16. Juli 2020 (Schrems II) hat zusätzlich zu Rechtsunsicherheiten geführt, was den rechtskonformen Einsatz amerikanischer Cloud-Provider betrifft. Laut Schrems-II-Urteil können US-Unternehmen keinen angemessenen Schutz personenbezogener Daten gewährleisten, weshalb zwischen der EU und den USA geschlossene Abkommen über den Schutz der Privatsphäre obsolet wurden.[16]

Unternehmen stehen seit dem Urteil des Europäischen Gerichtshofes vor der Herausforderung, dass insbesondere deutsche Datenschutzbehörden Datentransfers in die USA nur unter sehr engen Voraussetzungen als zulässig ansehen. Jedoch gab es wenig Hilfestellungen für Unternehmen, mit welchen technischen, rechtlichen oder organisatorischen Maßnahmen man Compliance-Risiken hätte minimieren können.

Denn selbst wenn die Daten in Europa verbleiben und z. B. in einem europäischen Rechenzentrum gehostet werden, werden aufgrund der Eingriffsbefugnisse von US-Geheimdiensten im Kontext der US-amerikanischen Gesetzgebung (FISA/Cloud-Act) immer wieder Bedenken laut, ob ein solches europäisches Cloud-Hosting durch amerikanische Anbieter von Behörden und Gerichten nicht doch als unzulässig eingestuft werden könnte. **Festzuhalten bleibt jedoch, dass Datentransfers in die USA und die Verarbeitung von personenbezogenen Daten durch amerikanische Unternehmen weiterhin erlaubt sind.**[17]

14 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (zuletzt abgerufen am 19.08.2022)

15 Deutsches Ärzteblatt (zuletzt abgerufen am 16.08.2022)

16 Visitor analytics (zuletzt abgerufen am 18.08.2022)

17 Dierks + Company (zuletzt abgerufen am 25.08.2022)

Das bestätigte auch ein Urteil des Oberlandesgerichts in Karlsruhe vom September 2022. Das Gericht stellte in seiner Urteilsbegründung klar, dass die Datenverarbeitung bei öffentlichen Vergabeverfahren weiterhin durch eine europäische Tochtergesellschaft von US-amerikanischen Cloud-Providern erfolgen darf. Wichtig sei hierbei lediglich, dass die personenbezogenen Daten in Deutschland verarbeitet würden.[18]

Maximilian Greschke,
CEO & Co-Founder, Recare

„Wir begegnen am deutschen Gesundheitsmarkt häufig dem Irrglauben, dass die besonders schützenswerten Gesundheits- und Sozialdaten im eigenen ‚On-Premises-Hosting' am sichersten aufgehoben seien. Tatsächlich deckt sich das sehr selten mit den vorhandenen IT-Kapazitäten in diesen Institutionen. Bei Cloud-Unternehmen hingegen sind die Kompetenzen in Bezug auf Anforderungen an IT-Sicherheit und Datenschutz, u. a. DSGVO, in der Zwischenzeit so ausgeprägt, dass eine Auslagerung der Daten im richtigen Setting nicht nur sicherer und zuverlässiger ist, sondern zwangsläufig auch günstiger und vor allem skalierbar."

Dr. Henrik Matthies,
CEO & Co-Founder, Honic

„Deutschland ist nicht mit einer, sondern gleich mit 17 Landesdatenschutzaufsichten gesegnet. Während andere EU-Länder das gemeinsame DSGVO-Framework zum Anlass genommen haben, ein einheitliches nationales Vorgehen zu ermöglichen, besteht in Deutschland auf föderaler Ebene noch nicht einmal ein Koordinations- oder gar Harmonisierungsgebot innerhalb der Aufsichten. Der angestrebte European Health Data Space (EHDS) fordert niedrigschwellige Möglichkeiten zur Datennutzung. Dies sollte zum Anlass genommen werden, für medizinische Versorgung und Forschung klare Gesetzesgrundlagen zu schaffen, die für alle Bundesländer einheitlich auszulegen sind."

Auf der politischen Ebene wird ein neues Datenübertragungsabkommen zwischen der EU und den USA angestrebt, das das Schrems-II-Urteil berücksichtigt und die Unsicherheit durch Rechtssicherheit auf politischer Ebene ausräumt. Das sog. Trans-Atlantic Data Privacy Framework nimmt die Privatsphäre und Freiheitsrechte der Einzelperson nach europäischem Standard in den Blick. Die Gesetzgebung ist hier klar gefordert, rechtssichere Rahmenbedingungen für alle Marktteilnehmer zu schaffen.

18 kma online (zuletzt abgerufen am 15.09.2022)

Zudem können Softwareunternehmen, die sensible Daten in die Cloud auslagern, schon heute durch zuverlässige technische Mittel wie eine Ende-zu-Ende-Verschlüsselung und Anonymisierung sicherstellen, dass das Risiko von unbefugten Zugriffen durch Dritte, bspw. US-Unternehmen oder -Behörden, deutlich reduziert wird.[19] Tiefergehende Informationen finden Sie im nachfolgenden Kapitel.

Cloud-Provider wie Microsoft und AWS bieten ihren Nutzer:innen die Möglichkeit, Daten verschlüsselt in der Datenbank zu speichern und ihren eigenen Encryption Key in die Cloud-Lösung mit einzubringen. Die Aufgabe, diesen auch konform zu konfigurieren, einzusetzen und in die eigene Applikation einzubauen, obliegt dann den Softwareanbietern.

Maximilian Greschke,
CEO & Co-Founder, Recare

„Grundsätzlich ist der Diskurs zu Schrems II absolut berechtigt und auch kritische Argumente zum Cloud-Act haben ihre Daseinsberechtigung. Was mir bei diesen oft emotionalen Diskussionen aber regelmäßig zu kurz kommt, sind die inzwischen ausgereiften und zuverlässigen technischen Möglichkeiten des Betreiberausschlusses. Durch eine Ende-zu-Ende-Verschlüsselung ist es bspw. weder Auftragnehmern noch Cloud-Dienstleistern möglich, die verarbeiteten Daten natürlichen Personen zuzuordnen. Somit haben auch US-amerikanische Muttergesellschaften oder gar US-Behörden keine realistische Chance, die verschlüsselten Daten zu entschlüsseln. Das wird in vielen öffentlichen Diskussionen nicht ausreichend abgebildet und steht damit einer differenzierten und lösungsorientierten Betrachtung der Herausforderung im Wege. Stattdessen werden höchst sensible Daten weiterhin in die Verantwortung überforderter IT-Abteilungen gegeben, deren Infrastruktur erwiesenermaßen deutlich anfälliger für Hackerangriffe oder andere interne wie externe Gefahren ist."

19 Datenschutznotizen (zuletzt abgerufen am 17.08.2022)

Cloud-Computing im Gesundheitswesen – Status quo, Potenziale, Entwicklungen

„Cloud" ist ein abstrakter Begriff, der ein breites Spektrum virtueller Lösungen und Dienste für Einzelpersonen und Unternehmen gleichermaßen beschreibt, bei denen die Datenverarbeitung und -speicherung ganz oder teilweise auf externen IT-Ressourcen (in der „Cloud"), also nicht auf dem Endgerät des Nutzers, stattfindet. Eine engere Definition erlaubt der Begriff Cloud-Computing, der auch Eigenschaften wie standardisierte Zugriffsmöglichkeiten für verschiedene Endgeräte oder die flexible, automatische Bereitstellung von benötigten IT-Ressourcen für den Anwender – ohne Interaktion durch einen IT-Mitarbeitenden – umfasst.[20] Die Vorteile von Cloud-Computing sind vor allem bedarfsorientierte Skalierbarkeit, effizientere Nutzung der IT-Ressourcen, erhöhte IT-Sicherheit durch regelbasierten Betrieb und Entlastung der IT-Mitarbeitenden. Cloud-Computing bietet viele weitere Potenziale, die besonders den Behandlungsabläufen im Gesundheitswesen zugutekommen können.[21]

Cloud-Computing-Dienste im Überblick:

Software as a Service (SaaS)	Unter SaaS versteht man ein Lizenz- und Vertriebsmodell des Cloud-Computings, mit dem Softwareanwendungen über das Internet angeboten werden. Hierbei erfolgt die Nutzung in der Regel auf Abonnementbasis.[17]
Platform as a Service (PaaS)	PaaS ist ein Service des Cloud-Computings, bei dem die Hardware sowie die Anwendungssoftware-Plattform von einem Drittanbieter bereitgestellt werden und von den Anwendern genutzt werden können.[18]
Infrastructure as a Service (IaaS)	Bei IaaS werden grundlegende IT-Ressourcen wie etwa Rechenleistung, Storage zur Speicherung von Daten sowie Netzwerkkapazitäten bereitgestellt. Hierbei behalten die Anwender Kontrolle über Betriebssysteme und Anwendungen, müssen aber üblicherweise die Infrastruktur selbst aus den benötigten Recheninstanzen und Speichern zusammenstellen.[19]

20 National Institute of Standards and Technology (zuletzt abgerufen am 26.09.2022)

21 Cloud Standards Customer Council (zuletzt abgerufen am 22.09.2022)

22 Salesforce (zuletzt abgerufen am 22.09.2022)

23 Redhat (zuletzt abgerufen am 22.09.2022)

24 Computerwoche (zuletzt abgerufen am 22.09.2022)

Beispiele für Einsatzgebiete von Cloud-Computing im Gesundheitssektor:

- die orts- und plattformunabhängige Nutzung von Software oder Anwendungen,
- der Datenaustausch zwischen verschiedenen Systemen in Echtzeit ohne umständliche Übertragung (durch eine gewährleistete Interoperabilität),
- die ortsunabhängige Verarbeitung und Analyse von Daten sowie
- die netzwerkbasierte Nutzung von Systemen.[21]

Bereits heute wird eine Vielzahl an Daten in Krankenhäusern gesammelt und verarbeitet, wie etwa klinische, Patienten- oder empirische Daten. Dies geschieht jedoch vielerorts noch immer manuell oder über überholte Systeme. Die Datenmenge wächst dabei exponentiell an, was die Verwaltung und Pflege der Daten schwierig und zeitaufwendig macht.[26] Laut eines IDC-Berichts aus dem Jahr 2018 soll das zu erhebende Datenvolumen im Gesundheitswesen deutlich schneller wachsen als in jedem anderen Sektor.[27] Die Analyst:innen erwarten bis 2025 einen Datenzuwachs von durchschnittlich 36 % pro Jahr.[28]

Die meisten Krankenhäuser sind aktuell jedoch nicht ausreichend ausgestattet, um Datenmengen dieser Größe effizient zu erfassen und zu verwalten, geschweige denn ihr volles Potenzial freizusetzen. Ein Großteil der vorhandenen Daten wird oft in Datensilos gehalten und erfordert manuelle Eingaben und Aktualisierungen. Fehlerhafte oder doppelte Dateneingaben können dann Beeinträchtigungen der Patientenbehandlung zur Folge haben.

Dr. med. Ilias Tsimpoulis,
Chief Medical Officer, Doctolib

„Ich wünsche mir, dass Krankenhäuser sich nicht den Kopf über IT-Lösungen zerbrechen müssen, sondern sich darauf fokussieren können, klinische Prozesse zu optimieren. Digitale Tools sollen sie dabei unterstützen. Genau dafür braucht es Systeme, die immer funktionieren und die automatisch im Hintergrund laufen – Cloud-Systeme werden diesen Anforderungen mehr gerecht und sind dazu noch kostengünstig."

25 Deutsches Ärzteblatt (zuletzt abgerufen am 25.08.2022)
26 I2next (zuletzt abgerufen am 17.08.2022 unter)
27 Seagate (zuletzt abgerufen am 17.08.2022)
28 Krankenhaus-IT (zuletzt abgerufen am 17.08.2022)

Potenziale, die sich durch Cloud-Computing für Krankenhäuser ergeben

1. Entlastung des IT-Personals

Nicht nur beim medizinischen Fachpersonal herrscht akuter Fachkräftemangel in den deutschen Krankenhäusern, auch in den IT-Abteilungen fehlt immer häufiger Personal. Eine IT-Infrastruktur in eigenen Rechenzentren zu betreiben bedeutet oftmals einen hohen zeitlichen Arbeitsaufwand für IT-Mitarbeiter:innen. Um das IT-Personal hier zu entlasten, sollten Fördergelder in moderne Technologien investiert und nicht länger für überholte Systeme mit teils hohen Folgekosten aufgewendet werden.

Für die Cloud in deutschen Krankenhäusern sprechen also nicht nur technisch-funktionelle, sondern auch vertraglich-wirtschaftliche Aspekte. Hier handelt es sich insbesondere um die Skalierbarkeit der IT-Kapazität und -Leistung.[29] Die Wartung, das Einspielen von Updates sowie das Release-Management führen die Cloud-Anbieter selbst durch – ohne Ausfall der Lösungen. Durch einen zusätzlichen geräte-, zeit- und ortsunabhängigen Zugriff im Bedarfsfall kann der Support der Anbieter auch kurzfristig unterstützen. Somit kann das IT-Personal stattdessen den Fokus seiner Arbeit auf die strategische, langfristige Gestaltung der IT-Landschaft im Krankenhaus legen.

Rolf Kranz,
Vorstandsmitglied, msg systems AG

„In den nächsten fünf Jahren werden nahezu sämtliche Anwendungslandschaften in der Cloud platziert werden. Dieser Weg in die digitale Transformation wird auch vor den Krankenhäusern nicht haltmachen."

Dr. med. Jens Deerberg-Wittram,
CEO, RoMed Kliniken des Landkreises Rosenheim

„Viele unserer Services haben wir in die Cloud ausgelagert, was einen deutlich geringeren Betreuungsaufwand im Bereich Maintenance und Support für unser Klinik-IT-Personal bedeutet. Gleichzeitig haben wir mit den Supportstrukturen des Cloud-Anbieters die Möglichkeit, unsere Patient:innen besser zu unterstützen und wichtige Informationen online für sie bereitzustellen."

2. Verlässliche IT-Sicherheit und umfassender Datenschutz

Im Vergleich zu anderen Industriesektoren ist das Gesundheitswesen in puncto IT-Sicherheit aktuell deutlich schlechter aufgestellt.[30] Identitätsdiebstahl, Erpressungen sowie der Verkauf von Daten stellen in der Gesundheitsindustrie ein hohes Risiko dar, weshalb für die gesundheitlichen Einrichtungen eine intensive Auseinandersetzung mit dem Thema IT-Sicherheit eine essenzielle Rolle spielt. Auch unter dem Aspekt einer immer weiter steigenden Datenmenge erhöhen sich die Anforderungen an die IT-Sicherheit. In den meisten Fällen können Cloud-Anbieter die Umsetzung dieser Anforderungen besser gewährleisten als die hauseigene Krankenhaus-IT, da Cloud-Rechenzentren vor Naturgewalten, aber auch vor Einbruch und Diebstahl durch höchste Sicherheitsvorkehrungen geschützt sind, die über die von lokalen Serverräumen hinausgehen.

29 HIMSS (zuletzt abgerufen am 19.08.2022)

30 Deutsches Ärzteblatt (zuletzt abgerufen am 17.08.2022)

Dr. Henrik Matthies,
CEO & Co-Founder, Honic

„In den letzten Jahren haben Hackerangriffe mit Lösegeldforderungen stark zugenommen, insbesondere im Gesundheitswesen, wo Daten fast ausschließlich On-Premises gespeichert sind. Clouds bieten ein skalierbares Sicherheitskonzept, das deutlich einfacher up to date gehalten werden kann. Darüber hinaus eröffnen sich neue Möglichkeiten der Datennutzung, z. B. für medizinische Forschung."

Grundsätzlich zählt IT-Sicherheit für den überwiegenden Teil der Cloud-Anbieter ohnehin zum Kerngeschäft. Denn um von Kund:innen in Betracht gezogen zu werden, müssen sie die Konformität zu wichtigen Regularien und „Best Practices" bspw. durch externe Auditoren bestätigen lassen. Zusätzlich können weitere Sicherheitsleistungen von großen Cloud-Anbietern wie Microsoft oder AWS in Anspruch genommen werden, um die Einhaltung der europäischen Datenschutzstandards einzuhalten.[31] Bei der Wahl der Cloud müssen gesundheitliche Einrichtungen besonderes Augenmerk auf die Verschlüsselung der Daten sowie den Standort des Servers legen, vor allem in Anbetracht des zuvor beschriebenen Schrems-II-Urteils.[32]

Laut Angaben der Hersteller, wie bspw. AWS, ist die Datenübermittlung in ein Drittland jedoch nicht in jedem Fall unzulässig. Hierfür gelten weiterhin die Anforderungen des Kapitels V der DSGVO. So kann eine Datenübermittlung unter Verwendung sog. Standardvertragsklauseln weiterhin DSGVO-konform erfolgen. Die Ausführungen gelten sowohl für „normale" personenbezogene Daten als auch für besondere Kategorien, wie eben Gesundheitsdaten.[33]

Admir Kulin,
CEO, mDoc

„Wenn wir ehrlich sind, funktioniert die Zukunft des Gesundheitswesens nicht ohne Cloud. Eine breit akzeptierte ePA? Ohne Cloud nicht möglich! Der Einsatz von künstlicher Intelligenz oder Natural Language Processing? Geht ebenfalls nur mit Cloud-Lösungen! Wir brauchen zwingend eine agile, anpassungsfähige und skalierbare IT-Infrastruktur – auch mit Blick auf die Kosten. Anstatt also über die Anschaffung von Hardware zu sprechen, müssten wir über Schnittstellen und Shared Infrastructure nachdenken. Nur die Cloud bietet uns den Spielraum, den wir brauchen, um den dynamischen Prozess der ‚Zukunftsgestaltung' immer wieder neu zu hinterfragen, gegebenenfalls den Kurs anzupassen, nur um dann wieder Vollgas geben zu können. Es sind also nicht ‚nur' Updates, die über die Cloud einfacher und kostengünstiger eingespielt werden können, auch eine 180-Grad-Wendung ist möglich, sollte sie morgen erforderlich sein. Was es jetzt für uns zu tun gibt? Genau diese Chance beim Schopfe zu packen und anstatt über das Für und Wider lieber darüber zu diskutieren, wie eine deutsche und/oder europäische Cloud-Lösung im Gesundheitswesen aussehen sollte. Denn dass wir sie brauchen, steht außer Frage, nur bitte nach unseren Regeln!"

31 Datenschutznotizen (zuletzt abgerufen am 17.08.2022)

32 kma online (zuletzt abgerufen am 17.08.2022)

33 Dierks + Company (zuletzt abgerufen am 25.08.2022)

3. Reduktion der Kosten

Aus kaufmännischer Perspektive bietet die Cloud skalierbare, nutzungsabhängige und flexible Preismodelle.[34] Durch die effiziente Nutzung von Cloud-Storage ergeben sich Kostenersparnisse für die Krankenhäuser, da nur tatsächlich genutzte Datenvolumen berechnet werden, ebenso kann der Personalaufwand reduziert werden.

Besonders für kleinere Krankenhäuser, die mit starkem Personalmangel im IT-Bereich zu kämpfen haben, bietet die Speicherung von Daten in der Cloud einen finanziellen Vorteil, da so auch die Kosten für die Anschaffung teurer Software sowie die Kosten für die Instandhaltung geringer ausfallen. Laut einer aktuellen McKinsey-Studie lassen sich durch die Digitalisierung im Gesundheitswesen jährlich 42 Mrd. Euro einsparen, ein Großteil der adressierten Potenziale basiert auf Cloud-Lösungen.[35] Auch eine aktuelle AWS-Umfrage zeigt das enorme wirtschaftliche Potenzial von Cloud-Lösungen: Leistungserbringer in der EU und Großbritannien können durch den Einsatz von Cloud-Lösungen in den nächsten 5 Jahren rund 14,4 Mrd. Euro einsparen, was ca. 5.665 Euro pro Krankenhausbett entspricht.[36]

Für Krankenhäuser macht es deshalb Sinn, die Potenziale von Cloud-Computing denen der On-Premises-Lösung gegenüberzustellen und Investitionen in bestehende IT-Infrastruktur kritisch zu hinterfragen. Andernfalls bleiben in den Jahren nach Auslaufen der initialen Förderung primär hohe Betriebskosten für die Nutzung überholter Technologie oder obsolet gewordene Softwarelösungen.[37]

4. Empowerment der Patient:innen durch Datenbereitstellung

Cloud-Lösungen können zudem dabei unterstützen, die Einbindung und Selbstbestimmtheit der Patient:innen zu fördern. Denn diese möchten immer mehr Herr über ihre eigenen Daten sein und als Kommunikationspartner:innen der Ärzt:innen wahrgenommen werden.

Monika Rimmele,
COO, DiGA Factory

„Während in den letzten Jahren die Digitalisierung des Gesundheitswesens auch in Deutschland deutliche Fortschritte gemacht hat, fehlt es an einer konsequenten Digitalisierungsstrategie anstelle kurzfristiger Finanzierungsansätze. Ohne diese langfristige Strategie werden staatliche Gelder punktuell und für stellenweise widersprüchliche Ziele ausgegeben. So bleibt beispielsweise beim KHZG die berechtigte Frage, wie viel der Gelder in nicht zukunftsfähige Lösungen investiert wurde. Es ist daher sehr zu begrüßen, dass das Gesundheitsministerium diesen Strategieprozess jetzt begonnen hat."

Laut Self Tracking Report nutzen bereits jetzt knapp 40 % der Patient:innen digitale Gesundheitstracker, rund 80 % der Befragten würden zudem ihre Daten für die medizinische Forschung bereitstellen. Ca. 70 % der Patient:innen möchten ihre Gesundheitsdaten in der elektronischen Patientenakte (ePa) erfassen. Die befragten Patient:innen erhoffen sich so insgesamt eine optimierte, auf ihre individuellen Bedürfnisse abgestimmte Verhaltensempfehlungen.[38]Je mehr die Patient:innen über eigene Erkrankungen sowie deren Therapieformen Bescheid wissen und mit einbezogen werden, desto höher sind die Chance und der Wille, diese bis zum Ende zu verfolgen.[39]

Auch die aktuelle „Annual European eHealth Survey" – eine jährlich durchgeführte Umfrage von HIMSS und McKinsey & Company – befragte mehr als 500 EHealth-Expert:innen aus 30 europäischen Ländern zum Thema

34 BMC (zuletzt abgerufen am 19.08.2022)
35 McKinsey (zuletzt abgerufen am 25.08.2022)
36 AWS (zuletzt abgerufen am 26.08.2022)
37 LinkedIn (zuletzt abgerufen am 17.08.2022)
38 EPatient Analytics (zuletzt abgerufen am 26.08.2022)
39 Nexus AG (zuletzt abgerufen am 17.08.2022)

Patient Empowerment. Sie gaben an, dass es für sie zunehmend wichtiger wird, Patient:innen den Zugriff auf ihre Gesundheitsdaten zu ermöglichen, damit diese ihr Therapieziel besser managen können. Das markiert eine Art Paradigmenwechsel – weg von einer krankenhauszentrierten Denkweise hin zu einer Gesundheitsversorgung, in der das Individuum eine deutlich stärkere Verantwortung für die eigene Gesundheit übernimmt.

Monika Rimmele,
COO, DiGA Factory

„Patient:innen verdienen und fordern vermehrt Zugriff auf ihre Gesundheits- und Krankheitsdaten. Eine zukunftsgerichtete, moderne Gesundheitsakte beinhaltet alle persönlichen Daten in Echtzeit. Dies erfordert eine cloudbasierte Datenhaltung – idealerweise unterstützt durch KI – sowie sichere, zertifizierte digitale Gesundheitsanwendungen, die Patient:innen in ihrem jeweiligen Gesundheits- oder Krankheitszustand helfen und dabei sicherstellen, dass die erhobenen Daten und Erkenntnisse in die Gesundheitsakte einfließen."

5. Bereitstellung von Daten für Forschung und künstliche Intelligenz

Auch für die medizinische Forschung bringt Cloud-Computing große Vorteile. Grundsätzlich können mittels maschinellen Lernens Patientendaten aggregiert und analysiert werden, wodurch Modelle entstehen, durch die die Forschung wertvolle medizinische Erkenntnisse gewinnen kann.

Eine aktuelle Herausforderung in der Forschung stellen die benötigten Rohdaten dar. Diese müssen institutsübergreifend – sprich von verschiedenen medizinischen Einrichtungen – zusammengetragen werden. Aufgrund der sensiblen Informationen ist dies datenschutztechnisch kein leichtes Unterfangen, weshalb die KI-gestützte Forschung durch den mangelnden Zugang zu Rohdaten zu scheitern drohte. Über Cloud-Computing können Machine-Learning-Modelle Zugriff auf verschlüsselte Daten beteiligter medizinischer Einrichtungen erhalten, während dies anderen Parteien, z. B. dem Cloud-Anbieter, sicher verwehrt bleibt.[40]

Prof. Dr. Jens Kleesiek,
Mitglied des Vorstands, Institut für Künstliche Intelligenz in der Medizin, UK Essen

„Wenn die eigene lokale Hardware nicht ausreicht, können Krankenhäuser Cloud-Ressourcen für das Training von KI-Algorithmen heranziehen. Dies ist energieeffizienter, nachhaltiger und ebnet den Weg zum ‚Green Hospital'. Für das Training und die Anwendung von Machine-Learning-Algorithmen hat unser Institut eine Infrastruktur entwickelt, die sich sowohl lokal als auch in der Cloud innerhalb von Minuten installieren lässt. Dies ermöglicht es, sich auf die Modellentwicklung bei der Forschung zu konzentrieren, und fördert die Wiederverwendung von (Open-Source)Softwarekomponenten."

40 Cloud Computing (zuletzt abgerufen am 17.08.2022)

Welche Anforderungen eine sichere Cloud-Computing-Strategie erfüllen muss

Damit Krankenhäuser Cloud-Lösungen erfolgreich einsetzen können, müssen zunächst Vertrauen und ein generelles Grundverständnis über die technischen Mechanismen geschaffen werden, um mögliche Bedenken aufzulösen. Hier spielen eine offene Kommunikation sowie eine gute Zusammenarbeit mit den jeweiligen Softwareanbietern eine wichtige Rolle. Gesundheitseinrichtungen, die Cloud-Dienstleistungen in Anspruch nehmen möchten, müssen die Verantwortlichkeiten und Risiken vollständig verstehen.

Eine Verschlüsselung der Daten innerhalb der Cloud und während des Datenaustausches zwischen den Nutzer:innen der Cloud muss sowohl technisch ausgeführt als auch rechtlich geregelt sein und umgesetzt werden. Auch eine strikte Benutzerauthentifizierung und -autorisierung mit entsprechenden Logdateien sind notwendig, um nur berechtigten Personen den Zugriff auf die Daten zu gewähren.

So gestalten Sie die Nutzung von Cloud-Diensten sicher und DSGVO-konform:

1. **DSGVO-Konformität**
   Eine 100 %ige Konformität mit der europäischen Datenschutzgrundverordnung und dem relevanten nationalen Rechtsrahmen sollte eine Grundvoraussetzung sein.
2. **Relevante Zertifizierungen**
   Der Datenschutz von jeweiligen Services sollte regelmäßig von anerkannten Instituten auditiert und zertifiziert werden.
3. **Datenzentren**
   Für die Datenspeicherung sollten Datenzentren genutzt werden, die den wichtigsten internationalen Standards (insbesondere ISO/IEC 27001) entsprechen.
4. **BSI-Vorgaben**
   Die Datenzentren müssen die Vorgaben des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllen (C5-Standard).[1]
5. **Verschlüsselte Daten**
   Alle Datenverbindungen sowie alle gespeicherten Daten sollten gemäß der Empfehlung des BSI und im Einklang mit aktuellen europäischen Vorgaben verschlüsselt sein.[2]
6. **Browserbasierte E2E-Verschlüsselung**
   Medizinische Dokumente sollten zusätzlich durch eine browserbasierte Ende-zu-Ende-Verschlüsselung auf Applikationsebene geschützt werden.[3]
7. **Sicherheit bei der Produktentwicklung**
   Zusätzlich können beim gesamten Produktentwicklungsprozess die sog. „Privacy by Design"- und „Security by Design"-Ansätze befolgt werden.[4]
8. **Penetrationstests**
   Der Einsatz von regelmäßigen externen Penetrationstests[5] und einem speziellen Bug-Bounty-Programm[6] gibt zusätzliche Sicherheit.

1 C5-Standard („Cloud Computing Compliance Controls Catalogue"): ein Kriterienkatalog für Cloud-Anbieter, der Mindestanforderungen an sicheres Cloud-Computing spezifiziert.

2 Entspricht den Empfehlungen des Europäischen Datenschutzausschusses (EDSA) im Nachgang zum sog. Schrems-II-Urteil vom Juli 2020 des Europäischen Gerichtshofs.

3 Zusätzlich zur TLS („Transport Layer Security"), einem Protokoll zum Schutz persönlicher Daten bei der Kommunikation von Nutzer:innen mit Anwendungen im Internet), wird eine Ende-zu-Ende-Verschlüsselung basierend auf Envelope Encryption und einer Public-Key-Infrastruktur auf der Applikationsschicht eingesetzt.

4 Der Ansatz erlaubt, Sicherheitslücken möglichst früh in der Softwareentwicklung zu identifizieren und zu beheben.

5 Penetrationstests testen die Sicherheit von Netzwerken und IT-Systemen durch Nachahmung von Hackingangriffe.

6 Bug-Bounty-Programm („Ethical Hacking"): gezielte Zusammenarbeit mit Hacker:innen, um Schwachstellen zu identifizieren.

Individuelle Herausforderungen einzelner Krankenhäuser ernst nehmen

Um Krankenhäuser von Cloud-Lösungen zu überzeugen, müssen die Cloud-Anbieter nicht nur Lösungen entwickeln, die auf die Bedürfnisse und Herausforderungen der Krankenhäuser zugeschnitten sind, sondern sie müssen auch zeigen, dass sie verlässlicher Partner sind, um den Wandel sinnvoll, erfolgreich und kompetent begleiten zu können. Sie sollten den Krankenhäusern das Potenzial verständlich darlegen und sie vor, während und nach der Implementierung mit einem umfassenden Plan und einer nachhaltigen Strategie unterstützen.

Ein so umfangreicher Wandlungsprozess hin zum Cloud-Computing kann nicht gelingen, wenn Krankenhäuser das Gefühl haben, auf sich allein gestellt zu sein. Es bedarf einer intensiven Betreuung beim Change-Management durch den jeweiligen Dienst-Anbieter und einer entsprechenden Schulung der Mitarbeitenden vor Ort.

Dr. med. Jens Deerberg-Wittram, CEO, Ro-Med Kliniken des Landkreises Rosenheim

„Die größte Herausforderung besteht nicht darin, den Kliniken einzelne Softwarelösungen aus der Cloud vorzuführen, sondern die Interoperabilität zwischen verschiedenen Lösungen und dem Klinikinformationssystem sicherzustellen. Eine nahtlose Integration in die bestehende Systemumgebung, z. B. beim Identitätsmanagement, wird entscheidend sein für die User-Akzeptanz."

Interoperabilität als Muss

In nicht wenigen Krankenhäusern sind ungeheure Datenmengen in nicht miteinander kompatiblen Dateiformaten vorhanden. Um einen effizienten Austausch dieser Daten und ein durchgehendes Zusammenspiel digitaler Dienste intern wie extern zu ermöglichen, braucht es eine vollständige Interoperabilität – sprich Systeme, die nahtlos miteinander arbeiten. Dies lässt sich nur durch eine flächendeckende Verbreitung von Standards zum Datenaustausch sicherstellen.[41]

Mithilfe von einheitlichen, interoperablen Standards sollen einerseits Datensilos vermieden und andererseits Mehrwerte aus den Daten für die Krankenhäuser, Patient:innen und das Gesundheitssystem im Allgemeinen generiert werden. Auch die aktuell zunehmend komplexer werdende IT-Landschaft mit immer mehr Systemen und Schnittstellen kann durch interoperable Standards, wie FHIR oder neueste IHE-Profile, gemanagt werden. Die neuesten Interoperabilitätsstandards sind gleich unter Berücksichtigung der Cloud-Anwendungen konzipiert worden, um deren Umsetzung zu vereinfachen.

Prof. Dr. Jens Kleesiek, Mitglied des Vorstands, Institut für Künstliche Intelligenz in der Medizin, UK Essen

„Daran, dass Standards wie FHIR und DICOM von immer mehr Herstellern und Krankenhäusern eingeführt werden, zeigt sich, wie wichtig das Thema Interoperabilität ist. In Hinsicht auf die Implementierung von FHIR in die Praxis ist Deutschland sicherlich ein Vorreiter. Dies erleichtert den Austausch und das Arbeiten mit den Daten sowie ihre Analyse. Je nachdem, wie man die Cloud nutzt (IaaS, PaaS oder SaaS usw.), muss die Kompatibilität demnach auch vom Cloud-Anbieter gewährleistet werden."

41 Deloitte (zuletzt abgerufen am 19.08.2022)

Gemeinsame Vision für den Gesundheitssektor

Die Stakeholder im Gesundheitswesen müssen Hand in Hand an einer gemeinsamen Vision für die Zukunft arbeiten. Durch eine zunehmende Anzahl an Patient:innen und somit auch Daten wird ein Datenzugriff für unterschiedliche interne und externe Leistungserbringer erforderlich sein, weshalb die IT in Krankenhäusern künftig eine zentrale Rolle einnehmen wird. Krankenhäuser, die sich zukunftssicher aufstellen möchten, sollten Lösungen einsetzen, die skalierbar sind und den Austausch mit externen Parteien, wie Patient:innen, Forschungseinrichtungen usw., ermöglichen.

Hierbei sollte nicht im Fokus der Diskussion stehen, ob die Wahl auf Cloud- oder On-Premises-Lösungen fällt. Entscheidend müssten der funktionelle Umfang sowie die Sicherheit und Zukunftsfähigkeit der Lösungen sein. Wichtig ist zudem, dass die Patient:innen im Mittelpunkt stehen, denn eine gute Patientenversorgung sowie eine Entlastung für das medizinische Personal können ohne die Ermächtigung von Patient:innen, ihre eigenen Gesundheitsdaten zu managen, nur schwer gelingen. Daten müssen unabhängig von Zeit und Ort verfügbar gemacht werden, um Patient:innen zu motivieren, die eigene Gesundheitsversorgung mit in die Hand zu nehmen. Denn gut informierte Patient:innen sind besser in der Lage, Gesundheitsangebote auf individueller Ebene zu beurteilen, Entscheidungen für oder gegen Therapien besser zu treffen und diese schlussendlich aktiv umzusetzen.[42]

Für eine moderne Patientenversorgung müssen sich die Stakeholder in den Krankenhäusern offen gegenüber neueren, in anderen Märkten bereits fest etablierten Technologien zeigen, und hierbei bedarf es der Unterstützung seitens der Anbieter und Stakeholder, das Potenzial und den Nutzen der jeweiligen Lösungen darzulegen.

STIFTUNG MÜNCH

Die Stiftung Münch wurde 2014 von Eugen Münch ins Leben gerufen. Das Stiftungsziel ist es, trotz einer alternden Gesellschaft weiterhin allen Menschen den Zugang zu nicht rationierter Medizin zu ermöglichen. Als Grundlage dient das von Eugen Münch entwickelte Konzept der Netzwerkmedizin. Die Stiftung unterstützt Wissenschaft, Forschung und praxisnahe Arbeiten in der Gesundheitswirtschaft und fördert den nationalen und internationalen Austausch. Sie arbeitet unabhängig und stellt ihr Wissen öffentlich zur Verfügung. Den Vorstand bilden Prof. Dr. Boris Augurzky (Vorsitz), Eugen Münch (stellv. Vorsitz), Prof. Dr. med. Bernd Griewing und Dr. Christian Zschocke; die Geschäftsführung liegt bei Annette Kennel.

42 Bundesverband Managed Care e. V. (zuletzt abgerufen am 19.08.2022)

Unterzeichnende des Whitepapers

Dr. med. Ilias Tsimpoulis, Chief Medical Officer Doctolib

Dr. med. Ilias Tsimpoulis ist promovierter Mediziner, Chief Medical Officer und VP Strategy bei Doctolib, wo er die Krankenhausstrategie leitet. Nach seinem Medizinstudium arbeitete er in der Abteilung für Radiologie an der Uniklinik Köln und anschließend in der strategischen Unternehmensberatung sowie für ein DAX-Unternehmen. Im Mai 2018 kam Dr. Tsimpoulis als Director Hospitals, Health Systems and Partnerships zu Doctolib und war von 2019 bis 2022 Managing Director in Deutschland. Durch seine langjährige Erfahrung in der Gesundheitsbranche kennt Dr. Tsimpoulis die Bedürfnisse der Zielgruppe Ärzt:innen und Kliniken aus erster Hand. Doctolib bietet u. a. ein Patientenportal für Krankenhäuser nach KHZG und wird heute bereits von mehr als 10 Mio. Patient:innen und über 20.000 Ärzt:innen in Deutschland genutzt.

Dr. med. Jens Deerberg-Wittram, CEO der RoMed Kliniken des Landkreises Rosenheim

Dr. med. Deerberg-Wittram ist seit 2019 Geschäftsführer und medizinischer Direktor der RoMed Kliniken. Vorher war er Director bei der Boston Consulting Group (BCG). Von 2012 bis 2014 war er der Gründungspräsident Patient:innen International Consortium for Health Outcomes Measurement, gegründet von der Harvard Business School, dem Karolinska Institutet und von BCG. Er arbeitete über 15 Jahre als Geschäftsführer einer privaten Klinikgruppe, als Berater bei BCG und im Management eines führenden Medtech-Unternehmens. Von 2012 bis 2015 war er Senior Fellow am Institute for Competitiveness and Strategy von Prof. Michael Porter an der Harvard Business School.

Maximilian Greschke, Co-Founder & CEO Recare

Maximilian Greschke studierte VWL an der Universität St. Gallen und Informatik an der Harvard University. Er brach sein Studium ab, um 2013 eine Technologiefirma im Bereich Retail Analytics in Berlin zu gründen. Nach dieser ersten unternehmerischen Erfahrung wechselte er 2014 zu der deutschen Start-up-Erfolgsgeschichte „Delivery Hero", wo er das Big-Data-Team aufbaute. Anfang 2017 gründete er die cloudbasierte Entlassmanagement-Plattform Recare, die mit ihren digitalen Lösungen den Versorgungspfad zwischen Kliniken, nachgelagerten Leistungserbringern und Kostenträgern optimiert und heute eine der führenden Plattformen für Versorgungskoordination im Gesundheitswesen ist.

Moon Kim, Wissenschaftlicher Mitarbeiter, Universitätsmedizin Essen (UME)

Moon Kim ist wissenschaftlicher Mitarbeiter in der Arbeitsgruppe Medizinisches Maschinelles Lernen am Institut für Künstliche Intelligenz in der Medizin (IKIM) der Universitätsmedizin Essen (UME). Seine Forschungsschwerpunkte sind Entwicklung von medizinischen Biomarkern für bessere Diagnostik und Therapiekontrolle von onkologischen Patient:innen, Anwendung von KI-Algorithmen zur besseren bildgebenden Diagnostik und Kuration medizinischer Daten für maschinelles Lernen. Er leitet außerdem das Annotation Lab, das sich auf die Annotation von medizinischen Daten spezialisiert hat. Er studierte Wirtschaftswissenschaften an der Ruhr-Universität Bochum und Medizin an der Universität Duisburg-Essen, wo er aktuell in Medizin promoviert.

Prof. Dr. Jens Kleesiek, Mitglied des Vorstands, Institut für Künstliche Intelligenz in der Medizin (IKIM)

Jens Kleesiek ist Inhaber des Lehrstuhls für Translationale bildgestützte Onkologie und leitet die Abteilung Medizinisches Maschinelles Lernen am Institut für Künstliche Intelligenz in der Medizin (IKIM) der Universitätsmedizin Essen (UME). Schwerpunkte seiner Forschung sind die Anwendung selbstüberwachter und schwach überwachter Lernparadigmen zur Erkennung klinisch relevanter Muster, die Integration multimodaler Datenquellen zur Verbesserung des Entscheidungsprozesses am Point of

Care und die Entwicklung von Infrastrukturen zur Bereitstellung von Daten für maschinelle Lernanwendungen. Er studierte Medizin in Heidelberg und Bioinformatik in Hamburg, wo er 2012 in Informatik promovierte. Nach der Ausbildung am Universitätsklinikum Heidelberg und am Deutschen Krebsforschungszentrum (DKFZ) erlangte er die Facharztreife in Radiologie, die Habilitation (venia legendi) und die Zusatzweiterbildung in der Medizinischen Informatik.

Rolf Kranz, Vorstandsmitglied msg

Rolf Kranz ist seit 2020 Mitglied des Vorstands der msg systems ag. Als Teil des Vorstandsteams, das für die Branche Insurance verantwortlich ist, treibt er das versicherungsspezifische Solution-Consulting-Geschäft der msg voran. Darüber hinaus verantwortet er die Branche Healthcare und leitet die Bereiche Insurance Internal Services, Global Delivery Services sowie Corporate Security & Quality. Zudem verantwortet er die Gruppenunternehmen PiAL, msg Romania, edith.care und SDA. Der Diplom-Informatiker ist seit über 20 Jahren in der IT-Branche tätig und ein ausgewiesener Kenner der Versicherungsindustrie und der Gesundheitsbranche. In seiner Karriere hat er zahlreiche Projekte zur Ausrichtung der IT und Transformation von Anwendungslandschaften begleitet. Zuletzt war er als Geschäftsbereichsleiter bei msg tätig und hat dabei u. a. die Marktsegmente Gesetzliche Krankenversicherung und Gesetzliche Unfallversicherung mit aufgebaut.

Admir Kulin, CEO mDoc

Admir Kulin wurde 1980 im heutigen Bosnien geboren und kam in den 1990er-Jahren nach Deutschland. Hier begann er eine Karriere als Profi-Basketballspieler und -trainer und absolvierte zeitgleich sein Studium der Wirtschaftswissenschaften mit Schwerpunkt Sportmanagement und Controlling. In den darauffolgenden Jahren arbeitete er als Leiter Controlling bei der Label of Sportswear GmbH und war als IT-Projektleiter bei der Nürburgring Automotive GmbH tätig. Anschließend wechselte er in die Gesundheitsbranche zur Vitaphone GmbH. Dort bekleidete er verschiedene Positionen und war zuletzt Mitglied der Geschäftsleitung. Heute verantwortet Admir Kulin als Gründer und Geschäftsführer der m.Doc GmbH die gesamte Ausrichtung des Unternehmens. Er ist als Spezialist für den Gesundheitsmarkt sowie digitale Plattformen und für seine innovativen Ideen und Geschäftsmodelle bekannt und deutschlandweit als Sprecher für IT- und Healthcare-Themen gefragt.

Dr. Henrik Matthies, Founder & CEO Honic

Dr. Henrik Matthies ist CEO und Mitgründer von Honic, der souveränen Forschungsplattform für deutsche Gesundheitsdaten. Bis Ende 2021 war er Managing Director des health innovation hub (hih) des Bundesministeriums für Gesundheit und hat zuvor mehrere Technologieunternehmen gegründet und aufgebaut. Durch seine sehr unterschiedlichen Erfahrungen bringt er die aktuellen technischen Möglichkeiten mit den besonderen Anforderungen des Gesundheitswesens zusammen.

Monika Rimmele, COO DiGA Factory

Monika Rimmele ist Politikwissenschaftlerin mit einem Master of Public Policy (MPP) von der Hertie School in Berlin. Im Laufe ihrer Karriere hat sie für alle drei Sektoren gearbeitet, u. a. für das Bundesministerium für Gesundheit, den Bundesverband Gesundheits-IT (bvitg) und Siemens Healthineers, dort zuletzt als Head of Digital Transformation. Ihre Schwerpunktthemen sind digitale Transformation, innovative neue Technologien, zukünftige Gesundheitssysteme und Green Health. Seit September 2022 ist Monika Rimmele Chief Operating Officer bei der DiGA Factory, die gemeinsam mit Kunden und Partnern digitale Gesundheitsanwendungen (DiGAs) und andere Innovationen auf den deutschen Markt bringt und damit zur digitalen Transformation des deutschen Gesundheitswesens beiträgt.

Dr. med. Mani Rafii

Dr. Mani Rafii blickt auf vielfältige Perspektiven im Gesundheitswesen zurück. Zuletzt war er Mitglied des Vorstands der BARMER. Mehr als 10 Jahre hat er als Klinikmanager und Geschäftsführer für eine private Klinikgruppe Verantwortung für Krankenhäuser übernommen. Zuvor war er für die Boston Consulting Group (BCG) tätig. Mani Rafii ist promovierter Mediziner. Aktuell berät und unterstützt er unterschiedliche Unternehmen des Gesundheitswesens als Senior Advisor in strategischen Fragestellungen.