12 Bildung von digitalen Health-Ökosystemen am Beispiel von Norwegen

Cornelius Maas

Skandinavien genießt seit Jahren seinen Ruf als Vorreiter in Sachen Digitalisierung und Gesundheitsversorgung – gerade, weil dort, insbesondere regulatorisch, einige Aspekte anders gehandhabt werden als in Deutschland.

12.1 Veränderungsbedarf in Deutschland

Leider beginnt für die Mehrheit der Patienten in Deutschland, die psychologische Beratung wahrnehmen möchten, ein zusätzlicher, mühsamer Leidensweg. Zunächst müssen sie im Regelfall ihren Hausarzt erreichen, oftmals verbunden mit telefonischen Warteschleifen, bis sie einen Termin erhalten. Ist der Termin vereinbart, werden sie untersucht und zu einem Psychotherapeuten überwiesen. Nach einem Erstgespräch mit dem Therapeuten beginnt die eigentliche Wartezeit erst. Denn: Hierzulande beträgt die durchschnittliche Wartezeit auf eine Zusage für einen Therapieplatz drei bis sechs Monate. Die Frustration, die sich für die leidtragenden Patienten einstellt, führt nicht selten dazu, dass sie aufgeben und sich mit ihrer Situation abfinden. Und das geschieht gerade im größten Gesundheitsmarkt Europas, der dafür prädestiniert sein müsste, qualitativ hochwertige Gesundheitsdienstleistungen anzubieten. Diese Wartezeiten liegen vor allem in der Mangel an kassenärztlichen Psychotherapeuten. Es ist jedoch nicht so, als gäbe es per se zu wenig Therapeuten – Das entscheidende Stichwort lautet: Kassensitz. Einen Kassensitz benötigt jeder Arzt, um seinen Patienten Leistungen anbieten zu können, von denen etwa 90% von der gesetzlichen Krankenkasse übernommen werden (Verband der Ersatzkassen e.V. 2022). Vor über 20 Jahren hat die Kassenärztliche Bundesvereinigung eine Bedarfs-

planung vorgenommen, nach der die Zahl der Kassensitze genau festgelegt wurde. Damit sollte verhindert werden, dass sich zu viele Kassenärzte an einem Ort niederlassen, um das medizinische Angebot angemessen verteilen zu können. Aber seit 1999 wurde die Anzahl der Kassensitze nicht mehr entsprechend der steigenden Nachfrage angepasst. Die wachsende Zahl der Patienten muss also mit der unzureichenden Anzahl von Ärzten, die gemäß einem älteren Erlass bestimmt und fortgeschrieben wurde, zurechtkommen.

Digitale Gesundheitsangebote haben viele Bezeichnungen und Funktionen, gemeinsam haben sie jedoch, dass sie den Zugang zur medizinischen Versorgung für Patienten erleichtern und den Betrieb für Ärzte effizienter gestalten und patientenorientierter machen können.

An Digital-Health-Start-ups mit entsprechenden Produkten mangelt es in Deutschland nicht, es sind eher die regulatorischen Rahmenbedingungen in der Umsetzung, denn diese sind für digital affine Mediziner wie auch Patienten teilweise sehr umfangreich. Selbst für vollständig digitale kassenärztliche Dienstleistungen, die Fernkonsultationen in ganz Deutschland ermöglichen könnten, wird ein Kassensitz benötigt, was das Angebot deutlich schmälert. Den Medizinern bleibt ohne Kassensitz daher nur das Ausweichen auf privatärztliche Leistungen, welche in Deutschland aufgrund der hohen Quote der gesetzlich Versicherten keinen adäquaten Ersatz bietet. Die in Deutschland weit verbreiteten Medizinischen Versorgungszentren (kurz MVZ), die kassenärztlich abrechnen können, müssen sich darüber hinaus an die Maßgabe halten, maximal 70% ihres Betriebs offline – also physisch – zu unterhalten.

12.2 Norwegen als Vorbild

Anders als in Deutschland gibt es in Norwegen keine Kassensitz-Regelungen. Der Bedarf an zusätzlicher Gesundheitsversorgung wird regelmäßig von regionalen Institutionen evaluiert und, wenn notwendig, können weitere Ärzte in den Katalog aufgenommen werden (Tikkanen et al. 2020). Auch die Regelungen hinsichtlich des digitalen Gesundheitsangebots sind anders: Im dem bereits Anfang 2000 von der norwegischen Regierung veröffentlichten Papier eNorway wird etwa Telemedizin nicht als zukünftige Option, sondern als Notwendigkeit dargelegt (Knudsen 2000).

Im dem bereits Anfang 2000 veröffentlichten Papier eNorway wird etwa Telemedizin nicht als zukünftige Option, sondern als Notwendigkeit dargelegt (Knudsen 2000).

Die eigens zu diesem Zweck gegründete Behörde für eHealth überwacht die Fortschritte und treibt die Modernisierung des Systems voran. eHealth gehört in Norwegen zu den Branchensegmenten mit der höchsten F&E-Intensität, Rezepte erhalten Patienten mittlerweile zu 80% digital (Germany Trade und Invest 2019) und auch die Konnektivität im Gesundheitssystem ist fortgeschrittener als in Deutschland: Allgemeinmediziner, Spezialisten und Krankenhäuser kooperieren in der Abwicklung von Fernkonsultationen und engagieren sich in Projekten, die danach als Empfehlungsgrundlage auf nationaler Ebene vorliegen. Eine wichtige Rolle spielen auch die Versicherungsunternehmen, denn obwohl auch die gesetzliche Krankenversicherung digitale Angebote abdeckt, schließen immer mehr Norweger private Zusatzversicherungen ab. Dieser neue Raum zur privatärztlichen Behandlung erschließt auch neue Märkte neben der Abrechnung

über die gesetzliche Versicherung. Die privaten und gesetzlichen Versicherungen sprechen sich für digitale Gesundheitsangebote aus und übernehmen zunehmend mehr digitale Leistungen. Die Lenkungswirkung dieser Unternehmen führt dazu, dass sich digitale Angebote immer mehr etablieren (Germany Trade and Invest 2019).

Kein Wunder also, dass sich Geschäftsmodelle im Bereich Digital-Health in Norwegen etablieren. Neben den rein-digitalen Angeboten gibt es auch Ansätze, nach denen Erstkonsultationen digital und Folgeberatungen bei Bedarf physisch abgehalten werden – und anders herum. So werden die Vorzüge der digitalen Konsultationen, Verschreibungen und Überweisungen bestmöglich genutzt und gleichzeitig der physische Arztkontakt aufrechterhalten.

Um zu verstehen, wie sich durch die günstigen regulatorischen Rahmenbedingungen digitale Ökosysteme entwickeln, die den PatientInnen eine komfortable, effiziente, ganzheitliche Behandlung ermöglichen, lohnt sich ein Blick auf den führenden Anbieter solcher *digi-physical*-Gesundheitsdienstleistungen: Dr. Dropin.

> Das Angebot von Dr. Dropin zeichnet sich durch eine ganzheitliche Gesundheitsversorgung aus – und schafft gleichzeitig einen gesundheitlichen und ökonomischen Mehrwert für Patienten, Ärzte und Versicherer. Dank agiler Strukturen können Patienten per App über ihr Smartphone Termine meist noch am selben Tag buchen, ohne lange Warteschleifen am Telefon. Aufgrund der Interoperabilität des Angebots kann vom behandelnden Allgemeinmediziner direkt eine Überweisung zum hauseigenen Spezialisten ausgestellt werden – vollständig digital und papierlos – sodass der Patient direkt Zugang zu Physio- oder Psychotherapeuten, aber auch Fachärzten erlangt. Dadurch, dass der Patient im Ökosystem des Unternehmens verbleibt, sind zudem präventive Maßnahmen wie Trainings- und Ernährungspläne viel eher vermittelbar, sodass gesundheitliche Risiken vermindert werden. Daraus ergeben sich nicht nur gesundheitliche Vorteile für den Patienten, sondern auch Kostenersparnisse für die Krankenversicherungen.

12.3 Potenziale für Deutschland

So vorteilhaft der skandinavische Markt hinsichtlich Digital-Health auch ist – er bleibt verhältnismäßig klein. Darum drängen Unternehmen aus dem nordischen Raum vermehrt in die großen Gesundheitsmärkte Europas, wie beispielsweise Großbritannien, Frankreich und Deutschland. Den vergleichsweise liberalen regulatorischen Bedingungen aus ihren Heimatmärkten begegnen sie dort nicht. Die Kassensitzproblematik, die nicht oder unzureichend vorhandenen Gesetzesgrundlagen für Telemedizin und die insgesamt unzulängliche digitale Infrastruktur stellen selbst die vielversprechendsten Unternehmen vor die Schwierigkeit, ihre Geschäftsmodelle auf den deutschen Markt zu übertragen.

Die Akzeptanz digitaler Gesundheitsangebote seitens der Politik und der Bevölkerung in Deutschland schreitet gleichzeitig voran. Seit September 2020 können digitale Gesundheitsangebote (kurz DiGAs) von einem Behandelnden verschrieben und von der Krankenkasse (somit kostenfrei für die Patienten) übernommen werden. Erstattungs-

fähige Angebote sind im DiGA-Verzeichnis gelistet und werden vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) geprüft. Firmen wie das Unternehmen Selfapy aus Berlin können so psychologische, erstattungsfähige Online-Kurse per App anbieten und füllen die lange Wartezeit, bis eine Therapie mit einem kassenärztlichen Psychotherapeuten erfolgen kann. Ab September dieses Jahres soll zusätzlich flächendeckend das E-Rezept eingeführt werden. Zukünftig soll also jede Apotheke E-Rezepte einlösen können. Auch das Krankenhauszukunftsgesetz treibt eine zunehmende Digitalisierung der Krankenhäuser und eine demzufolge verbesserte Konnektivität voran.

Unangetastet zu bleiben scheint die Kassensitz-Thematik: Die Kassenärztliche Bundesvereinigung sieht keinen Handlungsbedarf hinsichtlich der veralteten Vergabe und spricht sich gegen eine Erweiterung des Angebots und eine Neuauflage der diesbezüglichen Erlasse aus. Fraglich ist zudem, ob die teilweise signifikanten Preisreduzierungen der zuständigen Behörden für digitale Gesundheitsanwendungen angemessen sind angesichts der (berechtigten) Erfordernisse, welche DiGA-Anbieter im Sinne klinischer Evidenz und Datensicherheit erbringen müssen.

In Anlehnung an die Modelle anderer Länder gibt es also realisierbare Möglichkeiten, das Gesundheitssystem in Deutschland patienten- und versorgerfreundlicher zu gestalten. Dies kann am eingangs skizzierten Szenario verdeutlicht werden: Wenn Patienten psychotherapeutische Hilfe in Anspruch nehmen möchten, könnten sie in einem digitalisierten Gesundheitssystem unkompliziert einen Termin bei einem Allgemeinmediziner per App anstatt per Telefon vereinbaren digital oder physisch. Eine Überweisung könnte vollständig digital erfolgen, entweder direkt zu einem Psychotherapeuten oder auch überbrückend für eine digitale Gesundheitsanwendung wie die Online-Kurse von Selfapy. In einem verknüpften Gesundheitsökosystem ist hochqualitative Gesundheitsversorgung keine Option, sie wird durch Digitalisierung ermöglicht.

Literatur

Germany Trade and Invest (2019) Gesundheitsmarkt Skandinavien. URL: https://www.exportinitiative-gesundheitswirtschaft.de/EIG/Redaktion/DE/Publikationen/PDF/gesundheitsmarkt-skandinavien.pdf?__blob=publicationFile&v=2 (abgerufen am 23.09.2022)

Knudsen G (2000) eNorway – Action Plan. In: Regjeringen.no. URL: https://www.regjeringen.no/no/dokumenter/enorway-action-plan/id105562/ (abgerufen am 23.09.2022)

Tikkanen R, Osborn R, Mossialos E, Djordjevic A, Wharton GA (2020) International Healthcare System Profiles: Norway. URL: https://www.commonwealthfund.org/international-health-policy-center/countries/norway (abgerufen am 23.09.2022)

Verband der Ersatzkassen e.V. (2022) Daten zum Gesundheitswesen: Versicherte. URL: https://www.vdek.com/presse/daten/b_versicherte.html (abgerufen am 23.09.2022)

Dr. Cornelius Maas

Nach Beendigung seiner Profisport-Karriere stieg Cornelius Maas im Jahr 2015 bei der Venture Capital und Private Equity Gesellschaft SHS Capital ein. Als Partner verantwortet er beim Tübinger Fonds den Bereich Dealflow und ist verantwortlich für mehrere HealthTech-Investments von SHS wie Selfapy oder Dr. Dropin. Cornelius Maas hat in Leipzig an der HHL zum Thema Innovation-Management unter Andreas Pinkwart promoviert und ist Dozent an der ESB Reutlingen.

Auszug aus: D. Matusiewicz (Hrsg.) Plattformen und Tech-Giganten
ISBN: 978-3-95466-760-4.

13 IT-Sicherheit & Datenschutz: Einer für Alle, Alle für Einen

Torsten Redlich und Tobias Urban

13.1 Einführung

IT-Sicherheit und Datenschutz einer Gesamtlösung sind nur so gut wie ihre Umsetzung in den verschiedenen Einzelteilen einer Plattform. Die relevanten Teile sind in der Anwendung, System- und Infrastrukturebene einer Plattform-Lösung gleichermaßen zu finden. Die größten Schwachstellen sind ungewollte Einfallstore für verschiedenste Angreifer und ermöglichen Datendiebstahl, Sabotage des Dienstes oder Manipulation der Daten selbst.

In der Patientenversorgung wird die weitreichende Nutzung von Daten, die auf unterschiedlichste Art und Weise erhoben werden (z.B. bei den Leistungserbringern, im häuslichen Umfeld, in der Forschung), für medizinische Zwecke einen Innovationssprung mit sich bringen – wie bereits zuvor in anderen Industriezweigen. Um dies zu gewährleisten, entstehen Plattformen, die über mehrere Nutzergruppen und rechtlichen Einheiten hinweg die Erhebung, Verarbeitung und Verwertung der medizinischen Daten ermöglichen. Die nötigen technologischen und sicherheitspolitischen Leitkonzepte für den Aufbau von datenbasierten Ökonomiesystemen finden sich in Initiativen wie dem European Health Data Space (EHDS) oder dem Industrial Data Space respektive der davon abgeleitete Medical Data Space wieder. Der EHDS beispielsweise stützt sich dabei auf drei Grundsätze: Starkes Datenverwaltungssystem und Regeln für den Datenaustausch, Datenqualität und starke Infrastruktur und Interoperabilität (Europäische Union 2022). Nicht zu vergessen ist außerdem die Initiative Gaia-X, die maßgeblich zur Schaffung einer Referenzarchitektur und europäischer Datensouveränität beitragen soll(te).

Auszug aus: D. Matusiewicz (Hrsg.) Plattformen und Tech-Giganten
ISBN: 978-3-95466-760-4.

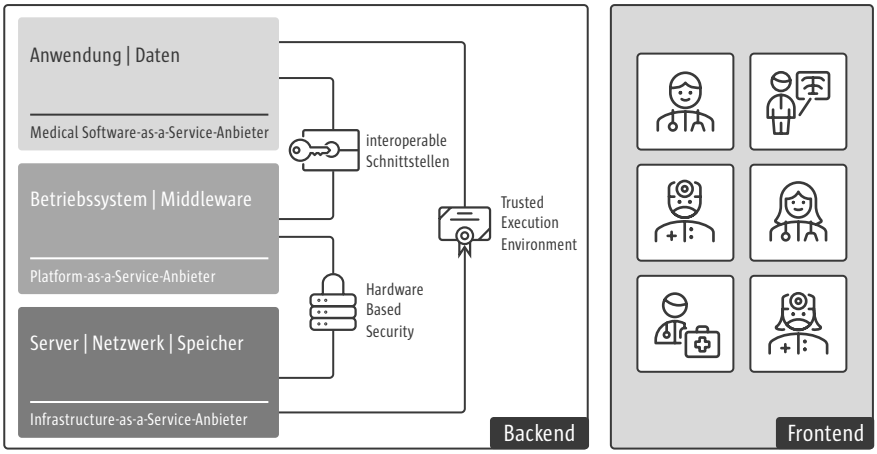

Abb. 1 Systematische Darstellung des Aufbaus einer Plattform mit den relevanten Ebenen aus Sicht der IT-Sicherheit

Plattform-Lösungen existieren bereits und werden in rasantem Tempo an Bedeutung gewinnen. Damit IT-Sicherheit oder Datenschutz nicht erst im Nachhinein Einzug hält – ein nicht seltenes Phänomen – werden im Folgenden typische Sichtweisen und Verpflichtungen der Akteure der verschiedenen Ebenen erörtert: Medical Software, Plattform und Infrastruktur (s. Abb. 1).

13.2 Medical Software – am Stand der Technik entlang

Aus Sicht der Endanwender muss eine Anwendung einfach und intuitiv bedienbar sein und einen klaren Nutzen bieten. Aus Sicht des Regulierers unterliegen medizinisch relevante Daten einem hohen Schutzniveau. Dabei gilt es die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu beachten. Welche Maßnahmen müssen nun auf Ebene der Anwendung getroffen werden, um das geforderte Schutzniveau und eine angemessene Abwehrstärke zu erreichen? Die Basis sind hier Sicherheitsthemen, wie die sichere Verwendung digitaler Identitäten, Kontrollierbarkeit der Datenspeicherung und -zugriffe, abgesicherter Datentransport und insbesondere die Sicherheit der Software selbst – Software-Architektur, Quellcode, u.a. Diese müssen nach dem sogenannten Stand der Technik ausgeprägt sein, beschrieben beispielsweise durch das Bundesamt für Sicherheit in der Informationstechnik mit Sicherheitsstandards wie der Technischen Richtlinie TR-03161 (BSI 2022) oder dem IT-Grundschutz. Abhängig vom medizinischen Verwendungszweck kann die Anwendung auch unter die Definition Software as a Medical Device (SaMD) und damit der Medizinproduktzulassung fallen. EU-Vorgaben aus der Medical Device Regulation (MDR) oder In Vitro Diagnostic Regulation (IVDR) bedingen zusätzliche Sicherheitsanforderungen. Wichtig ist an dieser Stelle zu unterscheiden, welche Sicherheitstechniken in der Anwendung selbst anzusetzen sind, und welche bereits durch die darunterliegende Ebene „Systemplattform“ geleistet und was zulässigerweise gefordert wird.

Auszug aus: D. Matusiewicz (Hrsg.) Plattformen und Tech-Giganten
ISBN: 978-3-95466-760-4.

13.3 Systemplattform – sicherheitstechnische Paradigmen etablieren

Grundsätzlich sind zwei Kernbereiche aus Sicht des Datenschutzes und der informationellen Selbstbestimmung besonders wichtig: Einwilligung in die Datennutzung und Transparenz in der Datennutzung. Einwilligungsmanagement ist komplex und nicht durch die Ebene „Anwendung" allein in den Griff zu bekommen.

Gemäß Art. 9 Abs. 2b, e der DSGVO ist die Verarbeitung von medizinischen Daten im Kontext der Primärversorgung (z.B. der Diagnose oder Behandlung von Krankheiten) ohne explizite Einwilligung möglich. Allerdings ist bereits heute der Bedarf hoch, erfasste Daten auch für weitere Zwecke zu nutzen (z.B. für die Forschung). Somit ist ein Werkzeug zur Umsetzung eines „Einwilligungsmanagements", das eine selbstbestimmte fallbezogene Nutzung der eigenen medizinisch relevanten Daten durch Dritte ermöglicht, unabdingbar. Dabei ist ein einmaliges Erteilen einer Einwilligung für alle möglichen Anwendungsfälle, zum Beispiel bei der Aufnahme in ein Krankenhaus, keine hinreichende Lösung. Aus Sicht des Datenschutzes und der informationellen Selbstbestimmung muss hier vielmehr eine Lösung zur Verfügung stehen, die eine feingranulare Steuerung der Datenverwertung in den unterschiedlichen Anwendungen möglich macht.

> Dies ist nur mit sicherheitstechnischen Paradigmen und Plattform-Services rund um das Daten-Management möglich. Blickt man auf die Gaia-X Initiative, bietet die Ebene der Systemplattform beispielsweise Federation Services, Data Integration, Data Exchange, Policy Enforcement und interoperable Schnittstellen an (eco 2022). Mit dem Ziel einheitliche und zuverlässige Sicherheitsverfahren der Ebene „Anwendung" bereitzustellen.

Eine Systemplattform in sich muss ebenso sicher aufgestellt sein und betrieben werden können. Sichere Betriebssysteme und Service-Architekturen sind auch hier durch Security-Best-Practices und Stand der Technik formuliert. Häufig auch mit dem Fokus auf Open Source Standards, was eine Überprüfung der Systemsoftware, Datenbanken, Frameworks und interoperablen Schnittstellen verspricht. Die Systemplattform selbst fordert und fördert umfassende IT-Sicherheit und bietet der Ebene „Anwendung" sichere, zuverlässige und akzeptierte Sicherheitsverfahren an.

13.4 Infrastruktur als vertrauenswürdiges Rückgrat

Die Infrastruktur bildet das Rückgrat einer jeden Plattform, den darauf etablierten Anwendungen und der sich entfaltenden datenbasierenden Ökonomie. Die Sichererstellung von Datensouveränität und das Etablieren sicherer Infrastrukturen sind damit von nationalem Interesse und sicherheitspolitischen Strategien geprägt.

Sicherheitspolitische Interessen, wie der zwingende Einsatz von zertifizierten und zugelassenen Techniken (Virtualisierungssoftware, Netzwerktechnik, Sicherheitssysteme, Speichertechnik), liegen hier auf der Hand und wurden in Teilen bereits im IT-Sicherheitsgesetz 2.0 verankert (BSI 2021). Die Überprüfbarkeit und Unabhängigkeit der Techniken selbst wird nicht selten über Open-Source/Open-Standards-For-

derungen verfolgt. Weitere Hilfestellung in der Ausgestaltung sicherer Infrastrukturen finden sich in der TR-03161 vom BSI (BSI 2022).

Eine bereits heute bedeutende Sicherheitseigenschaft der Infrastruktur ist die Abbildung rechtlicher Grundlagen zur Speicherung und Verarbeitung sensibler Daten. Hier ist insbesondere die Einhaltung der Datenschutz-Grundverordnung und die Sicherstellung des Verbleibes der Daten in Europa wichtig. Allerdings ist der reine Ort der Speicherung und Verarbeitung der Daten noch kein hinreichender Schutz für die hochsensiblen medizinischen Daten, die auf Plattformen immer mehr durch Dritte genutzt werden. Es muss sichergestellt werden, dass die Daten zu keinem Zeitpunkt von dem Betreiber der Infrastruktur eingesehen werden können. Dies impliziert die Verarbeitung der Daten in sogenannten vertrauenswürdigen Ausführungsumgebungen (Confidential Computing). Die Umsetzung ist beispielsweise von der gematik für ausgewählte Fachdienste der Telematikinfrastruktur gefordert. Confidential Computing wird ein zentrales Sicherheitsversprechen der Infrastruktur für die Ebenen Systemplattform und Anwendung sein können.

13.5 Fazit

IT-Sicherheit, Privatheit und Datenschutz müssen bei der Verarbeitung hochsensibler medizinischer Daten eine zentrale Rolle bei dem Design, der Umsetzung sowie im Betrieb der Anwendungen spielen. IT-Sicherheitsstrategien beschränken sich dabei nicht nur auf eine Ebene, sondern müssen als großes Ganzes und insbesondere im geforderten Zusammenspiel verschiedener technischer Komponenten gesehen werden. Bedeutend hierbei werden die Koordination der relevanten Sicherheitsforderungen (Regulierung), das Etablieren von Standards (zugelassene Techniken) und die praxistaugliche Verwertung (Anwendungsfälle) über alle Ebenen und verschiedene Zuständigkeiten sein.

Literatur

Bundesamt für Sicherheit in der Informationstechnik (2022) Technische Richtlinie TR-03161: Anforderungen an Anwendungen im Gesundheitswesen. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03161/tr-03161.html (abgerufen am 23.09.2022)

Bundesamt für Sicherheit in der Informationstechnik (2021) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (abgerufen am 23.09.2022)

Europäische Union (2022) European Health Data Space. URL: https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en (abgerufen am 23.09.2022)

eco – Verband der Internetwirtschaft e.V (2022) Gaia-X Föderationsdienste – Orchestrierungskonzept. URL: https://www.gxfs.eu/de/gxfs-ueberblick/ (abgerufen am 23.09.2022)

Torsten Redlich

Torsten Redlich ist stellvertretender Leiter der Division eHealth bei der secunet Security Networks AG. Er widmet sich seit mehr als 15 Jahren den Herausforderungen in der Absicherung sicherheitskritischer IuK-Infrastrukturen von Bundesbehörden und kritischen Infrastrukturen wie Teile des Gesundheitswesens. Sein Schwerpunkt liegt derzeit insbesondere auf der Wechselwirkung sicherheitspolitischer Strategien hoheitlicher Aufgabenträger und Verfügbarkeit von entsprechenden Sicherheitsprodukten im Gesundheitswesen.

Dr.-Ing. Tobias Urban

Tobias Urban arbeitet bei der secunet Security Networks AG in der Division eHealth. Dort befasst er sich mit regulatorischen Aspekten der IT-Sicherheit für Medizinprodukte und Forschungs- und Entwicklungsthemen zur vertrauenswürdigen Umsetzung moderner digitaler medizinsicher Lösungen. Vor seiner Tätigkeit bei der secunet hat Tobias Urban zu technischen Umsetzungsmöglichkeiten von Anforderungen der DSGVO an der Ruhr-Universität Bochum promoviert.

14 Patientenplattformen für die klinische Forschung

Julia Hitzbleck

14.1 Gesundheitsinformationen und Patientenplattformen in Zeiten der Digitalisierung

Wie bei fast allen anderen Themen in unserem Leben ist heute oft Dr. Google die erste Anlaufstelle für Informationen zu Gesundheit, körperlichen Beschwerden oder Medikamenten. Zusätzlich bietet eine wachsende Zahl an Patientenplattformen über webbasierte Portale oder Apps Patienten die Möglichkeit, ihre Gesundheit und Versorgung aktiv zu managen. Dabei werden unterschiedliche Funktionen angeboten, von der Terminbuchung, der Kommunikation mit dem Behandlungsteam bis hin zur Dokumentation von Gesundheitsdaten, einschließlich Symptomen, Medikamenten und Laborergebnissen. Andere Plattformen verbinden als soziale Netzwerke Patienten und Angehörige in Online-Communities, um Informationen und Ressourcen auszutauschen, Unterstützung zu finden und teilen neue Erkenntnisse. Die direkte Peer-to-Peer-Kommunikation in Foren oder geschlossenen Online-Communities hilft den Mitgliedern, von den Erfahrungen mit Medikamenten, Nebenwirkungen oder allgemeinen gesundheitlichen Herausforderungen zu lernen, die ihre Lebensweise beeinträchtigen und in der Diskussion mit ihren Ärzten oft zu kurz kommen. Auch wenn der Austausch in solchen Gruppen nicht als medizinischer Ratschlag verstanden werden darf, hilft es den meisten Patienten oder ihren Angehörigen, sich mit der Krankheit und damit verbundenen Herausforderungen weniger allein zu fühlen.

Auszug aus: D. Matusiewicz (Hrsg.) Plattformen und Tech-Giganten
ISBN: 978-3-95466-760-4.