medizin://dokumentation/informatik/
informationsmanagement/

mdi

ISSN 1438-0900

Heft 4 _ Dezember 2020 _ Jahrgang 22

CYBERCRIME UND DATENSCHUTZ IM GESUNDHEITSWESEN

BVMI DVMD

Editorial 95

Vorschau 95

Schwerpunkt

Datenschutzanforderungen an digitale Gesundheitsanwendungen _Hessel _Leffer _Potel 96

IT-Sicherheit am Universitätsklinikum Erlangen: Anforderungen, Umsetzung und Empfehlungen _Schneider _Feldberger 99

Der Elektronische Arztausweis – Umsetzung gesetzlicher Vorgaben _ Münzing 103

Datenschutz in einem Behandlungsverbund aus Sicht von multimorbiden Patienten mit Demenz _Steiner _Möller 106

Gib Cybercrime keine Chance! _Bosk 111

Kritische Schwachstellen in medizinischen Geräten _ Suleder _Grunow 115

Neuerung der Datenschutzgrundverordnung für die medizinische Forschung _Kaulke _Schlünder _Semler _Drepper 119

BVMI & DVMD

Köpfe im BVMI: Günther Steyer 125

Köpfe im DVMD: Andrea Großer 125

DVMD Nachrichten 126

Impressum 126

ONKOSTAR

Ihr neues modernes
Tumordokumentationssystem

- alle Entitäten
- alle Zertifizierungen
- Tumorkonferenzen

IT-CHOICE Software AG

dkfz. DEUTSCHES KREBSFORSCHUNGSZENTRUM IN DER HELMHOLTZ-GEMEINSCHAFT

Liebe Leserinnen und Leser,

Prof. Dr. Paul Schmücker
Hochschule Mannheim
Institut für Medizinische Informatik
p.schmuecker@hs-mannheim.de

Die Digitalisierung wird in allen Bereichen des Gesundheitswesens ständig ausgebaut. Die Vielfalt und Komplexität der Gesundheitsversorgung, aber auch die immer schnelleren methodischen, organisatorischen und technischen Entwicklungen sind nicht mehr ohne eine umfassende Informationsverarbeitung denkbar. Dies betrifft nicht nur die klassische Informationsverarbeitung im Krankenhaus, sondern auch sektorenübergreifende Versorgungsnetze, telemedizinische Anwendungen, die Einführung der Gesundheitstelematikinfrastruktur (GTI) sowie verstärkt auch die IT-Unterstützung der Forschung. Erschwerend bei der digitalen Transformation ist immer noch die unvollkommene Interoperabilität der heterogenen IT-Umgebungen mit zahlreichen Medienbrüchen und Kommunikationspartnern.

Das Gesundheitswesen gilt als einer der gefährdetsten Bereiche in Sachen IT-Sicherheit. Mit der fortschreitenden Digitalisierung nehmen die Cyberangriffe und Datenschutzverletzungen und damit auch die Anforderungen an den Datenschutz und die IT-Sicherheit zu. Spätestens mit der Verabschiedung des Digitale-Versorgung-Gesetzes (DVG) und des Patientendaten-Schutzgesetzes (PDSG) müssen sich die Einrichtungen des Gesundheitswesens mit den komplexen Themen Datenschutz und IT-Sicherheit auseinandersetzen. Gemäß IT-Sicherheitsgesetz (IT-SiG) und KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) stehen neue Vorgaben und Audits an. Ergänzend zu den bisherigen Sicherheitsanforderungen verlangt außerdem das Krankenhauszukunftsgesetz (KHZG) von den Kliniken den Auf- und Ausbau von umfangreichen Schutzmaßnahmen für die IT-Sicherheit.

Grundlegend kann festgestellt werden, dass eine 100-prozentige IT-Sicherheit nie realisiert werden kann. Mit der Einführung und dem Betrieb eines Informations-Sicherheits-Management-Systems (ISMS) kann jedoch die IT-Sicherheit unter Anwendung des Branchenspezifischen Sicherheitsstandards (B3S) sehr sicher gestaltet werden. In der Regel müssen zudem neue Organisationsstrukturen (z.B. IT-Sicherheitsbeauftrage) sowie angepasste Behandlungsabläufe geschaffen werden, was allerdings nicht ohne Ressourcen (Personal, Finanzmittel) umsetzbar ist. Dabei sollten aber Überregulierungen des Betriebs der Gesundheitseinrichtungen vermieden werden. Wichtig ist auch, dass in den Gesundheitseinrichtungen das Bewusstsein geschaffen wird, dass IT-Sicherheit kein Störfaktor im laufenden Betrieb ist und keine Mitarbeiter an den Pranger gestellt werden.

In diesem Heft werden aus Sicht des Datenschutzes und der IT-Sicherheit die neuen Gesetze und Verordnungen sowie Anforderungen, Schwachstellen und Lösungsansätze am Beispiel des Universitätsklinikums Erlangen behandelt. Die weiteren Beiträge beschäftigen sich mit den Möglichkeiten des Elektronischen Arztausweises in der GTI, dem Datenschutz in einem über Sektorengrenzen hinweg realisierten Behandlungsverbund von multimorbiden Demenzpatienten, der Sicherstellung der Integrität, Authentizität und Vertraulichkeit von Daten und Dokumenten durch Verschlüsselung sowie elektronische Signaturen und Zeitstempel, ferner mit kritischen Schwachstellen in der Medizintechnik und der Umsetzung der Anforderungen des Datenschutzes und der Informationssicherheit in der medizinischen Forschung.

Alle Beiträge unterstreichen, dass die zunehmende Digitalisierung im Gesundheitswesen bei gleichzeitig zunehmender Komplexität und Spezialisierung der Gesundheitsversorgung zu großen Herausforderungen für das Informationsmanagement der Gegenwart und Zukunft führt und weiterhin ein breites Forschungsfeld des Datenschutzes und der IT-Sicherheit bleibt.

Herzlicher Dank gebührt den Autoren dieses Heftes, aber auch den Sponsoren DMI GmbH & Co. KG, ID Information und Dokumentation im Gesundheitswesen GmbH & Co. KGaA, IT-CHOICE Software AG und promedtheus AG.

Viel Freude und neue Erkenntnisse beim Lesen wünscht Ihnen

Ihr Paul Schmücker.

Die nächsten Themenhefte

mdi 1_2021
Qualitätssicherung und Medizinmanagement
Verantwortliche Redakteure: Stein, Händel

mdi 2_2021
Ethik und Ökonomie im medizinischen Informationsmanagement
Verantwortliche Redakteure: Goldschmidt, Händel

mdi 3_2021
Informationsmanagement in der Pflege
Verantwortliche Redakteure: Bott, Sellmann

mdi 4_2021
Digitales Versorgungsgesetz – was hat es gebracht?
Verantwortliche Redakteure: Schmücker, Stein

Vorschau

Sie haben zu den genannten Themenheften eine Artikel-Idee? Bitte melden Sie sich bei Markus Stein mstein@rzv.de

Datenschutzanforderungen an digitale Gesundheitsanwendungen

Stefan Hessel ist Rechtsanwalt und Associate im Team Datenschutz & Cybersecurity bei reuschlaw Legal Consultants in Saarbrücken.
stefan.hessel@reuschlaw.de

Lena Leffer ist Diplomjuristin und wissenschaftliche Mitarbeiterin am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes und derzeit Stationsreferendarin bei reuschlaw Legal Consultants in Saarbrücken.
lena.leffer@reuschlaw.de

- Cyberangriffe und Datenschutzverletzungen im Gesundheitswesen nehmen wegen der voranschreitenden Digitalisierung zu.
- Der Gesetzgeber hat zahlreiche gesetzliche Regelungen zur Digitalisierung des Gesundheitswesens erlassen.
- Die neuen Gesetze und Verordnungen beinhalten strenge Vorgaben zu Datenschutz und IT-Sicherheit.
- Einzelne Regelungen sind Gegenstand einer kontroversen Debatte über die Angemessenheit des Schutzniveaus.
- Die Akteure im Gesundheitswesen müssen die neuen Vorschriften genau prüfen und umsetzen.

Ob Cyberangriffe auf Krankenhäuser [1], schwerwiegende und damit letztlich lebensbedrohende Sicherheitslücken in Medizingeräten [2] oder unzureichend geschützte Medizindaten im Internet [3] – immer wieder führt der Einsatz digitaler Technologien im Gesundheitswesen zu unerwünschten Nebeneffekten. Gleichzeitig eröffnet die Digitalisierung der Medizin jedoch neue Chancen für ein besseres Verständnis von Krankheiten und eine neuartige Patientenbetreuung. [4] Nicht zuletzt aus diesem Grund wird die Digitalisierung der Medizin vom Gesetzgeber zunehmend gefördert, aber auch gefordert. Um dabei den eingangs aufgezeigten Datenschutzrisiken zu begegnen, hat der Gesetzgeber zugleich eine Vielzahl an strengen Vorgaben zur IT-Sicherheit und zum Umgang mit Patientendaten erlassen. Der folgende Beitrag liefert einen Überblick zu den hierzu ergangenen Vorschriften, zeigt Problemfelder auf und erlaubt einen Einstieg in das aktuell viel diskutierte Feld der Regulierung von IT-Sicherheit und Datenschutz im Gesundheitswesen. Auf spezifische Anforderungen für kritische Infrastrukturen nach dem BSI-Gesetz soll an dieser Stelle nicht näher eingegangen werden (Siehe dazu den folgenden Beitrag von Schneider/Feldberger S. 99).

Medizinische Daten und die DSGVO

Mit der seit dem 25. Mai 2018 anwendbaren Datenschutzgrundverordnung (DSGVO) hat die Europäische Union für alle Mitgliedstaaten einen verbindlichen Rahmen zum Umgang mit personenbezogenen Daten geschaffen. Personenbezogene Daten sind Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Innerhalb der personenbezogenen Daten nehmen Gesundheitsdaten ebenso wie genetische oder biometrische Daten eine besondere Rolle ein. Sie gehören nach Art. 9 Abs. 1 DSGVO zu den besonderen Kategorien personenbezogener Daten und unterliegen damit einem strengen gesetzlichen Schutz. Die Verarbeitung von Gesundheitsdaten ist daher grundsätzlich untersagt. Ausnahmen kommen nur unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO in Betracht. [5] Danach ist eine Verarbeitung beispielsweise möglich, wenn eine ausdrückliche Einwilligung des Patienten vorliegt, lebenswichtige Interessen bedroht sind oder Gesundheitszwecke im Sinne von Art. 9 Abs. 2 lit. h DSGVO betroffen sind. Von den Gesundheitszwecken nach Art. 9 Abs. 2 lit. h DSGVO sind unter anderem die Gesundheitsvorsorge, arbeitsmedizinische Untersuchungen, die medizinische Diagnostik sowie die Versorgung, Behandlung oder Verwaltung im Gesundheits- oder Sozialbereich umfasst. Insbesondere eine Nutzung von Artikel-9-Daten für wirtschaftliche Zwecke – wie beispielsweise Werbung – ist regelmäßig nur mit ausdrücklicher Einwilligung des Patienten (Betroffener) zulässig. Wegen der hohen Sensibilität der Daten und dem damit einhergehenden Risiko für die Rechte und Freiheiten der Betroffenen unterliegen Artikel-9-Daten nach Art. 32 Abs. 1 DSGVO auch einem besonders hohen technisch-organisatorischen Schutzniveau. Wer entsprechende Daten verarbeitet, muss daher auch angemessene Maßnahmen zu deren Schutz treffen. Darüber hinaus erlaubt Art. 9 Abs. 4 DSGVO den Mitgliedstaaten, für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten sogar zusätzliche Bedingungen einzuführen oder aufrechtzuerhalten. Neben einheitlichen Regeln zum Umgang mit personenbezogenen Daten hat die DSGVO auch einen einheitlichen Rahmen für Sanktionen bei Verstößen gegen das Datenschutzrecht geschaffen. Wer gegen die DSGVO verstößt, muss nicht nur mit behördlichen Bußgeldern, sondern auch mit Schadensersatzforderungen Betroffener rechnen. Ein Bußgeld der Datenschutzaufsicht Baden-Württemberg gegen die dortige AOK zeigt, dass davon auch das Gesundheitswesen betroffen sein kann. [6] Die AOK musste in Zusammenhang mit einem Gewinnspiel wegen eines Verstoßes gegen die Pflichten zu sicherer Datenverarbeitung ein Bußgeld in Höhe von 1,24 Millionen Euro zahlen.

Wann liegen Gesundheitsdaten nach der DSGVO vor?

Sobald Gesundheitsdaten vorliegen, werden hohe rechtliche Anforderungen an deren Verarbeitung gestellt. Damit sind große praktische Auswirkungen verbunden – etwa die Kosten für technische Schutzmaßnahmen oder die Schaffung eines Systems zum Handling von Einwilligungen. Deshalb wird in der juristischen Praxis immer wieder diskutiert, ab wann Gesundheitsdaten vorliegen. Nach dem Wortlaut von Art. 4 Nr. 15 DSGVO

sind Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Grundsätzlich geht die DSGVO insoweit von einer weiten Definition aus [7], sodass personenbezogene Daten vergleichsweise einfach zu Gesundheitsdaten werden können. Denn der bloße Umstand, dass eine Person einen Arzt aufsucht, kann bereits Rückschlüsse auf deren Gesundheitszustand ermöglichen. Die Einbeziehung solcher Rückschlüsse würde – da Rückschlüsse auf die Gesundheit aus einer Unmenge von Faktoren möglich sind – jedoch dazu führen, dass letztlich fast jedes personenbezogene Datum als Gesundheitsdatum anzusehen wäre. [8] Diese Auffassung würde zu weitreichenden Verarbeitungsverboten führen. Das Verarbeitungsverbot bestünde dann auch unabhängig davon, ob ein Rückschluss tatsächlich gezogen wird bzw. eine Absicht hierzu besteht oder nicht. Eine solche Vorgehensweise ist daher abzulehnen.[9]

Digitale-Versorgung-Gesetz (DVG)

Das »Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation« (Digitale-Versorgung-Gesetz – DVG) ist am 19.12.2019 in Kraft getreten. Es handelt sich um ein Artikelgesetz, das umfangreiche Änderungen am Sozialgesetzbuch (SGB) Fünftes Buch (V) sowie an weiteren Gesetzen vornimmt. Wesentliche Neuerung ist der Auftrag an die Krankenkassen, mehr digitale Gesundheitskompetenz bei den Versicherten und digitale Innovationen im Gesundheitswesen insgesamt (vgl. §§ 20k, 68a SGB V) zu fördern. Hierdurch soll die Digitalisierung von allen Seiten maßgeblich vorangetrieben werden.

In engem Zusammenhang damit steht die Regelung des § 33a SGB V, der erstmals Bestimmungen zu sog. Gesundheitsapps und ähnlichen Anwendungen enthält. Im Gesetz werden diese in § 33a Abs. 1 S. 1 SGB V unter dem Begriff der »Digitalen Gesundheitsanwendungen« (DiGA) zusammengefasst. DiGA sind demnach Medizinprodukte niedriger Risikoklasse, deren Hauptfunktion wesentlich auf digitalen Technologien beruht und die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Kompensierung von Verletzungen oder Behinderungen zu unterstützen. Neben der erstmaligen Definition von DiGA hat der Gesetzgeber zugleich einen Anspruch der Versicherten auf Kostenübernahme sowie ein System zur Zulassung von DiGA erlassen. Eine wesentliche Bedeutung für das Zulassungssystem hat das Verzeichnis für digitale Anwendungen, das gemäß § 139e SGB V vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) geführt wird und in das Hersteller auf Antrag nach der Erfüllung strenger Regularien – insbesondere auch hinsichtlich des Datenschutzes und der IT-Sicherheit – aufgenommen werden können. Für die IT-Sicherheit von besonderer Bedeutung ist auch die Regelung des § 75b SGB V, wonach die Kassenärztliche Bundesvereinigung (KBV) bis zum 30.06.2020 verbindliche Maßstäbe für die IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung verabschieden sollte. Das aktuell ins Stocken geratene Verfahren sieht vor, dass die KBV in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesbeauftragten für den Datenschutz (BfDI) sowie den berufsständischen Kammern und der Deutschen Krankenhausgesellschaft (DKG) eine dem Stand der Technik entsprechende und jährlich zu aktualisierende Richtlinie zur IT-Sicherheit erlässt.

Letztlich regelt das DVG darüber hinaus auch elektronische Verordnungen (§ 86 SGB V), die Schaffung eines Forschungsdatenzentrums für Versichertenstammdaten (§ 303d SGB V) sowie den Ausbau der Telematikinfrastruktur und die Erleichterung der Videosprechstunde. Für Letztere gelten mit § 291g SGB V und der zugehörigen Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) bereits seit einigen Jahren hohe Datenschutz- und IT-Sicherheitsanforderungen.

DiGAV – Anforderungen an Gesundheitsapps & Co

Wie hoch die regulatorischen Anforderungen an Datenschutz und IT-Sicherheit im Gesundheitswesen sind, lässt sich gut am Beispiel der DiGA aufzeigen. Hierfür hat das Bundesministerium für Gesundheit (BMG) gemäß § 139e Abs. 9 SGB V Anfang April 2020 die »Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung« (Digitale Gesundheitsanwendungen-Verordnung [DIGAV]) erlassen. Diese beinhaltet einerseits Vorgaben für die Funktionssicherheit und -tauglichkeit, Qualität und Wirksamkeit (positive Versor-

Abkürzungen

BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragter für den Datenschutz
BMG	Bundesministerium für Gesundheit
DiGA	Digitale Gesundheitsanwendungen
DiGAV	Digitale Gesundheitsanwendungen Verordnung
DKG	Deutsche Krankenhausgesellschaft
DSGVO	Datenschutzgrundverordnung
DVG	Digitale-Versorgung-Gesetz
DSK	Datenschutzkonferenz
EWR	Europäischer Wirtschaftsraum
KBV	Kassenärztliche Bundesvereinigung
PDSG	Patientendaten-Schutz-Gesetz
SGB	Sozialgesetzbuch

Karin Potel ist Diplomjuristin und wissenschaftliche Mitarbeiterin am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes und derzeit Stationsreferendarin bei reuschlaw Legal Consultants in Saarbrücken.
karin.potel@reuschlaw.de

gungseffekte) der DiGA sowie andererseits umfangreiche Anforderungen an den Datenschutz und die Datensicherheit nach dem Stand der Technik. Hersteller bzw. Anbieter von DiGA müssen diese Vorgaben zwingend erfüllen, um in das bereits erwähnte Verzeichnis des BfArM aufgenommen zu werden und damit am Verfahren zur Kostenerstattung teilnehmen zu können. Unter den umfangreichen Vorgaben der DiGAV sind aus rechtlicher Perspektive insbesondere die folgenden Regelungen zum Datenschutz von Interesse. In § 4 Abs. 2 DiGAV schränkt das BMG die ohnehin schon strenge Zulässigkeit der Verarbeitung von Gesundheitsdaten weiter ein. So darf eine Verarbeitung personenbezogener Daten – unabhängig davon, ob es sich um Gesundheitsdaten handelt – grundsätzlich nur mit einer Einwilligung i.S.v. Art. 7 DSGVO erfolgen. Darüber hinaus dürfen personenbezogene Daten bei einer DiGA auch nur zu eng begrenzten Zwecken verarbeitet werden. Hierzu gehören nach § 4 Abs. 2 S. 1 Nr. 1 bis Nr. 3 DiGAV der bestimmungsgemäße Gebrauch der DiGA, der Nachweis positiver Versorgungseffekte und die Kostenerstattung. Nach § 4 Abs. 2 S. 1 Nr. 4 DiGAV ist darüber hinaus – sofern eine gesonderte Einwilligung des Nutzers vorliegt – auch die Verarbeitung personenbezogener Daten zur dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der DiGA zulässig. Ein ausdrückliches Verbot der Datenverarbeitung zu Werbezwecken findet sich in § 4 Abs. 4 S. 1 DiGAV. Weitere datenschutzrechtliche Vorgaben, deren europarechtliche Zulässigkeit durchaus fraglich ist [10], macht die DiGAV bei Datentransfers in Drittstaaten. Hierbei handelt es sich um Staaten außerhalb des Europäischen Wirtschaftsraums (EWR). In diese Länder dürfen Daten nur übermittelt werden, wenn ein Beschluss der EU-Kommission für ein angemessenes Datenschutzniveau vorliegt. Wegen des jüngsten EuGH-Urteils zum EU-US Privacy Shield (»Schrems II«-Entscheidung) [11] sind aktuell Datenübermittlungen in die USA unzulässig. Dies stellt die Anbieter von DiGA vor enorme Herausforderungen, da viele der im Zusammenhang mit Smartphones genutzten Anwendungen und Infrastrukturen US-basiert sind. Beispiele hierfür sind nicht nur der jeweilige Appstore von Google und Apple, sondern auch zahlreiche Clouddienste.

Patientendaten-Schutz-Gesetz (PDSG)

Mit dem Patientendaten-Schutz-Gesetz will der Gesetzgeber die Digitalisierung des Gesundheitswesens weiter beschleunigen und die elektronische Patientenakte, den elektronischen Medikationsplan sowie das eRezept möglichst schnell in die Patientenversorgung einbringen. Kritiker bemängeln jedoch, dass das Gesetz im Gegensatz zu den Ankündigungen von Bundesgesundheitsminister Spahn den Patientendatenschutz, etwa bei den Zugriffsmöglichkeiten der Betroffenen auf ihre Daten, nicht hinreichend berücksichtigt. Der BfDI hält das Gesetz sogar für europarechtswidrig und droht bei seiner Umsetzung mit rechtlichen Schritten gegen jene Krankenkassen, die das Gesetz nach seiner Verabschiedung befolgen. [12] Gleichwohl wurde das Gesetz zwischenzeitlich im Bundestag beschlossen und auch im Bundesrat durch die Nicht-Anrufung des Vermittlungsausschusses gebilligt.[13] Das Gesetz ist nach seiner Verkündung im Bundesgesetzblatt am 20.10.2020 in Kraft getreten. Ein Ende der Diskussion um das PDSG ist damit jedoch längst nicht absehbar.

Fazit

Die Digitalisierung des Gesundheitswesens schreitet mit zunehmender Geschwindigkeit voran. Hierdurch ergeben sich neue Bedrohungen für die IT-Sicherheit und den Datenschutz, wie z.B. Angriffe mit Verschlüsselungstrojanern auf die IT-Infrastruktur von Krankenhäusern oder das Abhandenkommen von Patientenakten durch unzureichend geschützte Geräte. Der Gesetzgeber stellt wegen dieser Bedrohungen zunehmend hohe Anforderungen an IT-Sicherheit und Datenschutz im Gesundheitswesen. Unabhängig von der kontrovers diskutierten Frage, ob diese Maßnahmen im Einzelfall notwendig bzw. ausreichend sind, müssen die Vorgaben gleichwohl von den Verantwortlichen umgesetzt werden. Aus der Sicht von Herstellern und Betreibern ist daher eine genaue Kenntnis der gesetzlichen Vorgaben und eine fortlaufende Beobachtung dieser erforderlich. ■

Quellen

[1] Schadsoftware – DRK-Krankenhäuser von Cyberangriff betroffen, online abrufbar unter: https://www.kma-online.de/aktuelles/it-digital-health/detail/drk-krankenhaeuser-von-cyberangriff-betroffen-a-41375, zuletzt abgerufen am: 12.10.2020.
[2] Slabodkin, Insulin pumps among millions of devices facing risk from newly disclosed cyber vulnerability, IBM says, online abrufbar unter: https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/, zuletzt abgerufen am: 12.10.2020.
[3] Datenleak – Millionen Patientendaten waren offenbar ungeschützt im Netz abrufbar, online abrufbar unter: https://www.zeit.de/digital/datenschutz/2019-09/datenleak-patienteninformationen-ingolstadt-kempen-passwort-datenschutz, zuletzt abgerufen am: 12.10.2020.
[4] Ehlers/Bartholomä, Medizin 4.0 (Digital Health) – Chancen und Risiken, online abrufbar unter: https://doi.org/10.1007/978-3-658-25141-3_18, zuletzt abgerufen am: 12.10.2020.
[5] Siehe dazu auch: DSK, Kurzpapier Nr. 17 – Besondere Kategorien personenbezogener Daten, online abrufbar unter: https://www.lda.bayern.de/media/dsk_kpnr_17_besondere_kategorien.pdf, zuletzt abgerufen am: 12.10.2020.
[6] Pressemitteilung, LfDI Baden-Württemberg verhängt Bußgeld gegen AOK Baden-Württemberg – Wirksamer Datenschutz erfordert regelmäßige Kontrolle und Anpassung, online abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/, zuletzt abgerufen am: 12.10.2020.
[7] Weichert, in: Kühling/Buchner, DSGVO BDSG, 3. Auflage 2020, Art. 4 Nr. 15 DSGVO, Rn. 1.
[8] Schneider, Schließt Art. 9 DSGVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303, 305.
[9] Vergleiche mit weiteren Erläuterungen: Hessel/Leffer, WhatsApp im Unternehmen? Zum datenschutzkonformen Einsatz des Messengers, CR 2020, 139, 141.
[10] Piltz/Hessel, Verbot von Datentransfers in die USA? Der aktuelle DiGA-Leitfaden ist eine Herausforderung für Anbieter von Gesundheits-Apps & Co., online abrufbar unter: https://www.reuschlaw.de/news/verbot-von-datentransfers-in-die-usa/, zuletzt abgerufen am: 12.10.2020.
[11] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II.
[12] BfDI, BfDI zu Folgen der Gesetzgebung des PDSG, online abrufbar unter: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html, zuletzt abgerufen am: 12.10.2020.
[13] Cornell, PDSG – manche Punkte bleiben strittig, online abrufbar unter: https://www.aerztezeitung.de/Wirtschaft/PDSG-manche-Punkte-bleiben-strittig-413250.html, zuletzt abgerufen am: 12.10.2020.

IT-Sicherheit am Universitätsklinikum Erlangen: Anforderungen, Umsetzung und Empfehlungen

IT-gestützte Prozesse schützen oder doch nur Paperwork fürs Audit?

- Durch IT-Sicherheit können IT-gestützte Prozesse fortlaufend geschützt werden. Dennoch wird es nie 100% IT-Sicherheit geben!
- Risikobasiert: Die »Mauer der IT-Sicherheit« sollte gleichmäßig aufgebaut werden, anstatt einzelne Leuchttürme zu realisieren.
- Trotz zunehmendem Regulationsdrucks dürfen klinische Prozesse nicht überreguliert werden (IT-Sicherheit mit Augenmaß!).
- IT-Sicherheit ist ein interdisziplinäres Vorhaben mit Fokussierung auf die Benutzer und deren Prozesse.

Lorenz Feldberger (M.Sc. WI) ist Mitarbeiter am Medizinischen Zentrum für Informations- und Kommunikationstechnik (MIK) am Universitätsklinikum Erlangen. Lorenz.Feldberger@uk-erlangen.de

Martin Schneider (Dipl.-Wi.-Ing.; MBA) ist Geschäftsführer des Medizinischen Zentrums für Informations- und Kommunikationstechnik (MIK) am Universitätsklinikum Erlangen. Martin.Schneider@uk-erlangen.de

Regulatorische Anforderungen aus dem BSI-Gesetz

Das BSI-Gesetz (BSIG) von 2009 wurde 2015 um das »Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)« ergänzt. Neben neuen Aufgaben und Befugnissen für das BSI lag der Fokus auf den Kritischen Infrastrukturen (KRITIS) [1]. Das sind Einrichtungen, die eine kritische Dienstleistung (kDL) »zur Versorgung der Allgemeinheit« erbringen und »deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde« [2]. Im Sektor Gesundheit sind Krankenhäuser KRITIS-Betreiber, wenn deren jährliche vollstationäre Fallzahl den Schwellenwert von 30.000 erreicht. Die kDL der KRITIS-Krankenhäuser ist die »stationäre medizinische Versorgung«. In den §§ 8a, 8b BSIG werden Vorgaben zur »Sicherheit in der Informationstechnik Kritischer Infrastrukturen« sowie zu einem entsprechenden Meldewesen gemacht. Jedoch sind weder im BSIG noch in der KRITIS-Verordnung konkrete Hinweise zur Umsetzung zu finden. Im BSIG ist zu lesen, dass der KRITIS-Betreiber verpflichtet ist, »angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden« [3]. Unter dem »Stand der Technik« wird die Einführung und der Betrieb eines ISMS (Informations-Sicherheits-Management-System) verstanden. Hierbei handelt es sich nicht um ein IT-System, sondern um ein Management-System, mit dem Maßnahmen geplant, umgesetzt und weiterentwickelt werden. Als Grundlage für den ISMS-Betrieb können bspw. die ISO 27000 ff. sowie der »Branchenspezifische Sicherheitsstandard« (B3S) herangezogen werden. Dieser beinhaltet zahlreiche organisatorische und technische Maßnahmen. Jeder Sektor kann seinen eigenen B3S entwickeln, der dann vom BSI freigegeben werden muss.

In der zentralen IT-Abteilung des Universitätsklinikums Erlangen (UKER), dem Medizinischen Informations- und Kommunikationszentrum (MIK), fiel die Entscheidung, ein ISMS nach der Struktur des B3S aufzubauen. Im Sektor Gesundheit wurde der »B3S für die Gesundheitsversorgung im Krankenhaus« vom BSI freigegeben.

Vorbereitung des IT-Sicherheitsaudits und Umsetzung des B3S

Schon weit vor der Auditplanung im Jahr 2017 war IT-Sicherheit ein fester Bestandteil des IT-Managements am UKER. Im Jahr 2016 wurde die bestehende Firewall durch eine redundant ausgelegte Next-Generation-Firewall ersetzt. Auf organisatorischer Seite waren die Stabstellen des IT-Sicherheitsbeauftragten (ITSB) und Datenschutzbeauftragten (DSB) besetzt. Dies war ein großer Vorteil für die Auditvorbereitung, denn zur gleichen Zeit startete am UKER das Großprojekt »Neues Klinisches Arbeitsplatzsystem (KAS)«. Es wurde damit begonnen, die IT-Landschaft grundlegend zu überarbeiten und zu verschlanken. Für dieses Großprojekt waren viele Mitarbeiter bereits eingeplant, die sich nun zusätzlich auf das IT-Sicherheitsaudit 2019 vorbereiten mussten. Dennoch wurde der Standpunkt vertreten, dass ein externer Berater das UKER aufgrund seiner komplexen klinischen und technischen Strukturen nicht zügiger und zielgerichteter durch das Audit führen könne als die eigenen IT-Mitarbeiter.

In der Auditvorbereitung wurden zusätzlich neue Rollen und Verantwortlichkeiten wie z.B. die des ISMS-Verantwortlichen geschaffen. Alle Beteiligten waren sich einig, dass die Vorbereitung auf das IT-Sicherheitsaudit viel mehr als nur Paperwork sei. Es ging darum, die eigene Risikosituation, soweit es geht, objektiv zu erfassen und zu bewerten, um dann mit Augenmaß die »Mauer der IT-Sicherheit« gleichmäßig hochziehen zu können. Dabei war es

oftmals schwierig, die über 200 B3S-Maßnahmen so umzusetzen, wie sie im exakten Wortlaut gefordert wurden. Wenn aufgrund des klinischen Prozessablaufs bzw. wegen technischer und baulicher Gegebenheiten vor Ort eine geforderte B3S-Maßnahme nicht exakt im Wortlaut erfüllt werden konnte, wurde diese Ausnahme begründet und dokumentiert.

Bevor die eigentliche Maßnahmenplanung aufgestellt wurde, musste der Anwendungsbereich (Scope) festgelegt werden. Nicht jedes IT-System unterstützt Prozesse der kritischen Dienstleistung (kDL). Einige IT-Systeme haben nur eine betriebswirtschaftliche Funktion und fallen daher aus dem Scope. Unter das BSIG fällt die IT des UKER, die die Prozesse der kDL unterstützt oder eine direkte Auswirkung auf sie hat. Ausgehend von der »stationären medizinischen Versorgung« wurden deren Kernprozesse fokussiert [2]. Im Folgenden identifizierte ein Expertenteam die IT-Systeme, die die kDL-Kernprozesse unterstützen. Diese IT-Systeme wurden als kDL-Systeme deklariert. Sie sind in drei Kritikalitäts-Klassen gegliedert. Klasse 1 und 2 sind kritische kDL-Systeme. Bei ihnen hat schon ein kurzer bzw. mittlerer Ausfall u.U. massive Auswirkungen auf den klinischen Betrieb. Hingegen sind kDL-Systeme der Klasse 3 nicht kritisch, da bei ihnen die maximal-tolerierbare Ausfallzeit (MTA) größer als 48 Stunden ist. Die Einstufung der kDL-Systeme erfolgte durch den ISMS-Verantwortlichen sowie durch IT-Mitarbeiter und Benutzer. Mitunter war es herausfordernd, den Benutzer bzw. Verantwortlichen zu identifizieren, der aus Anwendersicht für das jeweilige IT-System verantwortlich zeichnet. Die darauffolgende Terminplanung ging teilweise nur schleppend voran. Die Projektaktivitäten mussten parallel zu den Routineaufgaben und anderen Projekten bewältigt werden. Es herrschte zunächst die Meinung vor, dass die IT dies doch alles für die Anwender regeln müsse. In der Diskussion wurde den Anwendern jedoch schnell deutlich, dass das MIK nicht Prozesseigner ist. Nur der Prozesseigner kann entscheiden, wie wichtig die Verfügbarkeit eines prozessunterstützenden IT-Systems ist. Zudem muss er festlegen, wie während einer IT-Krise OHNE IT-System weitergearbeitet werden kann. Für Notfallsituationen wurden IT-Notfalldokumente erstellt. Es gibt zwei Typen von IT-Notfalldokumenten: Technische Dokumente für das MIK (Wiederanlauf- u. Wiederherstellungspläne der kDL-Systeme sowie der IT-Infrastruktur) und zum anderen die IT-Notfallpläne für die Benutzer. Sie wurden zusammen mit den Benutzern erstellt und schildern den »Plan-B« ohne IT-Unterstützung. Für die Dokumentation, Verfügbarkeit (z.B. Aushang) und Aktualisierung der IT-Notfallpläne sind die Benutzer verantwortlich. Für sie wurden auch Meldewege definiert, um sie bei einer IT-Krise entsprechend alarmieren zu können. Damit nicht jeder Incident eine klinikumsweite Alarmierung nach sich zieht, wurde ein Entscheidungsgremium etabliert, das Emergency Decision Board (EDB). Dieses Gremium entscheidet, wann eine IT-Krise vorliegt. Zudem empfängt, koordiniert und kommuniziert es entsprechende Meldungen. Um alle 8.000 Benutzer des UKER im Krisenfall erreichen zu können, wurde eine Schnittstelle zum zentralen UKER-Katastrophenmanagement geschaffen und der Meldeweg im übergreifenden UKER-Notfallplan verankert.

Neben der Umsetzung dieser organisatorischen Maßnahmen wurden auch technische Maßnahmen eingeleitet, um die IT-Sicherheit am UKER zielgerichtet zu erhöhen. Es wurden ein zusätzlicher Malware-Scan von externen Mails eingerichtet, ein internes und ein externes Schwachstellenmanagement geschaffen sowie ein Projekt zur Einführung eines »Network Access Control« (NAC) gestartet. In Zukunft soll mit dem NAC der Netzwerkzugang am UKER flächendeckend reglementiert werden. Zudem wurde ein technisches Ausfallkonzept für das neue KAS und weitere IT-Systeme entwickelt. Dabei wurde auf dem neuen KAS eine Funktionalität eingerichtet, die die erforderlichen Dateien in einem zeitlich festgelegten Intervall aus dem IT-System kopiert und auf ein gesichertes Ablage- und Verteilsystem schreibt. Von dort werden die Dateien automatisch auf die PCs und Laptops der Stationen verteilt, auf denen der entsprechende Patient liegt. Die Dateien sind verschlüsselt und somit für den Standard-KAS-Benutzer nicht lesbar. Der Zugriff ist nur im Notfall über ein gesondert bereitgestelltes, versiegeltes Passwort möglich. Alle Zugriffe auf die Dateien werden geloggt und protokolliert. Hierdurch kann das klinische Personal auch im Falle eines Totalausfalls der IT-Systeme auf die Patientenakte der einliegenden Patienten zugreifen.

Alle B3S-Maßnahmen sowie deren Umsetzungsstand wurden in dem Unternehmenswiki Confluence und dem Aufgabenmanagementtool JIRA dokumentiert, kommuniziert und nachgehalten. JIRA eignete sich dabei besonders gut zur Maßnahmendokumentation und -delegation. Um die B3S-Controls strukturiert erfassen und abarbeiten zu können, wird am

Abb. 1 Ausschnitt aus dem JIRA-Addon »insight« mit dem Beispiel »B3S-Maßnahme«

MIK das JIRA-Addon »insight« genutzt. Es bietet neben dem sehr guten Überblick über die B3S-Maßnahmen auch die Möglichkeit, inhaltliche Querverlinkungen zu schaffen und somit Maßnahmen miteinander verknüpfen zu können.

Organisation des IT-Sicherheitsaudits

Für einen formal korrekten Ablauf des IT-Sicherheitsaudits müssen auch die prüfende Stelle und deren Prüfteam Nachweise gegenüber dem KRITIS-Betreiber bzw. dem BSI vorweisen. So wurde geprüft, ob sich die Auditgesellschaft auch als prüfende Stelle eignet [4]. Neben der Audit-, IT-Sicherheits- und Branchen-Kompetenz muss das Prüfteam auch eine »spezielle Prüfverfahrens-Kompetenz für § 8a« nachweisen können [5]. Zusätzlich zu diesen Nachweisen wurden am UKER noch Informationsgespräche mit potenziellen prüfenden Stellen geführt. Das Ziel dieser Gespräche war es, noch vor der Auftragserteilung herauszufinden, ob die prüfende Stelle Kenntnisse von klinischen Prozessen besitzt und versteht, dass der Ablauf kritischer klinischer Prozesse nicht durch Maßnahmen der IT-Sicherheit beeinträchtigt werden darf (z.B. im Bereich der Notaufnahmen).

Schlussendlich wurde eine prüfende Stelle ausgewählt, die alle Kriterien erfüllt. Nach Unterzeichnung einer Geheimhaltungsvereinbarung wurde den Auditoren der Zugang zu den QM-Dokumenten, den Risikoeinschätzungen und internen Betriebsabläufen verschafft. Ein zehn Tage langes Vor-Ort-Audit wurde terminiert.

Durchführung und Ergebnis des IT-Sicherheitsaudits (2019)

Im Vor-Ort-Audit wurden QM-typisch die jeweiligen B3S-Vorgaben besprochen, die dazugehörigen UKER-Regelungen/QM-Dokumente in Augenschein genommen und der Nachweis zur Umsetzung geprüft. Die Anzahl und Qualität der angefertigten QM-Dokumente wurde positiv durch die Auditoren hervorgehoben. Da zahlreiche Verfahren und Arbeitsschritte umfassend in QM-Dokumenten niedergeschrieben wurden, konnte den Auditoren schnell vermittelt werden, wie die jeweilige B3S-Vorgabe am UKER umgesetzt ist. In der Auditvorbereitung wurde akribisch geprüft, ob die einzelne B3S-Maßnahme durch ein QM-Dokument abgedeckt ist. Bei der Erstellung wurden immer die Fachexperten hinzugezogen. Die Benutzer können die verschiedenen QM-Dokumente im zentralen QM-System ansehen. Zudem werden sie über neue Dokumente per E-Mail oder Intranet-Blog-Nachrichten informiert. Verständlicherweise bleibt ihnen neben dem aufwendigen Routine-Betrieb nur wenig Zeit, um die relevanten QM-Dokumente lesen zu können. Dass die Regelungen dennoch gelesen wurden, zeigte sich im Vor-Ort-Audit, da mehrmals auf diese Regelungen verwiesen wurde. Der zeitliche Ablauf des zehn Tage dauernden Vor-Ort-Audits verlief reibungslos, weil das MIK zuvor die vom beauftragten Audit-Team definierten Prüfschwerpunkte auf die jeweiligen Vor-Ort-Prüftage aufteilte und die entsprechenden Fachexperten zu den einzelnen Terminen einlud.

Nach Erhalt des Auditberichts waren alle beteiligten MIK-Mitarbeiter erfreut, dass sich die lange und intensive Vorbereitungszeit bezahlt gemacht hatte. Durch die objektive, konkrete, teilweise sehr kritische Prüfung wurden Mängel dokumentiert, die sich zum Großteil mit der Einschätzung der eigenen Risikosituation deckten. Zwar konnte während des Audits nicht der gesamte Scope vollumfassend geprüft werden, jedoch gab es bei den Prüfschwerpunkten keine unvorhersehbaren Lücken oder Schwachstellen. Lediglich in den Bereichen, die bereits auf der internen Agenda standen, wurden Mängel gefunden. Trotz der umfassenden zeitintensiven Vorbereitungen und anfänglichen Ungewissheit bzgl. des Prüfungsablaufs wurde die Durchführung des IT-Sicherheitsaudits 2019 am MIK als positiv bewertet. Dies lag vor allem daran, dass durch das externe Audit ein offizielles und objektives Bild der IT-Sicherheit am UKER geschaffen wurde, das bereits bekannte Schwachstellen mit dem Gewicht eines externen Audits erneut adressiert und dass das ISMS als fortwährendes Maßnahmensteuerungswerkzeug etabliert wurde.

100% IT-Sicherheit wird es nie geben, auch wenn es uns in unserer hochtechnisierten Welt schwerfällt, dies zu akzeptieren. Nicht nur durch Vorsatz, sondern durch einfaches Anklicken des »falschen« Links in

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritisverordnung nach dem BSI-Gesetz
B3S	Branchenspezifische Sicherheitsstandards
DSB	Datenschutzbeauftragter
EDB	Emergency Decision Board
ISMS	Informations-Sicherheits-Management-System
ITSB	IT-Sicherheitsbeauftragter
KAS	Klinisches Arbeitsplatzsystem
kDL	kritische Dienstleistung
KRITIS	Kritische Infrastrukturen
MIK	Medizinisches Zentrum für Informations- und Kommunikationstechnik
MTA	maximal-tolerierbare Ausfallzeit
NAC	Network Access Control
QM	Qualitätsmanagement
UKER	Universitätsklinikum Erlangen

einer Mail können schwerwiegende IT-Sicherheitsvorfälle entstehen. Im universitären Umfeld gleicht die Herausforderung bzw. der Spagat zwischen »Convenience« für die Anwender und den Erfordernissen der IT-Sicherheit oftmals der Quadratur eines Kreises. Eine Sensibilisierung des gesamten Personals und kontinuierliche Fortbildungen zum Thema IT-Sicherheit sind notwendig. Diese können auch gut im Format eines informativen Quiz erfolgen und in Abhängigkeit von einer erreichten Punktzahl auf den Kenntnisstand des Anwenders eingehen. Entscheidend ist auch, dass das IT-Sicherheitsmanagement in der Breite funktioniert und die »Mauer der IT-Sicherheit« täglich auf gleichmäßigem Niveau mit Augenmaß hochgezogen wird, ohne einzelne Leuchttürme mit offenstehenden Toren zu bauen.

Empfehlungen

Bislang liegt der Schwellenwert aus der KRITIS-Verordnung bei 30.000 vollstationären Fällen pro Jahr. Krankenhäuser unter dem Schwellenwert fallen daher nicht unter das BSIG. Von Branchenkennern wird aber vermutet, dass die Schwellenwertgrenze wahrscheinlich gesenkt wird.

Krankenhäusern, die sich erstmals auf eine KRITIS-Prüfung vorbereiten müssen, würden wir folgende Empfehlungen mit auf den Weg geben:

- Im Krankenhaus sollte das Bewusstsein geschaffen werden, dass IT-Sicherheit kein Störfaktor im laufenden Betrieb ist und keine Mitarbeiter an den Pranger gestellt werden. Vielmehr bietet IT-Sicherheit die Chance, Krankenhausdaten und -prozesse fortlaufend zu schützen, so dass die tägliche IT-gestützte Arbeit aufrechterhalten wird. Ohne besondere Panik zu schüren, sollte klar sein, dass medizinische Daten in den Händen von Erpressern oder der Totalausfall der IT ein zu vermeidender Worst Case sind.
- IT-Sicherheit ist nicht das alleinige Thema der IT-Abteilung. Es sind alle Bereiche und Prozesse des Krankenhauses betroffen. So sollte die Verantwortung für IT-Sicherheit bei dem Vorstand bzw. der Geschäftsführung des KRITIS-Betreibers liegen. Zudem ist es sinnvoll, die Umsetzungsverantwortung des ISMS bei der IT-Abteilung anzusiedeln. Davon losgelöst sollte die Beratungs- und Revisionsfunktion Aufgabe des IT-Sicherheitsbeauftragten (ITSB) sein. Über ein Schulungs- und Informationskonzept sollten Benutzer und externe Dienstleister über IT-Sicherheit unterrichtet werden.
- Neue Organisationsstrukturen sollten geschaffen werden, wie z.B. die Stabsstellen des ITSB und DSB oder die Rolle des ISMS-Verantwortlichen. Darüber hinaus sollen ISMS-Regelkreise eingeführt werden, die auf der Leitungs- bis hin zur Arbeitsebene stattfinden.
- IT-Sicherheit kostet Ressourcen, die von oberster Stelle getragen werden sollten. Investitionen in entsprechend ausgebildetes Personal und in zeitgemäße IT-Sicherheitstechnik müssen mit eingeplant werden.
- Eine gründliche Vorbereitung und Organisation des IT-Sicherheitsaudits beansprucht je nach Krankenhausgröße und Stand der IT-Sicherheit viel Zeit. Vor allem die Erstellung der benötigten QM-Dokumente kostet Zeit. Dabei ist es empfehlenswert, rechtzeitig anzufangen und die Fachexperten schon bei den ersten Entwürfen einzubinden.
- Während der Auditvorbereitung ist es wichtig, den Überblick über noch offene organisatorische und technische Maßnahmen zu behalten. Ein computergestütztes Maßnahmentracking ist empfehlenswert.
- Eine Überregulierung des klinischen Betriebs ist zu vermeiden. Regelungen sind wichtig und notwendig, jedoch sollten der Handlungsspielraum und der Umsetzungsweg nicht durch eine Vielzahl von Arbeitsanweisungen überreguliert werden.
- Auch wenn das IT-Sicherheitsaudit vorüber ist, ist es wichtig, am Ball zu bleiben, um gegenüber neuen Schwachstellen und Angriffsmustern gewappnet zu sein. Ein kontinuierlicher Verbesserungsprozess sollte etabliert werden.
- Bei der Maßnahmenumsetzung ist es empfehlenswert die »Mauer der IT-Sicherheit« gleichmäßig hochzuziehen und nicht einzelne Leuchttürme zu bauen. Mögliche Einfallstore, die bestehende IT-Sicherheitsmaßnahmen konterkarieren, müssen identifiziert und beseitigt werden.
- Die Expertise eines externen Beraters ist für die Vorbereitung des IT-Sicherheitsaudits empfehlenswert, wenn die internen Ressourcen nicht vorhanden oder ausreichend sind bzw. noch keine ausreichenden Strukturen im Bereich IT-Sicherheit geschaffen wurden. ■

Quellen

1] Bundesministerium der Justiz und für Verbraucherschutz: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), siehe https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html (abgerufen am 14.10.2020)
[2] Bundesministerium der Justiz und für Verbraucherschutz: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) unter https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (abgerufen am 14.10.2020)
[3] Bundesministerium der Justiz und für Verbraucherschutz: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (abgerufen am 14.10.2020)
[4] Bundesamt für Sicherheit in der Informationstechnik: Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG. Version 1.1 2020, S. 12-13
[5] Bundesamt für Sicherheit in der Informationstechnik: Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG. Version 1.1 2020, S. 16-17

Der Elektronische Arztausweis Umsetzung gesetzlicher Vorgaben

gekürzter und modifizierter Auszug aus dem Hessischen Ärzteblatt 9 2020, 467-470

©Caroline McKenney

Ralf Münzing ist Leiter EDV und Organisationsentwicklung bei der Landesärztekammer Hessen.
ralf.muenzing@laekh.de

Zahlreiche digitale Anwendungen in der Patientenversorgung stehen vor der Tür. Um diese Anwendungen nutzen zu können, benötigen Ärztinnen und Ärzte einen elektronischen Arztausweis (eArztausweis oder eHBA).

Drei digitale Startanwendungen der Telematik-Infrastruktur sollen künftig einer besseren ärztlichen Information und Kommunikation dienen: das Notfallfalldatenmanagement (NFDM), der elektronische Medikationsplan (eMP) und die Kommunikation im Medizinwesen (KIM), siehe Infokästen 2 bis 4.

Für die Nutzung dieser medizinischen Anwendungen macht der Gesetzgeber hierbei eine grundsätzliche Vorgabe: den elektronischen Arztausweis. Damit wird sichergestellt, dass nur berechtigte Personen auf die medizinischen Daten des Versicherten zugreifen können. Eine weitere Anwendung, die vor ihrer bundesweiten Einführung steht, ist die elektronische Arbeitsunfähigkeitsbescheinigung (eAU).

Neben der grundsätzlichen gesetzgeberischen Vorgabe sind es die Funktionen des eArztausweises, die seinen Einsatz im Rahmen der Anwendungen notwendig machen. Insbesondere ist dies die qualifizierte elektronische Signatur (QES), mit der medizinische Dokumente (NFDM, elektronischer Arztbrief etc.) rechtsgültig elektronisch unterschrieben werden. Die QES ist rechtlich einer eigenhändigen Unterschrift des Arztes oder der Ärztin in der analogen Welt gleichgestellt.

Bis zum Herbst dieses Jahres soll ein Update der Praxis-IT-Systeme zur Verfügung stehen, das die medizinischen Anwendungen NFDM, eMP und KIM ermöglicht (siehe Kästen 2 bis 4). Da Patientinnen und Patienten gegenüber dem Vertragsarzt einen Anspruch auf die Erstellung eines Notfalldatensatzes und unter bestimmten Voraussetzungen auf einen eMedikationsplan haben, ist mit einer ansteigenden Nachfrage nach elektronischen Arztausweisen zu rechnen. Beide Anwendungen setzen diesen voraus.

Grundsätzlich ändert sich darüber hinaus das Verfahren der Ausstellung einer Arbeitsunfähigkeitsbescheinigung (AU). Nach wie vor erhält der Versicherte eine AU als Papierausdruck, den er an seinen Arbeitgeber weiterreicht.

Die Zuleitung der AU an die Krankenkasse übernimmt dann aber nicht mehr der Versicherte selbst, sondern der ausstellende Arzt. Er übermittelt über die Telematik-Infrastruktur die elektronische AU, die mit dem eArztausweis signiert wird, an die zuständige Krankenkasse. Die Übermittlung findet mittels KIM statt (siehe Kasten 4). Dieses neue Verfahren gilt auch für Arbeitsunfähigkeitsbescheinigungen, die im Zuge des Entlassmanagements durch stationär tätige Ärztinnen und Ärzte ausgestellt werden.

© Bundesärztekammer

Abb. 1: Musterbeispiel für einen Arztausweis

(1) Die gesetzliche Vorgabe

Nach § 291a Abs. 5 SGB V fordert der Gesetzgeber, dass die elektronische Gesundheitskarte nur in Verbindung mit einem elektronischen Heilberufsausweis oder einem entsprechenden Berufsausweis genutzt werden kann. Der elektronische Heilberufsausweis soll über eine qualifizierte Signatur verfügen und eine sichere Authentifizierung ermöglichen. Gemäß hessischem Heilberufsgesetz wird der Heilberufsausweis für Ärzte (der eArztausweis) von den Ärztekammern an ihre Mitglieder ausgegeben.

(2) Notfalldatenmanagement, NFDM

Ärzte und Zahnärzte können wichtige medizinische Notfalldaten direkt auf der Gesundheitskarte speichern, sofern der Patient in die Speicherung einwilligt. Im Notfalldatensatz können folgende Informationen gespeichert werden:

- Chronische Erkrankungen (z.B. Diabetes, koronare Herzkrankheit) und wichtige frühere Operationen (z.B. Organtransplantation),
- regelmäßig eingenommene Medikamente,
- Allergien und Unverträglichkeiten (besonders Arzneimittelallergien mit bekannter schwerer allergischer Reaktion),
- weitere wichtige medizinische Hinweise (wie Schwangerschaft oder Implantate) und
- ergänzend Kontaktdaten von Angehörigen, die im Notfall benachrichtigt werden sollen, und von behandelnden Ärzten (z.B. dem Hausarzt) und Zahnärzten.

Der Notfalldatensatz wird durch den anlegenden Arzt mit der qualifizierten elektronischen Signatur des eArztausweises unterschrieben.

Quelle: Bundesärztekammer

Ursprünglich sollte die elektronische AU ab dem 1. Januar 2021 starten, allerdings hat am 31. Juli 2020 das Bundesgesundheitsministerium der Forderung nach einer Übergangsregelung für die geplante elektronische Arbeitsunfähigkeitsbescheinigung zugestimmt. Die Vertragsärzte bekommen nun neun Monate Aufschub und müssen voraussichtlich erst ab Oktober 2021 die AU-Daten elektronisch an die Kassen übermitteln.

Kernfunktionen des elektronischen Arztausweises

Der eArztausweis besitzt fünf Kernfunktionalitäten:

1. **Sichtausweis:** Wie sein klassisches Pendant – der Arztausweis aus Papier – dient er zusammen mit dem amtlichen Lichtbildausweis als Sichtausweis, bspw. um in einer Apotheke verschreibungspflichtige Medikamente zu erwerben.
2. **Signatur:** Der Inhaber kann mit dem eArztausweis eine elektronische Unterschrift (Qualifizierte elektronische Signatur, QES) erstellen. Diese elektronische Signatur ist der eigenhändigen Unterschrift rechtlich gleichgestellt. Mit ihr können Arztbriefe, Abrechnungsunterlagen für die Kassenärztliche Vereinigung, Notfalldaten auf der elektronischen Gesundheitskarte, elektronische Rezepte oder elektronische Arbeitsunfähigkeitsbescheinigungen rechtssicher und medienbruchfrei elektronisch unterschrieben werden. Die elektronische Signatur wird mittels der Eingabe einer selbst vergebenen, mindestens sechsstelligen PIN ausgelöst.
3. **Authentifizierung:** Mit dem eArztausweis ist es möglich, sich in der elektronischen Welt sicher als »Arzt« auszuweisen, z.B. an Portalen von Kammern oder Arztnetzen oder in der Telematik-Infrastruktur. Unsichere Anmeldeverfahren können ersetzt und auf ein höheres Sicherheitsniveau angehoben werden. Diese Funktionalität ist der Kern für den späteren Zugriff auf die elektronischen Patientenakten von Versicherten.
4. **Vertraulichkeit:** Der eArztausweis ist in der Lage, medizinische Daten sicher zu ver- und entschlüsseln. Damit steigt das Datenschutz- und Sicherheitsniveau bei der Übertragung personenbezogener medizinischer Daten oder bei vertraulichen Informationen deutlich.
5. **eGK-Zugriff:** Mit dem eArztausweis kann auf medizinische Daten zugegriffen werden, die auf der eGK des Patienten abgespeichert sind wie bspw. »Notfalldaten« und »elektronischer Medikationsplan«.

Der elektronische Arztausweis ist also zukünftig integraler Bestandteil der ärztlichen Berufsausübung. Dieser behält seine Gültigkeit auch dann, wenn der Arzt die Ärztekammer wechselt, er ist ein Heilberufsausweis gemäß SGB V §291a.

Grundsätzlich benötigen Ärztinnen und Ärzte einen solchen Ausweis, wenn sie zukünftig Anwendungen in der Telematik-Infrastruktur bedienen müssen. In den letzten Jahren wurde die Telematik-Infrastruktur durch Gesetze wie das Terminservice- und Versorgungsgesetz, das Digitale-Versorgung-Gesetz und das Patientendatenschutzgesetz immer feiner ausgestaltet und die Anwendungen immer detaillierter beschrieben. Insbesondere bei den elektronischen Anwendungen Notfalldatenmanagement, eMedikationsplan und elektronische Patientenakte erfolgt zukünftig der Zugriff über einen eArztausweis. Vertragsärztlich niedergelassene Ärzte müssen somit praktisch über einen eArztausweis verfügen.

Allerdings ist klar, das allen Ärzten, die keinen eArztausweis besitzen, der Zugriff auf bestimmte Informationen langfristig versperrt sein wird, auch stationär im Krankenhaus und rein privatärztlich Tätigen, die eventuell Daten der Gesundheitskarte auslesen möchten oder müssen. Insofern ist davon auszugehen, dass langfristig jeder Arzt einen solchen Ausweis haben muss.

Auch privatärztlich tätige Ärzte können einen eArztausweis bestellen, falls Sie ihn für Anwendungen der Telematik-Infrastruktur benötigen. Die Anbindung einer privatärztlichen Praxis an die Telematik-Infrastruktur ist noch nicht abschließend geklärt.

Sicherheit bei der Herausgabe des elektronischen Arztausweises

Da der eArztausweis in der digitalen Welt die oben genannten weitreichenden Einsatzmöglichkeiten hat, ist seine Ausgabe unter hohen Sicherheitsmaßnahmen vorgesehen. Eine sichere Identifizierung des antragstellenden Arztes oder der antragstellenden Ärztin ist – neben der sicheren Auslieferung – Voraussetzung für den Erhalt eines eHBA. Die Landesärztekammer Hessen ist zwar per Gesetz für die Herausgabe der eArztausweise zuständig, die notwendige technische Infrastruktur wird jedoch von zugelassenen sogenannten Vertrauensdiensteanbietern (VDA)

(3) Elektronischer Medikationsplan (eMP)

Ärzte, Zahnärzte und Apotheker können den E-Medikationsplan direkt auf der Gesundheitskarte speichern, sofern der Patient in die Speicherung einwilligt und der Patient mindestens drei verordnete Medikamente gleichzeitig einnimmt. Zu den Daten des E-Medikationsplans gehören:

- Angaben zur Medikation, d.h. alle Arzneimittel, die ein Patient einnimmt, und Informationen zur Anwendung (Dosierung, Zeitpunkt, Darreichungsform etc.). Dies umfasst sowohl die vom Arzt oder Zahnarzt verordneten Medikamente als auch Arzneimittel, die rezeptfrei in der Apotheke erworben wurden (OTC). Zusätzlich sind Arzneimittel aufgeführt, die aktuell nicht mehr angewendet werden, die jedoch für die Überprüfung der Sicherheit der Arzneimitteltherapie durch den Arzt, Apotheker oder Zahnarzt relevant sein können.
- Medikationsrelevante Daten wie Allergien und Unverträglichkeiten.

Quelle: Bundesärztekammer

(4) Kommunikation im Medizinwesen (KIM)

KIM sorgt für den sicheren Austausch von sensiblen Informationen wie Befunden, Bescheiden, Abrechnungen oder Röntgenbildern über die Telematikinfrastruktur zwischen verschiedenen Ärzten bzw. mit Apothekern etc. Nachrichten und Dokumente können künftig schnell und zuverlässig per sicherer E-Mail – mit oder ohne Anhang – ausgetauscht werden. KIM bringt folgende Vorteile:

- Vertraulichkeit der Nachrichten: Kartenbasierte Verschlüsselung macht ein unberechtigtes Mitlesen unmöglich. Sensible Daten können immer nur von demjenigen gelesen werden, für den sie gedacht sind.
- Fälschungssicher: KIM-Nachrichten können nicht unbemerkt manipuliert werden. Adressaten erkennen immer, ob sie die E-Mail so erhalten haben, wie sie der Absender auch verschickt hat.
- Geprüfte Identität: Empfänger einer Nachricht können immer sicher sein: Wer als Absender draufsteht, ist auch der Absender der Nachricht. Die Identitäten der KIM-Teilnehmer sind geprüft und bestätigt.
- Schnelle Auffindbarkeit: Alle KIM-Teilnehmer sind im zentralen Adressbuch z.B. über die Praxisanschrift auffindbar. Es entfällt ein umständliches und fehleranfälliges Suchen oder Austauschen von E-Mail-Adressen.
- Abrechenbarkeit: KIM ist das sichere Übermittlungsverfahren nach § 291b Abs. 1e SGB V und dadurch die Basis für eine mögliche Vergütung.

Der eArztausweis wird für die Verschlüsselung der versendeten Inhalte sowie für die Signatur bspw. eines angehängten Arztbriefs genutzt.

Quelle: Bundesärztekammer

angeboten. Diese VDA produzieren konform zur eIDAS-Verordnung der EU die Ausweise und betreiben die Infrastrukturen für die Prüfbarkeit der elektronischen Signaturen etc. Aktuell sind die folgenden Anbieter seitens der Ärztekammern zugelassen:

- Bundesdruckerei (D-Trust GmbH),
- medisign GmbH,
- SHC Stolle & Heinz Consultants GmbH/Atos GmbH und
- T-Systems GmbH.

Jeder Vertrauensdiensteanbieter bietet mindestens die kostenlose Identifizierung des Antragstellers in einer Postfiliale (sog. Postident-Verfahren) an. Darüber hinaus können weitere unterschiedliche Identifizierungsverfahren der VDA (z.B. Video-Ident, Online-Identifizierung mittels des neuen Personalausweises) in Anspruch genommen werden.

Beantragung eines elektronischen Arztausweises bei der Landesärztekammer Hessen

Um ihren Mitgliedern die Beantragung eines eArztausweises so leicht wie möglich zu machen, hat die Ärztekammer den Bestellvorgang in ihrem Mitgliederportal integriert. Zur Antragstellung sind u.a. folgende Schritte erforderlich:

1. Im Schritt 1 erfolgt die Prüfung und Bestätigung der Meldedaten durch die Landesärztekammer Hessen. Sind diese korrekt, werden sie später für die Vorbefüllung des Antrages verwendet.
2. Bei einer Erstbestellung eines elektronischen Arztausweises wird eine sogenannte Telematik-ID vergeben. Diese ist eine eindeutige Nummer des Karteninhabers in der Telematikinfrastruktur und notwendig, um dem Karteninhaber beispielsweise Zugriffsrechte zuweisen zu können.
3. Danach wählt der Arzt/die Ärztin einen von den Ärztekammern zugelassenen Vertrauensdiensteanbieter (Kartenhersteller) aus, der seine/ihre Karte produzieren wird. Über Links kann man sich über die Kartenhersteller sowie deren Leistungen und Kosten informieren.
4. Im nächsten Schritt erhalten die Ärzte/Ärztinnen nochmals eine Übersicht der Daten. Nun können sie die verbindliche Bestellung auslösen.

Abkürzungen

AU	Arbeitsunfähigkeitsbescheinigung
eAU	elektronische Arbeitsunfähigkeitsbescheinigung
eGK	elektronische Gesundheitskarte
eHBA	elektronischer Heilberufsausweis
eIDAS	elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
eMP	elektronischer Medikationsplan
EU	Europäische Union
FAQ	Frequently Asked Questions (häufige Fragen)
ID	Identifikation
KIM	Kommunikation im Gesundheitswesen
LÄKH	Landesärztekammer Hessen
NFDM	Notfalldatenmanagement
OTC	Over-the-counter (OTC drug - rezeptfreies Arzneimittel)
PIN	Persönliche Identifikationsnummer
QES	qualifizierte elektronische Signatur
SGB	Sozialgesetzbuch
VDA	Vertrauensdiensteanbieter

5. Nun ist der Antragsprozess im Portal der Landesärztekammer Hessen abgeschlossen. Die Mitarbeiterinnen und Mitarbeiter der Landesärztekammer bereiten die Daten der Ärzte/Ärztinnen für die Übergabe an den Kartenhersteller auf. Nach der Datenübergabe bekommen die Antragsteller eine E-Mail-Nachricht mit einer Vorgangsnummer des Kartenherstellers und einen Link zu dessen Antragsportal. Die Vorgangsnummer wird im Antragsportal des Kartenherstellers benötigt, um den mit seinen Daten bereits gefüllten Antrag laden und weiterbearbeiten zu können. Dazu dient der in der E-Mail-Nachricht enthaltene Link. Die Weiterbearbeitung des Antrages im Portal des Kartenherstellers beinhaltet das Ausfüllen verschiedener Antragsunterlagen sowie das Hochladen eines Passbildes.
6. Der Antrag muss nun ausgedruckt und unterschrieben werden.
7. Abschließend findet die Identifizierung des Antragstellers anhand eines gültigen amtlichen Ausweisdokuments (Personalausweis, Reisepass, ggf. Aufenthaltsbescheinigung) statt, wozu der Antragsteller eine Identifizierungsstelle (z.B. Postfiliale) aufsuchen muss. Nach erfolgter Identifizierung sind dort die vollständigen Antragsunterlagen abzugeben.

Im Hintergrund erfolgt eine Weiterleitung und Freigabe des Antrags durch die Landesärztekammer Hessen gegenüber dem Kartenhersteller. Sie prüft, ob der Antragsteller Mitglied der Ärztekammer und Arzt ist, und erteilt dem ausgewähltem Vertrauensdiensteanbieter die Erlaubnis, den eArztausweis herzustellen. Der Anbieter produziert und versendet den eArztausweis – getrennt von einem PIN-Brief – an den Antragsteller.

Die Ärztin oder der Arzt muss den erhaltenen Ausweis »in Betrieb nehmen« bzw. aktivieren, das heißt, es müssen individuelle PINs gesetzt und der Erhalt und die erfolgreiche Inbetriebnahme gegenüber dem Kartenhersteller bestätigt werden. Daraufhin schaltet der Kartenhersteller den Ausweis frei. ■

Bianca Steiner (M.Sc. Informatik mit Schwerpunkt Medizinische Informatik) arbeitet seit 2015 als wissenschaftliche Mitarbeiterin am Peter L. Reichertz Institut für Medizinische Informatik in Braunschweig. Bianca.Steiner@plri.de

Datenschutz in einem Behandlungsverbund aus Sicht von multimorbiden Patienten mit Demenz

- Hoher Versorgungs- und Dienstleistungsbedarf multimorbider Demenzpatienten über Sektorengrenzen hinweg.
- Für eine effiziente Versorgung sollten Behandlungsverbünde Zugriff auf relevante Patientendaten haben.
- Einwilligung der Betroffenen zur Durchführung medizinischer Maßnahmen im Behandlungsverbund i.d.R. erforderlich.
- Einwilligungs(un)fähigkeit von Patienten mit einer demenziellen Erkrankung ist nur schwer valide festzustellen.
- S2k-Leitlinie »Einwilligung von Menschen mit Demenz in medizinischen Maßnahmen« bietet wichtige Handlungsempfehlungen.

Herausforderung bei der Versorgung multimorbider Demenzpatienten im Behandlungsverbund

Die sich demografisch und soziokulturell wandelnde Gesellschaft stellt das Gesundheitssystem vor eine Vielzahl von Herausforderungen sowohl aus medizinischer als auch aus gesundheitsökonomischer Perspektive. Die Entwicklung neuer Versorgungskonzepte und eine gezielte digitale Modernisierung der Versorgungsprozesse bieten große Potenziale, diese Herausforderungen zu bewältigen. Insbesondere bei der Behandlung multimorbider Patienten mit Demenz spielen digitale Lösungen eine immer größere Rolle. Sie können im intersektoralen Versorgungsprozess dazu beitragen, Behandlungsverbünde aufzubauen, die den Menschen und seine Erkrankung in den Mittelpunkt rücken, um ihn effizient und effektiv zu versorgen.

Schätzungen zufolge leiden in Deutschland etwa 1,6 Millionen Menschen über 65 Jahre an einer demenziellen Erkrankung [1]. Unter anderem führt die immer höhere Lebenserwartung in Deutschland dazu, dass die absolute und relative Anzahl stetig weiter steigt, mit einer geschätzten Prävalenz von 2,4 bis 2,8 Millionen im Jahr 2050 [1].

Begleitet wird die Demenz häufig von weiteren Erkrankungen (Komorbidität), die mit dem fortschreitenden Alter und der Verschlechterung des Gesundheitszustands assoziiert sind [2]. Die daraus resultierende Multimorbidität geht häufig mit einem hohen Versorgungs- und Dienstleistungsbedarf, sowohl pflegerisch als auch medizinisch, über alle Sektoren einher. Dabei werden die allgemeingültigen Herausforderungen der intersektoralen Versorgung im Behandlungsverbund durch demenzbedingte Einschränkungen der Kognition, Wahrnehmung und Artikulation nochmals

verstärkt [3]. So sind Menschen mit einer Demenz, vor allem in fortgeschrittenen Stadien, oft nicht mehr in der Lage, selber über ihre persönlichen und gesundheitlichen Daten Auskunft zu geben oder über deren Schutz zu entscheiden.

Fortlaufend sind vom Patienten Entscheidungen zu diagnostischen und therapeutischen Maßnahmen zu treffen [4]. Aufgrund fehlender Transparenz im Versorgungsprozess, fehlenden Wissens über die eigene Erkrankung sowie der Vielzahl an möglichen Maßnahmen sind oftmals bereits Patienten ohne kognitive Einschränkung mit diesen Entscheidungssituationen überfordert. Hinzu kommt, dass i.d.R. eine explizite Einwilligung zur Durchführung der Maßnahmen erforderlich ist [4].

Doch wie sieht es mit der Einwilligungsfähigkeit eines Patienten mit einer demenziellen Erkrankung aus? Wird diese im Behandlungsverbund überhaupt benötigt? Wie kann festgestellt werden, ob ein Demenzpatient noch einwilligungsfähig ist bzw. ob die Einwilligungsfähigkeit im Sinne des »Supported Decision Making« hergestellt werden kann [4]? Wie kann bei Entscheidungen durch Dritte gewährleistet werden, dass die Interessen des Patienten gewahrt sind? Diesen Fragen widmet sich der vorliegende Artikel zunächst generell am Anwendungsfall des Behandlungsverbunds und schließlich an einem konkreten Projekt zum intersektoralen Versorgungsmanagement multimorbider Demenzpatienten.

Datenschutzrechtliche Rahmenbedingungen im Behandlungsverbund

Nach Art. 5 Abs. 1 sowie Art. 6 Abs. 1 der europäischen Datenschutzgrundverordnung (DSGVO) ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur erlaubt, soweit dies auf einer gesetzlichen Ermächtigungsgrundlage gestattet ist bzw. eine Einwilligung der Betroffenen vorliegt. Personenbezogene Daten, wie die Stammdaten eines Patienten, dürfen von Behandlern aufgrund allgemeingültiger Erlaubnistatbestände, wie der Erfüllung eines Vertrags (Art. 6 Abs. 1 DSGVO), verarbeitet werden. Soweit bekannt, lässt sich die Weitergabe und Verarbeitung von Daten in einem Behandlungsverbund mit den in Betracht kommenden Tatbeständen zur Verarbeitung personenbezogener Daten von Art. 9 DSGVO nicht abdecken. So wird bspw. bei der Datenverarbeitung in Behandlungsverbünden i.d.R. kein unmittelbarer Versorgungsvertrag mit den Betroffenen geschlossen, wie es bei der einrichtungsbezogenen Versorgung üblich ist. Insbesondere im Hinblick auf die in einem Behandlungsverbund verarbeiteten Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO reichen die in Betracht kommenden Tatbestände nicht aus. Bei diesen personenbezogenen Daten handelt es sich um sensible, besonders schützenswerte und infolgedessen als besonders kritisch zu bezeichnende Daten. Hier sieht das Datenschutzrecht eine Verarbeitung grundsätzlich nur unter den gesetzlichen Schranken des Art. 9 DSGVO (hier nicht anwendbar) bzw. auf Basis einer freiwilligen, informierten Einwilligung der Betroffenen vor. Zusätzlich unterliegen sämtliche Daten der Patienten (d.h. nicht nur die Gesundheitsdaten) den beruflichen Verschwiegenheitspflichten nach § 203 Strafgesetzbuch (StGB) auf Seiten der Behandler. Sofern ihnen die Weitergabe der umfassend geschützten Angaben über einen Patienten nicht nach einer gesetzlichen Norm bzw. in raren berufsrechtlich anerkannten Gründen der Verfolgung eigener Interessen gestattet ist, ist ihnen eine Weitergabe der geschützten Angaben an eine andere Einrichtung oder einen anderen Behandler (und in manchen Fällen sogar innerhalb ihrer eigenen Einrichtung) nur mit vorheriger Einwilligung, hier im Speziellen einer Schweigepflichtentbindung, möglich. Dementsprechend wird als Ermächtigungsgrundlage und inhaltliche Grenze für die Zusammenarbeit und den Informationsaustausch zwischen den Behandlern in einem Behandlungsverbund multimorbider Demenzpatienten eine Einwilligungs- und Schweigepflichtentbindungserklärung benötigt. Auch wenn eine demenzielle Erkrankung die Einwilligungsfähigkeit eines Patienten nicht von vorneherein ausschließt [4], so liegt gerade in späteren Stadien der Erkrankung, in denen die kognitive Beeinträchtigung zunimmt, häufig keine Entscheidungs- und Einwilligungsfähigkeit mehr vor.

Einwilligung und Einwilligungsfähigkeit demenziell erkrankter Patienten

Bei der Einholung einer Einwilligung eines Demenzpatienten zur Durchführung diagnostischer und therapeutischer Maßnahmen sowie bei der Bestimmung der Einwilligungsfähigkeit und angemessenen Vertretung der Interessen der Patienten existiert eine Vielzahl von Herausforderungen. Die S2k-Leitlinie »Einwilligung von Menschen mit Demenz in medizinischen Maßnahmen« bietet daher 33 Handlungsempfehlungen »[…] zur Sicherung der [Autonomie und] Handlungsfähigkeit von Menschen mit Demenz in Entscheidungssituationen […]« [4]. Darüber hinaus dient die Leitlinie dazu »[…] auf Seiten der handelnden Berufsgruppen die ethische Qualität der Entscheidung und die Rechtmäßigkeit (u.a. informierte Einwilligung) […]« [4] zu gewährleisten.

Zunächst ist zu beurteilen, ob ein Patient mit einer demenziellen Erkrankung selbst noch einwilligungsfähig ist oder nicht. Hierbei kommen neben einfachen Leitfragen auch geriatrische Assessments, wie der Mini-Mental-Status-Test, zum Einsatz, um die Kriterien Informationsverständnis, Einsicht, Urteilsvermögen und Kommunizieren einer Entscheidung zu prüfen [4]. Hierbei ist festzuhalten, ob vorhandene Einschränkungen dauerhaft oder nur vorübergehend

Nach Tätigkeiten im anbulanten Sektor, hier Qualitätsmanagement und Praxisorganisation, leitet Claudia Möller (Dipl.-Pflegewirtin (FH)) seit 2015 den Zentralen Dienst FuE & Innovationsmanagement bei AGAPLESION gAG. Claudia.Moeller@agaplesion.de

Tab. 1: Berechtigungsgruppen und deren Rechte in CASEPLUS-SimPat

Berechtigungsgruppen	Zuordnung	Beschreibung der Rechte
Behandler	Hausärzte, Fachärzte, Krankenhausärzte, Pflegekräfte	Dokumentation der Behandlung. Erstellen von Zugriffstoken.
Entlassmanagement im Krankenhaus	Sozialarbeiter im Krankehaus	Dokumentation in der stationären Behandlungsakte. Erstellen von Zugriffstoken.
Angehöriger/Patient	Eltern, Kinder, Geschwister, Vormund, Patient	Einsehen der Fallakte im Angehörigen-Portal. Hoch- und Herunterladen eigener Dokumente.
Systemadministrator	SimPat-Mitarbeiter	Konfiguration von Berechtigungsgruppen.
Benutzeradministrator	SimPat-Mitarbeiter	Anlegen und Pflege des Adressbuchs sowie von Benutzern.
Case-Manager	SimPat-Mitarbeiter	Angehörigen Aufgaben und Erinnerungen zur Unterstützung zuweisen. Netzwerk anlegen und pflegen.

sind und damit die Einwilligungsfähigkeit evtl. wiederhergestellt werden kann. Ist die Prüfung nicht eindeutig, wird dazu geraten, die entsprechenden Tests und Befragungen, ggf. mit Unterstützung durch eine Vertrauensperson, zu wiederholen. Das Ergebnis der Prüfung ist gemäß § 630f Abs. 1 und Abs. 2 Satz 1 Bürgerliches Gesetzbuch (BGB) entsprechend zu dokumentieren.

Ist der Patient einwilligungsfähig, ist dieser in geeigneter Form, schriftlich und mündlich, über die Art und den Umfang der Verarbeitung seiner personenbezogenen Daten im Behandlungsverbund aufzuklären (§ 630e BGB). Dabei ist darauf zu achten, dass die Information und Aufklärung »[…] die sprachlichen, kognitiven und emotionalen Kompetenzen des Patienten berücksichtigt […]« [4].

Ist der Patient einwilligungsunfähig, ist die Einwilligung zur Verarbeitung personenbezogener Daten im Behandlungsverbund sowie zur Schweigepflichtentbindung – nach entsprechender Aufklärung und Information – durch eine berechtigte dritte Person einzuholen (§ 630d Abs. 1 Satz 2 und § 630e Abs. 4 BGB), d.h. den gesetzlichen Vertreter des Patienten oder einen rechtsgeschäftlich Bevollmächtigten [4]. Auch in diesem Fall ist der Patient, soweit möglich und soweit dies nicht seinem Gesundheitszustand schadet, in angemessener, den Defiziten angepasster Form über das Vorhaben aufzuklären (§ 630e Abs. 5 BGB). Bei dem gesetzlichen Vertreter kann es sich entweder um einen Familienangehörigen, Berufsbetreuer oder qualifizierten ehrenamtlichen Betreuer handeln. Solange der Patient noch dazu in der Lage ist, selbstständige bzw. assistierte Entscheidungen zu treffen, kann dieser seinen Betreuer und dessen Aufgabenumfang selbst bestimmen. Über eine Vorsorgeverfügung bzw. Vorsorgevollmacht kann hierbei definiert werden, wer als gesetzlicher Vertreter bei einer Verschlechterung des Gesundheitszustands mit Verlust der Entscheidungsfähigkeit eingesetzt werden soll [4]. Andernfalls wird ein gesetzlicher Vertreter zugewiesen. Bei der Einwilligung durch Dritte sind stets die Wünsche und Präferenzen des Demenzpatienten zu berücksichtigen. Dabei stellt sich die Frage, von wem diese am besten umgesetzt werden können, einem Berufsbetreuer oder einem Angehörigen. Während ein Berufsbetreuer mehr Erfahrung mit den entsprechenden Prozessen hat, ist davon auszugehen, dass ein selbst als gesetzlicher Vertreter gewählter Angehöriger besser einschätzen kann, was der Patient tatsächlich will. Dies muss jedoch nicht zwingend heißen, dass dies auch im Sinne des Patienten umgesetzt wird. Oftmals handelt es sich um hoch emotionale Entscheidungen, die dann eher im Interesse des Angehörigen statt des Patienten getroffen werden; es sei denn die Entscheidung ist explizit in der Vorsorgevollmacht hinterlegt.

Das SimPat-Projekt

»Sicherung intersektoraler Versorgung durch ein IT-gestütztes Dienstleistungskonzept für multimorbide Patienten mit Demenz« (SimPat) ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Verbundprojekt, das im Rahmen des »Aktionsplans Dienstleistung 2020« unter der Maßnahme »Dienstleistungsinnovationen durch Digitalisierung« durchgeführt wurde. SimPat umfasst die Entwicklung, Umsetzung und Evaluation eines digitalen Fallmanagementsystems für multimorbide Patienten mit Demenz [5]. Durch den Einsatz der IT-Lösung »CASEPLUS-SimPat« soll der Behandlungsverbund zwischen betreuenden Angehörigen, professionell Pflegenden, Ärzten und Therapeuten gestärkt werden, indem die Interaktion zwischen den unterschiedlichen Leistungserbringern erleichtert wird [5]. CASEPLUS-SimPat konzentriert sich auf die interdisziplinäre Versorgung von Demenzpatienten mit einer sturzbedingten Fraktur, wie einer Femurfraktur, und einem sich anschließenden stationären Krankenhausaufenthalt. Das Fallmanagementsystem adressiert primär die Schnittstelle zwischen stationärer und ambulanter Versorgung – im Sinne des Rahmenvertrags über ein Entlassmanagement beim Übergang in die Versorgung nach Krankenhausbehandlung nach § 39 Abs. 1a S. 9 SGB V. CASEPLUS-SimPat ist damit als eine digitale Fallakte anzusehen, die eine zeitnahe Bereitstellung relevanter Informationen für die an der Versorgung eines Patienten beteiligten Akteure ermöglicht. Somit kann sowohl die Versorgung im Krankenhaus als auch die nachfolgende Versorgung frühestmöglich organi-

siert, optimiert und damit für alle Beteiligten eventuell wirtschaftlicher gestaltet werden. Informationen zum aktuellen Behandlungsfall werden strukturiert für einzelne Behandler bereitgestellt. Hierzu zählen sowohl Informationen zur Fallsteuerung, wie das Aufnahmedatum im Krankenhaus oder das voraussichtliche Entlassdatum, als auch Informationen zur Behandlungsdokumentation, wie die Anamnese, Diagnose, Befunde oder Angaben zum einweisenden und weiter behandelnden Arzt. Durch eine Auflistung der beteiligten Akteure – Einrichtungen, Behandler und Ansprechpartner – wird außerdem die Kontaktaufnahme zur Klärung versorgungsrelevanter Fragen erleichtert. Ebenso können Dokumente für andere Behandler im Fallmanagementsystem hinterlegt werden, wie z.B. Arztbrief, Medikationsplan, Wunddokumentation oder Pflegebegleitbericht [5]. Für eine gute Versorgung relevante, aber teilweise fehlende Informationen zur bisherigen Versorgung, zu Medikamenten und zu Allergien sowie zum persönlichen Umfeld, zu Vorlieben und zu Verhaltensweisen sind mittels CASEPLUS-SimPat einfach auszutauschen.

Zur besseren Einbindung von (pflegenden) Angehörigen in den Versorgungsprozess wird das Fallmanagementsystem durch ein Angehörigen-Portal ergänzt. Dieses bietet Angehörigen Zugriff auf versorgungsrelevante Informationen und Dokumente und stellt eine Vielzahl von E-Learnings rund um das Thema Demenz bereit [5].

Umsetzung datenschutzrechtlicher Anforderungen im SimPat-Projekt

Die datenschutzrechtlichen Anforderungen im SimPat-Projekt wurden in einem umfangreichen Datenschutzkonzept festgehalten. Dies beinhaltet neben einer detaillierten Betrachtung der beteiligten IT-Systeme, in Bezug auf die Datensicherheit und den Datenschutz, u.a. eine Übersicht der technischen und organisatorischen Maßnahmen im System nach Art. 32 Abs. 1 und Art. 25 Abs. 1 DSGVO sowie eine ausführliche Risikoanalyse. Rechtsgrundlage für die Datenverarbeitung bilden die EU-DSGVO und das Bundesdatenschutzgesetz (BDSG). Da das AGAPLESION ELISABETHENSTIFT (EKE) in Darmstadt als Pilotstandort des Projekts eine Einrichtung der evangelischen Kirche ist, unterliegt dieses weiterhin dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

Ansprache und Identifikation geeigneter Patienten

Die Ansprache der Patienten bzw. Betreuer und die Identifikation als mögliche SimPat-Patienten erfolgen möglichst bei Aufnahme im Krankenhaus; in einigen Fällen auch zu einem späteren Zeitpunkt bei Aufnahme auf der »Interdisziplinären Alterstraumatologie« (IDA) des EKE. Durch einen Facharzt für Innere Medizin und Geriatrie oder Sozialarbeiter im Krankenhaus werden hierbei folgende Kriterien geprüft:

1. Stationärer Behandlungsbedarf nach einem traumatischen Sturzereignis
2. Relevante kognitive Einschränkung (positiver IDA-Check)
3. Stationäre Aufnahme auf der Geriatrie, IDA oder der Unfallchirurgischen Station

Bei Erfüllung der Kriterien und vorliegender, unterzeichneter Einwilligungserklärung wird der Patient im klinischen Informationssystem als Teilnehmer des Projekts gekennzeichnet. Dies führt zu einem automatischen Stammdatenexport aus dem klinischen Informationssystem des EKE und zum Import der Daten in CASEPLUS-SimPat. Auch weitere bereits zur Verfügung stehende behandlungsrelevante Patientendaten werden in diesem Schritt automatisiert ins Fallmanagementsystem übernommen.

Einwilligung der Betroffenen und Zugriffssteuerung

Voraussetzung für den Einsatz von CASEPLUS-SimPat in einem Behandlungsverbund ist die Einwilligung der Betroffenen, dass deren personenbezogene Daten im Sinne des Art. 4 Abs. 1 DSGVO bzw. § 4 Abs. 1 und 2 DSG-EKD im klinischen Informationssystem erhoben und im Fallmanagementsystem verwendet werden sollen. Hierzu zählen neben den Patienten auch deren gesetzliche Vertreter sowie die am Behandlungsverlauf beteiligten Akteure, wie z.B. Hausärzte, Krankenhausärzte und Pflegepersonal (siehe Tabelle 1). Das EKE fungiert hierbei als Betreiber der Plattform CASEPLUS-SimPat sowie teilnehmendes Krankenhaus und verantwortliche Stelle für die Übermittlung und Verarbeitung der Daten. Behandler – im Pilotprojekt niedergelassene Ärzte, Altenpflege, ambulanter Pflegedienst – werden als verantwortliche Stellen für die

Abkürzungen

BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung
BDSG	Bundesdatenschutzgesetz
CRUD	Create, Read, Update, Delete
DSG-EKD	Datenschutz in der Evangelischen Kirche in Deutschland
DSGVO	Datenschutzgrundverordnung
EKE	AGAPLESION ELISABETHENSTIFT
EU-DSGVO	Europäische Datenschutzgrundverordnung
IDA	Interdisziplinäre Alterstraumatologie
SimPat	Sicherung intersektoraler Versorgung durch ein IT-gestütztes Dienstleistungskonzept für multimorbide Patienten mit Demenz
StGB	Strafgesetzbuch

ihnen übermittelten Daten bzw. von ihnen bereitgestellten Inhalte für die Zwecke der Durchführung ihrer Funktion im Behandlungsverlauf per Beitrittserklärung in das Projekt eingeschlossen. Patienten treten dem Projekt entweder selbst oder gerade in späteren Stadien der Demenzerkrankung durch einen gesetzlichen Vertreter per Einwilligungserklärung bei. Dabei ermächtigen sie das EKE zur Datenverarbeitung im Sinne des mit CASEPLUS-SimPat durchzuführenden Fallmanagements und entbinden die von ihnen in der Einwilligungserklärung explizit angegebenen Behandler von ihrer Schweigepflicht. Auch eine nachträgliche Schweigepflichtentbindung und somit eine Beteiligung an der in CASEPLUS-SimPat hinterlegten Fallakte ist möglich. Dies erfolgt über einen Zugriffstoken, der von einem Sozialarbeiter im Krankenhaus über CASEPLUS-SimPat erstellt, dem Patienten oder Betreuer in gedruckter Form ausgehändigt und anschließend von diesem an den entsprechenden zu berechtigenden Behandler übergeben wird. Auf diese Weise kann nicht nur die Einwilligung zum Informationsaustausch zwischen Behandlern erteilt, sondern auch die freie Behandlerwahl gewährleistet werden.

Rollen und Rechte im Rahmen der Behandlungsdokumentation und -steuerung

Die eigentliche Betreuung bzw. Behandlungssteuerung des Patienten erfolgt innerhalb der beteiligten Sektoren durch einzelne an der Fallakte beteiligte Behandler. Dabei hat jeder Behandler ausschließlich auf die Reiter, Funktionen und Daten einer Fallakte Zugriff, die seiner Rolle entsprechen. Insgesamt wird zwischen sechs Rollen und somit Berechtigungsgruppen unterschieden (siehe Tabelle 1). Weitere Berechtigungsgruppen können zur Laufzeit des Systems von einer entsprechend berechtigten Person über die Funktion »Berechtigungsgruppen bearbeiten« erstellt und konfiguriert werden. Somit ist es bspw. möglich, weitere Behandler wie Therapeuten in die Fallakte einzubinden und für diese individuellen Sichten bereitzustellen.

Das Rechtemodell sieht vor, Berechtigungen gemäß dem CRUD-Ansatz – Create, Read, Update, Delete – einzeln zu vergeben. Behandler können jeweils nur die Fälle einsehen und bearbeiten, die ihnen bzw. ihrer Organisation zugeordnet sind. Die entsprechende Berechtigung wird über die Zuweisung des Krankenhauses (Organisation) bzw. eines Leistungserbringers (Einzelperson) zu einer Fallakte erteilt. Dies geschieht entweder durch direkte Freigabe durch den Patienten bzw. gesetzlichen Vertreter oder aber über einen Zugriffstoken. Angehörige bzw. Patienten erhalten nur Zugriff auf Daten und Dokumente des »eigenen« Falls.

Fazit

Im Gesundheitswesen kommen immer mehr digitale Lösungen zur Verbesserung der (intersektoralen) Versorgung zum Einsatz. Dies zeigt u.a. die Zulassung erster Digitaler Gesundheitsanwendungen. Wie das SimPat-Beispiel zeigt, kann der Datenschutz in einem Behandlungsverbund bereits rein technisch, organisatorisch und datenschutzrechtlich gelöst werden. Allerdings sind gerade die Prozesse der Zugriffssteuerung zu Fallakten und der Einwilligung oftmals nicht am Patienten orientiert und wenig benutzerfreundlich. Die Vielzahl an zu vermittelnden medizinischen und pflegerischen sowie datenschutzrechtlichen Informationen bewirkt, dass sich viele Patienten, Angehörige und z.T. auch Behandler nur ungenau mit den Inhalten einer Einwilligung auseinandersetzen, ohne diese im Detail zu verstehen. Durch die sprachlichen, kognitiven und emotionalen Kompetenzen eines demenziellen Patienten werden die Information und die Aufklärung dieser, egal ob mit oder ohne Unterstützung, nochmals erschwert. Zudem ist häufig nur schwer zu beurteilen, was der Patient tatsächlich will und ob in seinem Sinne gehandelt wird. Die S2k-Leitlinie »Einwilligung von Menschen mit Demenz in medizinischen Maßnahmen« bietet eine Vielzahl von Handlungsempfehlungen, um die Interessen der Patienten zu wahren. Dabei werden eine unterstützte Entscheidungsfindung, soweit noch möglich, sowie eine Vorsorgeverfügung zur Handlung im Interesse des Patienten ausdrücklich empfohlen. ■

Quellen

[1] Bickel H. Informationsblatt 1. Die Häufigkeit von Demenzerkrankungen (06.2020). Im Internet: https://www.deutsche-alzheimer.de/fileadmin/alz/pdf/factsheets/infoblatt1_haeufigkeit_demenzerkrankungen_dalzg.pdf; [Zugriff: 07.10.2020].
[2] Kopf D, Hewer W. Komorbide Erkrankungen bei Demenz. Z Gerontol Geriat 2015; 48: 303–304.
[3] Deuschl G, Maier W (01.2016). S3-Leitlinie Demenzen. Im Internet: https://www.awmf.org/uploads/tx_szleitlinien/038-013l_S3-Demenzen-2016-07.pdf; [Zugriff: 07.10.2020].
[4] Deutsche Gesellschaft für Gerontologie und Geriatrie, Deutsche Gesellschaft für Psychiatrie und Psychotherapie, Psychosomatik und Nervenheilkunde, Deutsche Gesellschaft für Neurologie (Hrsg.). Einwilligung von Menschen mit Demenz in medizinische Maßnahmen. Interdisziplinäre S2k-Leitlinie für die medizinische Praxis. Stuttgart: Kohlhammer; 2020.
[5] Steiner B, Zippel-Schultz B, Popa A, Hellrung N et al. CASEPLUS SimPat: An Intersectoral Web-Based Case Management System for Multimorbid Dementia Patients. J Med Syst. 2020: 44(3): 63.

Gib Cybercrime keine Chance!

Sichere Identifizierung und Vertrauensdienste für elektronische Transaktionen mit elektronischen Signaturen.

Jürgen Bosk ist Geschäftsführer des Competence Centers für die Elektronische Signatur im Gesundheitswesen e. V. (CCESigG) in Braunschweig info@ccesigg.de

- Es besteht die Gefahr, dass Cyberkriminelle Zugang zu Daten bekommen, diese entwenden oder unerkannt verändern.
- Es sollten der Zugang zu Inhalten mit geeigneten Verfahren (Verschlüsselung) verhindert und die Integrität (Veränderung) der »Datenschätze« nach dem Stand der Technik beweiskräftig nachgewiesen werden können.
- Gesetze, Verordnungen und Richtlinien (eIDAS-VO, Vertrauensdienstegesetz, IT-Sicherheitsgesetz, IT-Sicherheitsmanagement nach ISO 27001, Patientendatenschutzgesetz, BSI Branchenspezifische Sicherheitsstandards B3S etc.) nennen die notwendigen organisatorischen und technischen Maßnahmen, die in den Einrichtungen etabliert werden sollten und als kritische Infrastruktur umgesetzt werden müssen.
- Nach der Datenschutzgrundverordnung (DSGVO) werden Verstöße gegen den Datenschutz mit erheblichen finanziellen Strafen geahndet

Einleitung

Cybercrime ist keine Erfindung der Unterhaltungsindustrie. Cybercrime ist ein quantitativ und qualitativ an Bedeutung gewinnendes Kriminalitätsphänomen. Das Gesundheitswesen gilt als eines der gefährdetsten Bereiche in Sachen IT-Sicherheit. Nach dem Cyber Security Intelligence Index von IBM Security ist das Gesundheitswesen inzwischen das weltweit interessanteste Angriffsziel für Cyberkriminelle. Im Rahmen des 10. Kongresses der UN zum Thema »Prevention of Crime and the Treatment of Offender« wurde zwischen den Bereichen Cybercrime im engeren Sinne (CCieS) und im weiteren Sinne (CCiwS) unterschieden. Diese Abgrenzungen werden seitdem unter Anpassung länderspezifischer Anpassungen auf juristischer und polizeilicher Ebene herangezogen.

Neue Bedrohungsszenarien und gesetzliche Anforderungen

In der Folge drängt der Gesetzgeber darauf, dass nicht nur Kliniken, sondern auch Hersteller die IT-Sicherheit ihrer IT-Landschaften und Medizinprodukte gewährleisten. Hierbei sind der generelle Mangel an in der Thematik geschulten IT-Fachleuten und die beschränkte Verfügbarkeit finanzieller Mittel. Mit steigendem Digitalisierungsgrad entstehen neben den bisherigen Bedrohungen auch neue Szenarien und Angriffsziele. Noch vor kurzer Zeit hat man lediglich die Bedrohung durch Virenangriffe als wesentlichen Bestandteil einer Cyberbedrohung gesehen.

Aktuelle gesetzliche Anforderungen an inter- und intrasektorale Kommunikation zwischen Leistungserbringern, Kostenträgern und Patienten erfordern zunehmend elektronische Anbindungen an die digitale »Außenwelt«. Immer mehr medizinische Geräte werden in die klinischen KIS-Landschaften eingebunden. Neben den bekannten Sicherheitsrisiken können permanent neue Sicherheitslücken mit dem Ausbau der digitalen Landschaften sowie der elektronischen Datenübertragung und Archivierung sowie mit der Einführung mobiler Arbeitsplätze und von Funktions- und Serviceerweiterungen entstehen. Hinzu kommt, dass auch Cyberkriminelle generell den Wert medizinischer Daten erkannt haben.

In der Folge drängt der Gesetzgeber darauf, dass nicht nur Kliniken, sondern auch Hersteller die IT-Sicherheit ihrer IT-Landschaften und Medizinpro-

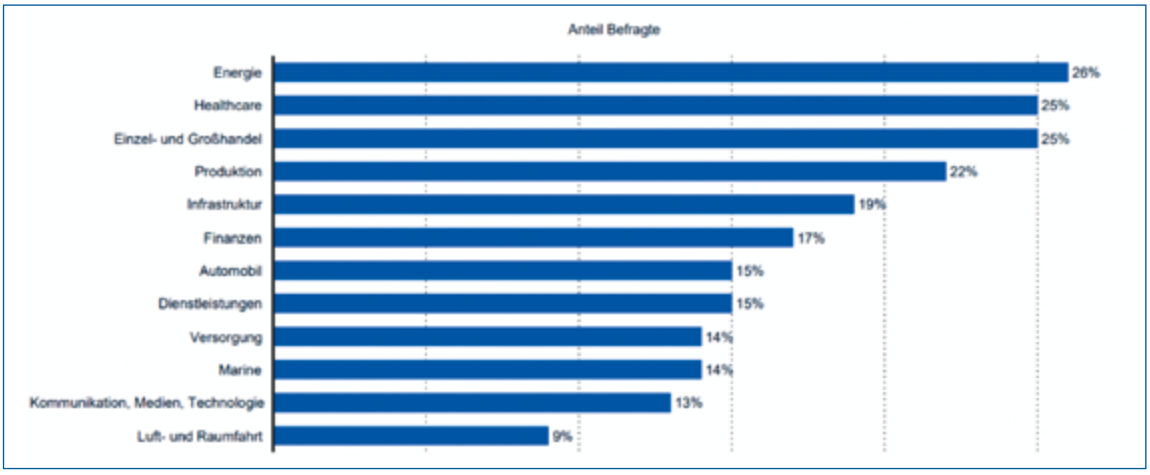


Abb. 1
Umfrage zu Cyberangriffen weltweit nach Wirtschaftszweigen im Jahr 2017 [1].

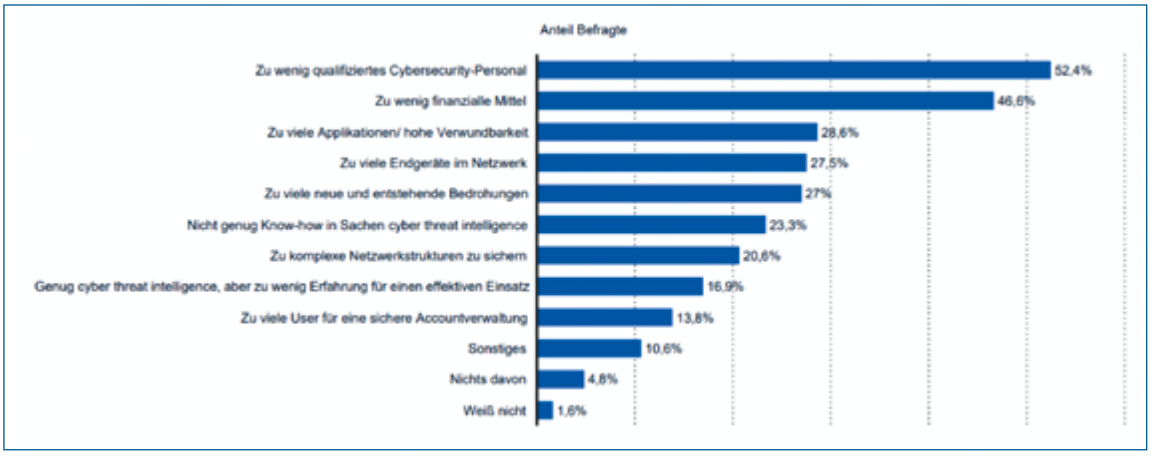


Abb. 2 Hindernisse bei der Prävention von Cyberangriffen im Gesundheitswesen [2]. Erhebungszeitraum: Dezember 2017 bis Januar 2018, weltweite Befragung, Anzahl Teilnehmer an der Befragung: 239.

dukte gewährleisten. Hierbei sind generelle Mängel an in der Thematik geschulten IT-Fachleuten und die beschränkte Verfügbarkeit finanzieller Mittel für resultierend notwendige Investitionen eine zusätzliche Herausforderung für die Kliniken. Unzureichend gewartete IT-Infrastrukturen mit veralteten und nicht gepflegten Betriebssystemen stellen in vielen Fällen ein großes Risiko dar und stehen Angriffen oft hilflos gegenüber. Nicht ohne Grund ist im Krankenhauszukunftsgesetz (KHZG) ein fester Anteil von 15 Prozent der förderfähigen Investitionen für die IT-Sicherheit vorgegeben.

Zum Computerbetrug als Cybercrime im engeren Sinne (CCieS, § 263a StGB) gehören seit dem 01.01.2016 in der Polizeilichen Kriminalstatistik (PKS) [3] z.B. verschiedene Arten des Kreditbetrugs, Überweisungsbetrug und Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel, aber auch Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB.

Cybercrime im weiteren Sinne (CCiwS) wird als sonstiger Computerbetrug gemäß § 263a Abs. 1 und 2 StGB sowie als Vorbereitungshandlungen gemäß § 263a Abs. 3 StGB sowie als missbräuchliche Nutzung von Telekommunikationsdiensten behandelt. Im Wesentlichen geht es dabei um:

- das Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen,
- Datenhehlerei (§§ 202a bis 202 d StGB),
- die Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB),
- Datenveränderung und Computersabotage (§§ 303a, 303b StGB) und
- die missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB).

Die Patientenakte im Fokus der Cyberkriminellen

Im Fokus der Cyberkriminellen stehen oftmals elektronisch archivierte Patientenakten. Diese stellen angesichts der »Haltbarkeit« ihrer Daten einen besonderen Wert und somit ein priorisiertes Ziel da. Erbeutete Zugangs- oder Anmeldedaten können leicht geändert werden oder haben ein kontrolliertes Gültigkeitsintervall. Patientenakten enthalten personenbezogene Informationen, die einen langen Gültigkeitszeitraum haben und unter Umständen, wie Geburts- und Sozialversicherungsdaten, nicht oder nur schwer geändert werden können. Mit den enthaltenen Informationen lassen sich neben dem Verkaufswert der geraubten Daten Erpressungen oder Identitätsdiebstähle realisieren.

Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, sodass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten (§ 269 StGB) sowie das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (§ 303a StGB) stellen eine enormes Gefährdungspotential für elektronisch archivierte Patientenakten dar. Löschungen sowie unbemerkte oder nicht nachweislich inhaltliche Veränderungen nur einer elektronisch archivierten Patientenakte können erhebliche wirtschaftliche, rechtliche und rufschädigende Wirkung hervorrufen.

Haftungsrisiko durch die Datenschutzgrundverordnung

Mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) drohen Schadensersatzprozesse, Abmahnungen und Bußgelder. Durch Rechtsfolge droht Vorständen und Geschäftsführern betroffener Unternehmen eine persönliche Haftung mit ihrem Privatvermögen. Die DSGVO unterscheidet bei Verstößen gegen die Regelungen verschiedene Rechtsfolgen und Sanktionsmöglichkeiten, insbesondere mit Haftung und Recht auf materiellen und immateriellen Schadensersatz (Art. 82 DSGVO) sowie mit möglichen Geldbußen (Art. 83 DSGVO) bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Vorjahresumsatzes des Unternehmens. Das Risiko des Eintretens einer schuldhaft verursachten Situation sollte auf jeden Fall so weit wie möglich verringert werden. Einen hundertprozentigen Schutz gegen Cyberangriffe gibt es nicht.

Sicherer und beweiskräftiger Nachweis der Integrität und Authentizität von Daten und Dokumenten durch elektronische Zeitstempel und Signaturen (Vertrauensdienste)

Durch den Einsatz elektronischer Zeitstempel und Signaturen kann sichergestellt werden, dass Dokumente zu einem bestimmten Zeitpunkt einer Person oder Organisation vorgelegen haben und langfristig prüfbar ist, dass die Dokumente und Daten nach ihrer Erstellung bzw. Validierung oder Unterschrift nicht mehr verändert wurden. Im Verständnis einer revisionssicheren Archivierung ist es erforderlich, die Gültigkeit elektronischer Sicherungen wie Zeitstempel und Signaturen durch geeignete Revisionsverfahren aufrechtzuerhalten.

Zur Sicherung der Beweiskraft der elektronischen Dokumentation sind gesicherte elektronische Dokumentationsprozesse erforderlich, welche die Vertraulichkeit und Verfügbarkeit der Daten über den gesamten Archivierungszeitraum sicherstellen. Hierfür sollten elektronische Zeitstempel und Signaturen verwendet werden, die die Integrität und Authentizität der archivierten Dokumente sicherzustellen.

Digitale Zeitstempel bieten den Nachweis, dass ein elektronisches Dokument zu der angegebenen Zeit dem Erzeuger des Zeitstempels vorgelegen hat. Somit kann ein Erstellungsdatum oder ein fristgerechter Eingang mit bestätigter Integrität des Dokuments beweiskräftig nachgewiesen werden.

Eine Elektronische Signatur ist das Pendant zur eigenhändigen Unterschrift. Eine Elektronische Signatur gibt Auskunft über die Identität des Erstellers oder den Urheber und belegt damit die Authentizität eines Dokuments. Darüber hinaus kann der Originalzustand des Dokuments, seine Integrität, zweifelsfrei nachgewiesen werden.

Rechtssicherheit aufgrund europaweiter einheitlicher Regelungen durch die Verordnung über elektronische Identifizierung und Vertrauensdienste

Seit dem 1. Juli 2016 gilt in allen EU-Mitgliedstaaten die »Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt« (eIDAS-VO). Die eIDAS-Verordnung ersetzt im Wesentlichen das deutsche Signaturgesetz (SigG) und die deutsche Signaturverordnung (SigVo). Ziel der eIDAS-Verordnung ist, einheitliche europäische Regelungen für elektronische Signaturen, Siegel und Zeitstempel zu schaffen und einen einheitlichen Umgang mit diesen Vertrauensdiensten zu bieten. Dabei wird die Differenzierung zwischen einfachen, fortgeschrittenen und qualifizierten Signaturen im Wesentlichen beibehalten. Neu sind elektronische Siegel und Fernsignaturen [5]. Damit sind qualifizierte Signaturen nicht mehr personengebunden, und elektronische Zertifikate müssen nicht mehr auf einer Signaturkarte gespeichert werden. Unternehmen können sich nun elektronisch adäquat zum konventionellen Siegel ausweisen, und qualifizierte Unterschriftszertifikate können von zugelassenen Vertrauensdiensteanbietern online zugänglich gemacht werden.

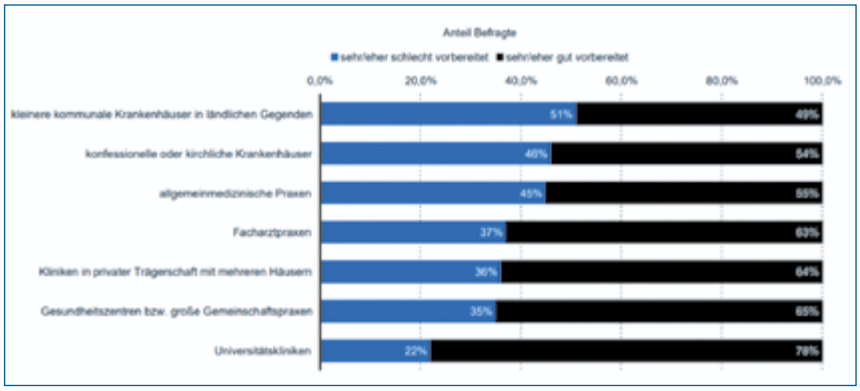


Abb. 3: Inwieweit sind Kliniken und Praxen auf Cyberangriffe vorbereitet? Erhebungszeitraum: November bis Dezember 2018, Region Deutschland, Anzahl der Befragten 1.000, Erheber PwC. [4]

Zur Umsetzung der eIDAS-VO in deutsches Recht und zur Regelung der Zuständigkeiten und Befugnisse wie der Bundesnetzagentur (BNetzA) oder des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde das Durchführungsgesetz verabschiedet. Kernstück ist das neue Vertrauensdienstegesetz (VDG). Dieses löst das bisherige deutsche Signaturgesetz (SigG) ab und ist in Ergänzung der eIDAS-VO geltendes deutsches Recht für elektronische Signaturen, Siegel und Zeitstempel.

Um bei einer elektronischen Übermittlung die übertragenen Daten und Dokumente vor Veränderung, Verlust oder Diebstahl zu schützen und eine Übertragung nachweislich zu machen, wurden Dienste wie »elektronische Einschreiben« gemäß Artikel 3 Nr. 36 der eIDAS-VO eingeführt. Diese Dienste gelten nach Artikel 44 der eIDAS-VO als qualifizierte Dienste, wenn sie von einem qualifizierten Vertrauensdiensteanbieter geleistet werden, durch welchen die eindeutige Identifizierung des Absenders und des Empfängers sichergestellt und darüber hin-

Abkürzungen

BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
B3S	Branchenspezifischer Sicherheitsstandard
CCiwS	Cybercrime im weiteren Sinne
CCieS	Cybercrime im engeren Sinne
DKG	Deutsche Krankenhausgesellschaft
DSGVO	Datenschutz-Grundverordnung
eIDAS-VO	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
ISMS	Informations-Sicherheits-Management-System
KHZG	Krankenhauszukunftsgesetz
KIS	Krankenhausinformationssysteme
PKS	Polizeiliche Kriminalstatistik
KRITIS	Kritische Infrastruktur
SigG	Signaturgesetz
SigVO	Signaturverordnung
StGB	Strafgesetzbuch
VDG	Vertrauensdienstegesetz

aus die Kommunikation (Versand/Empfang) durch eine qualifizierte Signatur oder einen qualifizierten Siegel gesichert ist. Damit ist die Möglichkeit einer unbemerkten Veränderung ausgeschlossen. Die enthaltenen qualifizierten Zeitstempel ermöglichen den Nachweis von Datum und Zeit der Versendung und des Empfangs.

Qualifizierte Zertifikate für die Onlineauthentifizierung gemäß Artikel 3 Nr. 39 der eIDAS-VO sollen eine sichere Authentifizierung von Personen ermöglichen und identitätsbasierenden Betrug im Internet erschweren. Diese Identitätsdienste müssen von einem qualifizierten Vertrauensdiensteanbieter ausgestellt sein. Die notwendigen personenbezogenen, vertrauenswürdigen Mindestangaben (gemäß Artikel 3 Nr. 39, Anhang IV) sind durch fortgeschrittene Signaturen oder Siegel zu schützen.

Anforderungen an die Versorgungssicherheit

Krankenhäuser, die zur »Kritischen Infrastruktur« (KRITIS) zählen (vollstationäre Fallzahl größer als 30.000 pro Jahr), müssen sich gemäß IT-Sicherheitsgesetz gegen Cyberattacken und Systemausfälle besonders schützen. Doch auch für kleinere Häuser empfiehlt sich die Beachtung dieser Vorgaben für mehr Versorgungssicherheit.

Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V. (KH-IT) probte zusammen mit dem Landeskriminalamt Baden-Württemberg am 07. November 2019 den Ernstfall. Ein Krankenhaus war das Ziel eines fiktiven Cybercrimeangriffs. Es wurde mit der Verschlüsselung der Patientenakten gedroht. Durch ein mangelhaftes Informations-Sicherheits-Management haben die Verantwortlichen im Krankenhaus die Erpressermail zu spät zur Kenntnis bekommen und versäumten es, die geforderte Summe in digitaler Währung zu überweisen. Die in der Realität zu erwartenden Folgen wären dramatisch gewesen [6].

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) empfiehlt, ein nachvollziehbares, zertifizierbares Informations-Sicherheits-Management-System (ISMS) einzuführen. Ziel ist, das Schutzniveau für Unternehmen, Verwaltungen und Organisationen zu erhöhen. Die Deutsche Krankenhausgesellschaft (DKG) hat dem Bundesamt für Sicherheit in der Informationstechnik (BSI) am 2. April 2019 eine erste Version für den »Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus« vorgelegt. Damit setzt die DKG das IT-Sicherheitsgesetz aus dem Jahr 2015 um, das allgemeine Anforderungen formuliert und KRITIS-Betreibern und deren Branchenverbänden auferlegt, branchenspezifische Sicherheitsstandards (B3S) zu erarbeiten. Der Standard B3S beschreibt über 160 Maßnahmen, die nötig sind, um eine gesicherte Informationstechnik nach dem Stand der Technik zu gewährleisten.

Der B3S-Standard betrifft nicht nur den Schutz der technischen Infrastruktur. Neben den vier klassischen Schutzzielen des Informationssicherheits-Managements (Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit) werden auch Patientensicherheit und Behandlungseffektivität als wesentliche Aspekte definiert. Der Standard zielt darauf, die medizinische Versorgung der Patienten zu gewährleisten. Eine sichere, zuverlässige Informationstechnik ist dafür essentielle Voraussetzung. Neben technischen Aspekten sind organisatorische, strukturelle und prozessuale Verantwortung auf Führungsebene zu berücksichtigen.

Fazit

Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit sind die Basis einer gesicherten Digitalstrategie und Datenkompetenz. Eine gelebte revisionssichere Archivierung bildet die Grundlage für Verfügbarkeit und Vertraulichkeit. Qualifizierte Zeitstempel und Signaturen garantieren die Integrität und Authentizität der Daten und Dokumente im elektronischen Langzeitarchiv und sind essentiell für eine sichere und nachweisliche elektronische Kommunikation. Damit sind die Daten und Dokumente sicher gegen eine unbemerkte Veränderung durch Cyberkriminelle gewappnet. Datenobjekte, die mit einer qualifizierten Signatur verschlüsselt übertragen werden, können nur von dem richtigen Empfänger geöffnet und eingesehen werden. Der Empfänger kann sicher sein, das Dokument von dem erwarteten Versender in prüfbar unveränderter Form erhalten zu haben. Eine illegale Kenntnisnahme ist durch die mit der Signatur verbundene Verschlüsselung nach Stand der Technik nicht möglich. Qualifizierte Signaturen und Zeitstempel sichern zuverlässig die Übertragung von Daten und Dokumenten zwischen Sender und Empfänger, geben Schutz gegen unberechtigte Einsichtnahme durch anerkannte (zugelassene) Verschlüsselungsverfahren und garantieren die Möglichkeit, eine Veränderung archivierter oder kommunizierter Daten und Dokumente jederzeit feststellen und rechtskräftig beweisen zu können. ■

Quellen

[1] Microsoft, Veröffentlichung durch MMC aus MMC Cyber Handbook, April 2018, Seite 6
[2] HIMSS aus HIMSS Cybersecurity Survey, April 2018, Seite 17
[3] Bundeskriminalamt (BKA): Cybercrime Bundeslagebild 2018 und 2019, siehe https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html
[4] Umfrage zur Sicherheit vor Cyber-Angriffen von Kliniken und Praxen 2018, PwC, Januar 2019, aus Datensicherheit in Kliniken und Arztpraxen 2019, Seite 7
[5] Prof. Dr. Alexander Roßnagel in Zusammenarbeit mit dem TeleTrust Deutschland e.V.: Die eIDAS-Verordnung in der deutschen Rechtsordnung, 1. Auflage, 2016, ISBN 978-3-8487-3544-0 (Print), ISBN 978-3-8452-7877-3 (ePDF)
[6] Krankenhaus IT-Online Journal, Index > News/Newsarchiv > Übung für den Ernstfall: Cyberangriffe auf Krankenhäuser, http://www.medizinedv. de/modules/AMS/article.php?storyid=4877

Kritische Schwachstellen in medizinischen Geräten

Aktuelle Erfahrungen eines IT-Sicherheitsdienstleisters an einem Fallbeispiel

- Nach den Regularien erfolgt die Betrachtung der IT-Sicherheit hauptsächlich im Kontext der daraus resultierenden Patientenrisiken.
- Zulassungsprozesse müssen deutlich fokussierter IT-Sicherheitsanforderungen stellen.
- Jedes aktive Medizinprodukt sollte spätestens vor dem Inverkehrbringen tiefgreifend auf IT-Sicherheitsmängel untersucht werden.
- Effiziente Reaktion auf Schwachstellen in einem Medizinprodukt ist nur mit etablierten und wohldefinierten Prozessen möglich.

Die digitale Vernetzung ist in vielen Lebensbereichen bereits weit verbreitet. Auch in der Gesundheitsbranche werden rasant zunehmend immer mehr medizinische Geräte vernetzt. Die Sicherheit dieser Geräte spielt bereits jetzt eine große Rolle, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Bericht zur Lage der IT-Sicherheit in Deutschland 2018 sowie 2019 anhand der stetig steigenden Produktpalette an smarten Medizingeräten aufzeigt [1]. Dies wird laut BSI durch die steigende Anzahl an Angriffen auf diese Geräte mit potentiellen Bedrohungen für die Patientensicherheit deutlich unterstrichen.

Laut BSI muss ein Kompromiss zwischen medizinischer Funktionalität und Maßnahmen zur Stärkung der IT-Sicherheit gefunden werden, um eine reibungslose Verwendung der Medizingeräte im Alltag sicherstellen zu können [1]. Zudem müssen Hersteller die IT-Sicherheit bei der Entwicklung und Herstellung von Medizinprodukten von Anfang an berücksichtigen.

Schwachstellen in Medizinprodukten

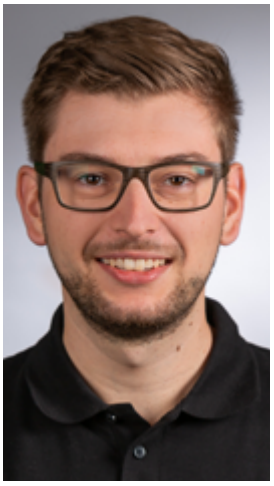
In der Vergangenheit gab es mehrere Veröffentlichungen zur IT-Sicherheit von Medizinprodukten. Zum Beispiel berichteten Billy Rios und Jonathan Butts in ihrem Vortrag »Understanding and Exploiting Implanted Medical Devices« über kritische Schwachstellen in implantierten medizinischen Geräten [2]. Das ERNW White Paper 66 fasst den Stand der Sicherheit von Medizinprodukten auf der Grundlage öffentlich verfügbarer Informationen zusammen [3]. Darüber hinaus haben von ERNW durchgeführte Untersuchungen an Patientenmonitoren, Spritzenpumpen, Elektroenzephalographiesystemen, Heimüberwachungsgeräten und einem Magnetresonanztomographen gezeigt, dass die analysierten Geräte von mehreren teils kritischen Schwachstellen betroffen waren [4,5].

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) veröffentlicht eine Liste von Meldungen zu IT-Sicherheitsproblemen in Medizinprodukten [6]. Hier muss im Blick behalten werden, dass Meldungen an das BfArM nur erfolgen, wenn ein Einfluss der Schwachstellen auf die Patientensicherheit nicht ausgeschlossen werden kann.

Derzeit gibt es keine systematische Studie, die die Prävalenz und Kritikalität von Schwachstellen in aktiven Medizinprodukten feststellt und bewertet, da Zugang zu einer Vielzahl von unterschiedlichsten Geräten nur sehr selten gegeben und eine Prüfung in Produktivumgebungen riskant ist. Daher liegen nur wenige Daten über die Wirksamkeit regulatorischer Maßnahmen zur Verhinderung solcher Schwachstellen vor, beispielsweise wenn ein Medizinprodukt Zugang zum deutschen Markt erhält. Das BSI-Projekt »Manipulation von Medizinprodukten (ManiMed)« ist das erste Projekt, das die allgemeine IT-Sicherheitslage vernetzter Medizinprodukte bewertet. Hierbei wird die IT-Sicherheitslage anhand von Penetrationstests erfasst, die für eine Auswahl vernetzter medizinischer Geräte auf dem deutschen Markt aus fünf verschiedenen Gerätekategorien durchgeführt wurden.

Rahmen für die Sicherheit von medizinischen Geräten

Die Sicherheit und Leistungsfähigkeit der in Deutschland verwendeten Medizinprodukte sind durch aufeinander abgestimmte Gesetze und Verordnungen reglementiert. Als Rahmen sind hier das Medizinproduktegesetz (MPG) sowie die europäischen Richtlinien über aktive Implantate (90/385/EWG), über Medizinprodukte (93/42/EWG) und In-vitro-Diagnostika (98/79/EG) zu nennen. Die Entwicklung des Medizinprodukts wird von einem komplexen Prozess begleitet, der neben Anforderungen an die Patientensicherheit eine obligatorische Risikoanalyse vorschreibt. Diese Risikoanalyse muss den Nutzen des Produkts mögliche Risiken gegenüberstellen. Der Nachweis der Sicherheit und der therapeutischen oder diagnostischen Leistungsfähigkeit wird für ein Medizinprodukt in einem Konformitätsbewertungsverfahren nachgewiesen. Hier ist es besonders wichtig, darauf hinzuweisen, dass der Begriff Sicherheit in der deutschen Sprache missverständlich ist und in der Regel Patientensicherheit (vgl. Englisch: Safety) und nur untergeordnet IT-Sicherheit (vgl. Englisch: Security) reflektiert. IT-Sicherheit wird durch die Bewertungsverfahren nach MPG [7] beziehungsweise der Verordnung (EU) 2017/745 über Medizinprodukte (MDR) [8] hauptsächlich im Kontext der daraus resul-



M.Sc. Julian Suleder ist Security Analyst & Researcher bei der ERNW Research GmbH und studierte Medizinische Informatik in Heidelberg/Heilbronn.
jsuleder@ernw.de

M.Sc. Florian Grunow studierte Medizinische Informatik in Mannheim und ist Geschäftsführer der ERNW Enno Rey Netzwerke GmbH.
fgrunow@ernw.de

tierenden Patientenrisiken beurteilt. Konkrete Risiken durch Schwachstellen, die keine konkrete Bedrohung der Patientensicherheit begründen, werden von diesem Rechtsrahmen nicht explizit behandelt. Verweise auf konkrete Anforderungen an die IT-Sicherheit finden sich in diesen Gesetzen und Verordnungen ebenfalls nicht.

Vorgehen bei der Kenntnisnahme von Schwachstellen

Änderungen an Medizinprodukten, die die IT-Sicherheit betreffen, erfolgen häufig im Kontext des Behebens von identifizierten Schwachstellen, wie z.B. Meldungen durch das ICS-CERT der CISA in den USA [12] zeigen. Grundsätzlich werden nicht alle identifizierten Schwachstellen behoben, sondern nahezu immer eine Restrisikoanalyse oder Aufwandsabschätzung durchgeführt, um eine Priorisierung der Schwachstellen vorzunehmen und einen Teil mitsamt deren Risiken zu akzeptieren, da die Kritikalität zu gering oder der Aufwand einer Behebung z.B. durch Veränderung des Systemdesigns zu groß ist.

Schwachstellen können auch bei einem vermeintlich sicheren System nie vollumfänglich ausgeschlossen werden. Daher ist besonders der professionelle Umgang mit Schwachstellen ein wichtiger Bestandteil des Produktlebenszyklus. Werden Schwachstellen durch externe Parteien gemeldet, wird meist ein Coordinated Vulnerability Disclosure (CVD) durchlaufen. Ein CVD kann durch einen Hersteller eines Medizinprodukts nur mit etablierten und wohldefinierten Prozessen erfolgreich durchgeführt werden. Diese Prozesse müssen nachvollziehbar und transparent im Unternehmen etabliert sein, bevor Schwachstellen gemeldet werden, damit eine Behebung zeitnah erfolgen kann. Zudem sollte jeder Hersteller eines aktiven Medizinprodukts einen öffentlichen Kontakt für das Melden von Sicherheitslücken angeben, um möglichst reibungslose CVD-Prozesse zu ermöglichen. In der IT-Branche haben sich hierzu Zeiträume von bis zu 90 Tagen ab Kenntnisnahme bis zur Veröffentlichung der Schwachstellen etabliert. Für Medizinprodukte gibt es in Deutschland aus regulatorischer Sicht keine Frist oder einen Zeitraum, der für Disclosures eingehalten werden muss, sofern die Schwachstellen keinen Einfluss auf die Patientensicherheit haben.

Abkürzungen

LE	Bluetooth Low Energy
BSI	Bundesamt für Sicherheit in der Informationstechnik
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
CISA	Certified Information Systems Auditor
CVD	Coordinated Vulnerability Disclosure
ERNW	ERNW Research GmbH
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
ManiMed	Manipulation von Medizinprodukten
MDR	Medical Device Regulation
MPG	Medizinprodukte-gesetz
PIN	Persönliche Identifikationsnummer

Fallbeispiel: DANA Diabecare RS Insulinpumpe

Im Rahmen des ManiMed-Projekts des Bundesamts für Informationssicherheit (BSI) wurden schwerwiegende Schwachstellen bei der Untersuchung der in Deutschland verfügbaren DANA Diabecare RS Insulinpumpe des koreanischen Herstellers SOOIL Developments Ltd. festgestellt [9]. Die Schwachstellen wurden durch den Hersteller behoben, dabei wurde ein Coordinated Vulnerability Disclosure (CVD) durchlaufen. Ein CVD ist der Prozess der Analyse und Validierung der Meldung von Schwachstellen, der Entwicklung von Updates, der Validierung der Eigenschaften des Medizinprodukts sowie des Ausrollens des Updates.

Die Insulinpumpe wird von Patienten zur Verabreichung von Insulin bei der Behandlung von Diabetes mellitus (Typ-1-Diabetes) verwendet und stellt eine weniger invasive und deutlich flexiblere Alternative zu mehreren täglichen Insulininjektionen dar. Die DANA Diabecare RS Insulinpumpe ist die zentrale Komponente des Therapiesystems und kann neben den Eingabemöglichkeiten am Gerät selbst mit mobilen Apps des Herstellers über ein proprietäres Kommunikationsprotokoll auf Basis einer Bluetooth Low Energy (BLE) – Schnittstelle gesteuert werden.

Schwachstellen im proprietären Kommunikationsprotokoll

Die schwerwiegenden Schwachstellen betreffen das proprietäre Kommunikationsprotokoll zwischen der Insulinpumpe und den zugehörigen mobilen Applikationen. Während der Sicherheitsüberprüfung konnte festgestellt werden, dass ein Teil der Sicherheitsfunktionalitäten alleinig in den mobilen Anwendungen implementiert und entsprechende Prüfungen nicht durch die Insulinpumpe selbst vorgenommen werden [9]. Als Beispiel kann hier angeführt werden, dass Nutzer zur Sperrung des Bedienfelds der Insulinpumpe eine persönliche Identifikationsnummer (PIN) wählen. Diese PIN ist ebenfalls für die Nutzung der mobilen Anwendungen notwendig, bevor eine Steuerung der Insulinpumpe erfolgen kann. Diese PIN wird hierbei nur durch die mobilen Anwendungen und nicht durch die Insulinpumpe selbst geprüft. Ein Angreifer ohne Kenntnis der PIN, der direkt mit der Insulinpumpe und ohne Verwendung der Anwendung interagiert, kann die Überprüfung folglich unterlassen. Dazugehörig folgt, dass die mobile Applikation Kenntnis der korrekten PIN haben muss, um eine Prüfung durchführen zu können. Die PIN wird während jedem Kommunikationsaufbau zwischen Insulinpumpe und mobiler Applikation ausgetauscht. Als Konsequenz können nicht authentifizierte Angreifer die PIN via Bluetooth Low Energy (BLE) auslesen [9].

Die Kommunikation der mobilen Applikationen mit der Insulinpumpe erfolgt verschlüsselt. Es konnte festgestellt werden, dass alle kryptografischen Schlüssel, die im proprietären Kommunikationsprotokoll Ver-

wendung finden, deterministisch generiert werden. Diese sind von der Hardware-Uhr der Insulinpumpe, der Seriennummer und der bereits angesprochenen PIN abhängig. Während der Sicherheitsüberprüfung gelang es, diese Zusammenhänge in konkrete Formeln zur Berechnung der PIN und aller anderen kryptografischen Schlüssel zu überführen. Ferner hängt die Authentifizierung mobiler Anwendungen nur vom Besitz eines dieser Schlüssel, des sogenannten Pairing Key, der bei der Kopplung von Insulinpumpe und mobiler Applikation ausgetauscht wird, ab. Alle kryptografischen Schlüssel inklusive Pairing Key werden nicht ausreichend geschützt und zwischen Insulinpumpe und mobilen Applikationen kommuniziert [9].

Auswirkung auf die Patientensicherheit

Die Gesamtheit und Kombination der identifizierten Schwachstellen ermöglichen es Angreifern, die DANA Diabecare RS-Insulinpumpe über Bluetooth Low Energy (BLE) zu übernehmen und fernzusteuern. Die Durchführung dieses Angriffs erfordert das Mitschneiden eines einzelnen Kommunikationsaufbaus zwischen einer Insulinpumpe und einer gekoppelten mobilen Anwendung durch einen Angreifer in entsprechender Reichweite unter Verwendung einfacher Bluetooth Low Energy (BLE) - Hardware. Anschließend kann der Angreifer alle über Bluetooth Low Energy (BLE) nutzbaren Funktionen der Insulinpumpe (z.B. erhöhte Insulingabe mit resultierendem Schock oder anderen Konsequenzen) über das proprietäre Kommunikationsprotokoll nutzen. Der Angriff ist automatisiert durchführbar [9]. Abbildung 1 zeigt die Insulinpumpe nach Durchführung des Angriffs. Das System wurde mit blauer Tinte gefüllt, welche während des Videos aus der Kanüle austritt. Das vollständige Video ist online verfügbar [10].

Eine entsprechende Dringende Sicherheitsmitteilung veröffentlichte der Verantwortliche nach § 5 MPG am 8. Mai über das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) [11]. Der Hersteller stellte ein Firmware-Update für die Insulinpumpe bereit, welches alle identifizierten Schwachstellen durch Anpassung des Kommunikationsprotokolls behebt. Das Firmware-Update kann mit Hilfe des jeweiligen lokalen Händlers auf eine DANA Diabecare RS - Insulinpumpe aufgespielt werden [11]. Zudem ist ein Update der mobilen Applikationen auf Android und iOS notwendig, um auch hier eine Kompatibilität mit dem veränderten Kommunikationsprotokoll sicherstellen zu können. Um das Risiko einer Beeinträchtigung der Patientensicherheit vorübergehend zu verringern, empfiehlt der Hersteller, die Bluetooth-Low-Energy (BLE) - Schnittstelle der Insulinpumpe durch Aktivierung des Flugmodus zu deaktivieren. Im Flugmodus könne der therapeutische Zweck der Insulinpumpe beibehalten werden, da das Gerät über die am Gerät vorhandenen Eingabemöglichkeiten genutzt werden könne und die Steuerung über mobile Anwendungen optional sei. Darüber hinaus implementiere das Gerät Funktionalitäten zur Erhaltung der Patientensicherheit wie z.B. eine

Abb. 1: Abgabe von Insulin durch einen Angreifer nach Übernahme und Fernsteuerung der Insulinpumpe

Quellen

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland. Siehe https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (abgerufen am 18.09.2020)
[2] Billy Rios, Jonathan Butts. Understanding and Exploiting Implanted Medical Devices. Black Hat USA 2018. Siehe https://www.blackhat.com/us-18/briefings/schedule/index.html#understanding-and-exploiting-implanted-medical-devices-11733 (abgerufen am 18.09.2020)
[3] Julian Suleder, Andreas Dewald, Florian Grunow. Medical Device Security: A Survey of the Current State. ERNW White Paper 66. 2018. Siehe https://ernw-research.de/en/whitepapers/issue-66.html (abgerufen am 18.09.2020)
[4] Süddeutsche Zeitung (SZ). Nächtliches Desaster. 2015. Siehe https://www.sueddeutsche.de/wirtschaft/medizintechnik-naechtliches-desaster-1.2534424 (abgerufen am 18.09.2020)
[5] Florian Grunow. The patient's last words: I am not a target! 2015. Siehe https://insinuator.net/2015/07/the-patients-last-words-i-am-not-a-target/ (abgerufen am 16.09.2020)
[6] Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). Cybersicherheit von Medizinprodukten. Siehe https://www.bfarm.de/DE/Medizinprodukte/RisikoerfassungUndBewertung/Cybersicherheit/kundeninfos_cybersicherheit_node.html (abgerufen am 18.09.2020)
[7] Gesetz über Medizinprodukte (MPG)
[8] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates
[9] Julian Suleder: Safety Impact of Vulnerabilities in Insulin Pumps. ERNW White Paper 69. 2020. Siehe https://ernw-research.de/en/whitepapers/issue-69.html (abgerufen am 18.09.2020)
[10] ERNW Research GmbH. Demo: Hijacking the DANA Diabecare RS Insulin Pump. Internetadresse (abgerufen am 18.09.2020): https://www.youtube.com/watch?v=0GMe2poiYtE
[11] Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM): Dringende Sicherheitsinformation zu Insulinpumpe DANA Diabecare RS und zur mobilen Anwendung AnyDANA von SOOIL Development Co. Ltd. Siehe https://www.bfarm.de/SharedDocs/Kundeninfos/DE/07/2020/17203-19_kundeninfo_de.html (abgerufen am 18.09.2020)
[12] Cybersecurity & Infrastructure Security Agency (CISA) – ICS-CERT Advisories. Siehe https://www.us-cert.gov/ics/advisories (abgerufen am 18.09.2020):

maximale Tagesdosis. Nach Angaben des Herstellers ist kein Vorkommnis der Ausnutzung der Schwachstellen außerhalb des Projekt-Prüflabors in Heidelberg bekannt [11].

Die Übermittlung und Analyse der Schwachstellen, die Evaluierung und Implementierung der Maßnahmen, die Evaluation der Wirksamkeit der umgesetzten Sicherheitsmaßnahmen, die Koordination des Ausrollens einer aktualisierten Firmware sowie entsprechende regulatorische Prozesse nahmen unter dauerhafter und vertrauensvoller Mitwirkung des Herstellers insgesamt über ein Jahr in Anspruch [9].

Ein Weg zu sichereren medizinischen Geräten

Erfahrungen aus vergangenen Sicherheitsuntersuchungen zeigen, dass die IT-Sicherheitslage zwischen verschiedenen Herstellern erheblich variiert und stark von ihrer Reife in diesem Bereich abhängt. Daher stellt sich die Frage, wie die Reife und damit die IT-Sicherheitslage der verschiedenen Anbieter auf ein gleich hohes Niveau angehoben werden können. Dies hängt zum einen vom rechtlichen Rahmen ab, der die Anforderungen definiert, auf deren Grundlage Medizinprodukte für den Markt zugelassen werden. Auf der anderen Seite ist dies von der Motivation des Anbieters selbst abhängig, sich mit IT-Sicherheitsthemen zu befassen, einen sicheren Entwicklungslebenszyklus für seine Medizinprodukte sowie eine zeitnahe und effektive Reaktion auf offenbarte Schwachstellen zu implementieren.

Nicht selten entstehen Sicherheitslücken durch Diskrepanzen vom spezifizierten und realen Verhalten eines soziotechnischen Systems. Diese Diskrepanz kann mit rein auditiver Methodik von Spezifikations- und Zulassungsdokumenten nicht identifiziert werden. Ein bewährtes Mittel hingegen sind externe Penetrationstests, in welchen ein komplexes, aktives Medizinprodukt möglichst vor einer produktiven Verwendung sicherheitstechnisch tiefgreifend untersucht wird. Abhängig von der Gerätefunktionalität werden hier externe medizinische als auch nicht medizinische, drahtlose wie auch kabelgebundene Netzwerkschnittstellen, Bluetooth- und USB-Schnittstellen, sowie Update-, Wartungs- und Konfigurationsmechanismen auf Schwachstellen untersucht und vorhandene Sicherheitsmaßnahmen auf Wirksamkeit geprüft.

Wie das Beispiel der DANA Diabecare RS - Insulinpumpe zeigt, ist eine Untersuchung des Komplettsystems an Stelle von einzelnen Anwendungen zu bevorzugen, um Annahmen an die Umgebung und Vertrauensverhältnisse zu Schnittstellen zwischen Komponenten ebenfalls zu untersuchen. Eine Diskrepanz in den Annahmen zu deren letztlicher Umsetzung kann zu schwerwiegenden Sicherheitsproblemen führen. ■

Neuerung der Datenschutzgrundverordnung für die medizinische Forschung

im Allgemeinen sowie die Bedeutung der Datenschutz-Folgenabschätzung im Speziellen

- Überblick über die neuen Regeln für die medizinische Forschung unter der Datenschutzgrundverordnung
- Alles übersichtlich und in einem Dokument-Datenschutz-Folgenabschätzung und Datenschutzkonzept
- Der Datentreuhänder – ein zentrales Instrument zur Sicherung der Gewährleistungsziele in der Datenschutz-Folgenabschätzung

Dr. rer. nat. Knut Kaulke ist Biologe und wissenschaftlicher Mitarbeiter im Bereich Datenschutz, IT und Qualitätsmanagement der Geschäftsstelle der TMF.
Knut.Kaulke@tmf-ev.de

Irene Schlünder
Irene Schlünder ist Juristin und Referentin für Recht und Bioethik bei der TMF.
Irene.Schluender@tmf-ev.de

Neuerung der DS-GVO für die medizinische Forschung im Allgemeinen

Nach anfänglicher Aufregung setzt sich immer mehr die Erkenntnis durch, dass die Datenschutzgrundverordnung (DS-GVO) doch wesentlicher weniger Umwälzungen gebracht hat als zunächst angenommen. Zwar gibt es sicherlich umfangreichere Informationspflichten gegenüber den Probanden, z.B. eine Stärkung der Rechte auf Einsicht, Kopie und Korrektur, aber bereits beim Recht auf **Portabilität**, das erstmals ausdrücklich gesetzlich verankert wurde, zeigt sich, dass manch gut gemeinter Ansatz nicht automatisch zu einer effektiven Stärkung der Betroffenenrechte führt. Denn zunächst ist durchaus unklar, welche Daten im Bereich der medizinischen Forschung als vom Datensubjekt selbst bereitgestellt gelten können oder doch eher als vom Forscher generiert anzusehen sind (z.B. Laborwerte oder genetische Daten [1]). Oft aber scheitert die Übergabe selbst bei eindeutigem Recht auf Portabilität häufig schlicht an den technischen Möglichkeiten, insbesondere an gängigen Formaten. Neu ist ebenfalls das **»Recht auf Vergessenwerden«**, aber auch hier ist unklar, welche Neuerung hiermit gegenüber dem vorher auch schon bestehenden Anspruch auf Löschung verbunden sein soll. In der medizinischen Forschung kreisen die Diskussionen jedenfalls nach wie vor eher um die Festsetzung konkreter Löschungsfristen als um ein neues Recht auf Vergessenwerden. **Keine Neuerung** gibt es trotz anders lautender Annahmen im Bereich der **Anonymisierung**: Hier ist auf die viel zu wenig rezipierten Grundsatzüberlegungen des Generalanwaltes des Europäischen Gerichtshofs (EuGH) zum Personenbezug von dynamisch vergebenen IP-Adressen zu verweisen, die ausführlich begründen, warum die Anonymität von Daten – also die Abwesenheit eines Personenbezugs – nicht absolut gegeben sein muss, sondern von den Möglichkeiten der Identifizierung auf Basis der zur Verfügung stehenden Kontextinformationen abhängt [2]. Der Wortlaut der Erwägung Nummer 26 der DS-GVO zeigt zudem sehr deutlich, dass sich die Kriterien der Bewertung von Personenbezug und Anonymität auch mit der Einführung der DS-GVO nicht geändert haben (vgl. [3, ab S. 143]). Vielmehr nimmt die Formulierung die Gedanken zur Anonymität unter der Europäischen Datenschutzrichtlinie von 1995 ausdrücklich auf.

Im Bereich der Einwilligung ist vor allem die Erleichterung der **elektronischen Einwilligung** zu nennen, die nun die »Textform« statt der »Schriftform« genügen lässt und damit endgültig den Weg frei macht für das Häkchen auf einer Seite im Internet. Es bleiben jedoch einige Fragen in zentralen Punkten offen, und zwar trotz oder gerade wegen der Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung [4], die eine enge Beschränkung der sogenannten **breiten Einwilligung** nahezulegen scheinen, was nicht dem Geist des Erwägungsgrundes Nummer 33 der DS-GVO und nicht den Erfordernissen der medizinischen Forschung in vielen Bereichen, z.B. dem Biobanking, entspricht. In Deutschland setzt sich allmählich der Konsens durch, dass beispielsweise eine Beschränkung des medizinischen Forschungszwecks auf »die Verbesserung von Diagnose, Therapie und Vorbeugung« möglich und auch ausreichend ist, soweit flankierende Maßnahmen zur Datensicherheit und Transparenz getroffen werden (siehe die Mustereinwilligungserklärung der Medizininformatik-Initiative des BMBF [5]). Auf die Einwilligungserklärungen wirken sich allerdings **die deutlich ausgeweiteten Informationspflichten** der Art. 12 bis 14 DS-GVO aus. Im Hinblick auf bisher erteilte Einwilligungen scheint sich folgender Konsens abzuzeichnen: Sie gelten fort, sofern sie der Art nach den Bedingungen der DS-GVO entsprechen (Erwägungsgrund 171, Satz 3 DS-GVO). Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen; für bereits abgeschlossene und ausgewertete Studien, deren Daten jedoch noch weiterhin gespeichert bleiben, besteht auch keine Informationspflicht gegenüber den Teilnehmern. Dies ist anders, wenn noch Daten erhoben werden. Zu ergänzende Informationen gegenüber bisher üblichen Einwilligungserklärungen sind in der Regel: Name und Kon-

Sebastian C. Semler ist Arzt und Geschäftsführer der TMF. Sebastian.Semler@tmf-ev.de

Dr. rer. nat. Johannes Drepper ist Psychologe und Leiter des Bereichs Datenschutz, IT und Qualitätsmanagement der Geschäftsstelle der TMF. Johannes.Drepper@tmf-ev.de

taktdaten der für die Datenverarbeitung verantwortlichen Stelle oder Person, die Kontaktdaten des/der zuständigen Datenschutzbeauftragten, das Bestehen eines Beschwerderechts bei einer Datenschutz-Aufsichtsbehörde, **die Rechtsgrundlage** der Verarbeitung sowie das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Die Betroffenen sind außerdem auf ihr Recht hinzuweisen, Auskunft (einschließlich unentgeltlicher Überlassung einer Kopie) über die sie betreffenden personenbezogenen Daten zu erhalten sowie ggf. deren Berichtigung oder Löschung zu verlangen.

Teilweise geklärt wurde inzwischen die Rechtsgrundlage bei klinischen Studien nach dem Arzneimittelgesetz (AMG): Hier ist im Regelfall für die eigentliche Studiendurchführung nicht die Einwilligung der Probanden die Grundlage der Datenverarbeitung, sondern die entsprechende gesetzliche Verpflichtung nach AMG [6,7]. Offen bleibt dabei aber, welche Rechtsgrundlage die Nachnutzung der Daten nach Studienende (Sekundärnutzung) erlauben kann und ob hierfür eine Zweckvereinbarkeit nach Art. 5 (1) b DS-GVO angenommen werden kann. Aufgrund dieser Unsicherheit und mangels spezieller gesetzlicher Regelung – eine solche gibt es beispielsweise in Frankreich oder der Schweiz – wird eine solche Nachnutzung in Deutschland weiterhin eine Einwilligung mit entsprechend breiter Zweckbeschreibung voraussetzen.

Eine neuere Diskussion betrifft die Frage, ob an die **Pseudonymisierung** strengere Anforderungen unter der DS-GVO zu stellen sind. Der Wortlaut legt zunächst nahe, dass die Daten, in denen die direkt einer Person zuordenbaren Daten durch ein Pseudonym ersetzt wurden, nur dann als pseudonym gelten können, wenn sie ein Deidentifikationsniveau aufweisen, das anonymen Daten entspricht. In diesem Sinne wurde Pseudonymisierung unter dem alten BDSG allerdings nie verstanden und das aus gutem Grund. Denn die Pseudonymisierung von Forschungsdaten diente von Anfang an als Sicherheitsmaßnahme bei der Nutzung von Daten auf der Basis einer Erlaubnis, meist einer Einwilligung der Probanden. Die Anonymisierung dagegen befreit vom Vorliegen einer Rechtsgrundlage für die weitere Datennutzung. Dies hat sich grundsätzlich auch unter der DS-GVO nicht geändert, daher war die Lesart der Definition der Pseudonymisierung in Artikel 4 DS-GVO zunächst keine andere. Inzwischen wird allerdings unter Bezugnahme auf den Wortlaut manchmal auch ein höheres Deidentifikationsniveau und damit eine stärkere Vergröberung pseudonymer Daten verlangt. Im Auftrag der TMF hat Roßnagel hierzu die Literatur gesichtet und analysiert. Er kommt allerdings zu dem Schluss, dass sich die Bedeutung des Pseudonymisierungsbegriffs bei Berücksichtigung aller relevanten Textstellen der DS-GVO gegenüber der früheren europäischen Richtlinie und dem alten BDSG nicht geändert hat [3, S. 174 ff.]. Dennoch wird man mit dem Begriff Pseudonymisierung in Einwilligungserklärungen derzeit vorsichtig umzugehen haben. Richtig und wichtig bleibt zudem der Hinweis, dass deidentifizierte Daten auch bei Löschung des Schlüssels nicht automatisch zu anonymisierten Daten werden. Vielmehr ist die Anonymität regelmäßig gesondert festzustellen. Die Einschaltung von Treuhandstellen zur Verwaltung der identifizierenden Daten und der Einwilligungserklärungen bleibt vor allem in der akademischen Forschung in Deutschland ein Fixpunkt, während sie im übrigen Ausland nicht überall zum gängigen Repertoire von Schutzmaßnahmen gehört.

Die Regelungen zur Verantwortlichkeit für die Datenverarbeitung sind ebenfalls im Grundsatz gleich geblieben: Es gibt die Rollen als allein Verantwortlicher, gemeinsam Verantwortlicher und als Datenverarbeiter im Auftrag. Verschoben haben sich aber Regelungen im Bereich der Haftung: Der Auftragsverarbeiter hat eine eigene Verantwortlichkeit erhalten, und für die gemeinsame Verantwortlichkeit wurde ausdrücklich die gesamtschuldnerische Haftung eingeführt. Dies führt zu einer neuen Brisanz in der Bestimmung der Rollen in der Praxis. Der europäische Datenschutzausschuss erarbeitet hierzu eine Stellungnahme, die sich derzeit in einer Konsultationsphase befindet [8].

Was bleibt an wirkungsvollen Neuerungen? Da wären wohl zuerst die **deutlich verschärften Sanktionen** zu nennen. Freilich ist mit einschlägigen Erfahrungen erst in weiterer Zukunft zu rechnen, da die Kapazitäten der deutschen Aufsichtsbehörden für eine Ausweitung der Kontrollen sehr begrenzt sind. Ferner hat sich die gute Zusammenarbeit und die frühzeitige Abstimmung mit den Aufsichtsbehörden nach dem Muster der TMF als sehr hilfreich erwiesen.

Insbesondere im Rahmen einer der Kerntätigkeiten der TMF, der Beratung und Evaluierung von Datenschutzkonzepten durch die AG Datenschutz, ist oft eine Neuerung der DS-GVO einzubeziehen: die Datenschutz-Folgenabschätzung (DS-FA) gem. Art. 35 DS-GVO. Diese wird im Bereich medizinischer Forschung regelmäßig notwendig sein, zumindest dann, wenn mit sensiblen Gesundheitsdaten in größerem Umfang gearbeitet wird. Der DS-FA ist daher hier ein ausführlicherer Abschnitt gewidmet.

Die Datenschutz-Folgenabschätzung

Wenn Verarbeitungen personenbezogener Daten möglicherweise mit einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen einhergehen, müssen vor Beginn diese Risiken genau analysiert und geeignete technische und organisatorische Schutzmaßnahmen zur Eindämmung dieser Risiken festgelegt werden. Diese Analyse sowie die Festlegung geeigneter Maßnahmen und

eine abschließende Bewertung der Restrisiken sind Gegenstand eines neuen Instruments der DS-GVO: der Datenschutz-Folgenabschätzung (DS-FA) nach Art. 35 Abs. 1 DS-GVO. Eine Datenschutz-Folgenabschätzung dient somit als geeigneter Nachweis für die Einhaltung der Datenschutz-Grundverordnung durch den Verantwortlichen. Dazu gehört auch, dass sie gemäß Art. 35 Abs. 7 DS-GVO detaillierte Darstellungen der geplanten Verarbeitungsvorgänge sowie der Zwecke der Verarbeitung beinhaltet. Neben den Risiken sollten sowohl die Notwendigkeit als auch die Verhältnismäßigkeit der Verarbeitungsvorgänge evaluiert werden. Daraus ergibt sich die erforderliche Formulierung geeigneter Gegenmaßnahmen zur Minimierung der Risiken und somit zur Sicherstellung des Schutzes personenbezogener Daten.

Nach Art. 35 Abs. 3 DS-GVO ist die Durchführung einer DS-FA insbesondere dann notwendig, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO – hierzu gehören Gesundheitsdaten – geplant ist. Bei größeren medizinischen Forschungsprojekten ist also regelmäßig auch eine DS-FA durchzuführen. Abschließend gehört zur DS-FA auch eine Bewertung der verbleibenden Restrisiken für die Betroffenen. Sind diese weiterhin hoch, muss der Verantwortliche nach Art. 36 Abs. 1 DS-GVO vor der Durchführung der Verarbeitung die zuständige Aufsichtsbehörde konsultieren.

Verhältnis von Datenschutzkonzept und Datenschutz-Folgenabschätzung

Die Inhalte einer DS-FA finden sich auch zu gewissen Teilen in typischen Datenschutzkonzepten für medizinische Forschungsprojekte wieder. So werden in Datenschutzkonzepten regelmäßig Maßnahmen beschrieben, die personenbezogene Daten wirksam schützen. Ebenfalls wird an dieser Stelle über die Zwecke, die Angemessenheit und die Erforderlichkeit der Datenverarbeitung informiert und Letztere auch begründet.

Neben Gemeinsamkeiten dieser Datenschutzinstrumente sind auch inhaltliche Unterschiede feststellbar. So enthält ein Datenschutzkonzept, welches typischerweise auch als Grundlage für einen Eintrag im Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO dient, eine ausführliche Darstellung der Rechtsgrundlagen für die Datenverarbeitung. In der DS-FA spielen die Rechtsgrundlagen hingegen keine prominente Rolle. Mit der Einführung der DS-FA wird ein neuer inhaltlicher Aspekt eingeführt, der vor Inkrafttreten der DS-GVO in Datenschutzkonzepten in diesem Umfang nicht vertreten war – die Analysen von Risiken für betroffene Personen sowie die Formulierung von konkret diesen Risiken zugeordneten Gegenmaßnahmen. Eine inhaltliche Gegenüberstellung von Datenschutzkonzept und DS-FA ist in Tab. 1 dargestellt.

Inhalte	Datenschutzkonzept	Datenschutz-Folgenabschätzung
Zweck	✓	✓
Verantwortlichkeit	✓	(✓)
Rechtsgrundlage(n)	✓	✗
Prozessbeschreibung	✓	✓
Daten und Datenflüsse	✓	✓
Risiko-Analyse	✗	✓
Schutzmaßnahmen (TOMs)	✓	✓
Fristen	✓	(✓)
Abschließende Risikobewertung	✗	✓

Tab. 1: Inhaltliche Unterschiede und Gemeinsamkeiten von Datenschutzkonzept und Datenschutz-Folgenabschätzung in der medizinischen Forschung

Strategie zur Implementierung einer Datenschutz-Folgenabschätzung im Datenschutzkonzept

Die Risiko- und Schutzbedarfsanalyse der Datenverarbeitungsvorgänge für betroffene Personen sind der zentrale Bestandteil der DS-FA. Damit der Verantwortliche dieser Risiken gewahr werden kann, ist es sehr hilfreich, wenn zunächst ein Schema des Datenflusses im Projekt erstellt wird, um kritische Punkte des Datenschutzes in den Verarbeitungsvorgängen zu identifizieren und sie als Risiko zu formulieren. Hierbei können Überlegungen zu den Hintergründen der Ereignisse zielführend sein, die zu datenschutzrechtlichen Schäden bei betroffenen Personen führen. Die zentrale Orientierung bieten bei der Recherche nach Risiken die Gewährleistungsziele des Datenschutzes, die die typischen Ziele der IT-Sicherheit, Verfügbarkeit, Integrität und Vertraulichkeit, umfassen. Zu ergänzen ist aber insbesondere vor dem Hintergrund der DS-GVO noch das eigenständige Gewährleistungs-

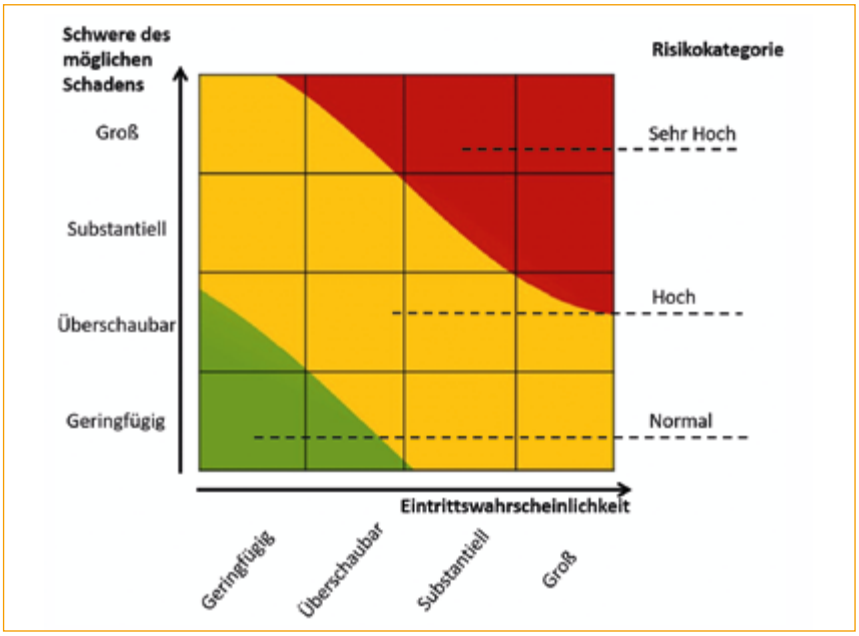


Abb. 1: Modifizierte Matrix zur Risikobewertung nach Kurzpapier Nr. 18 der Datenschutzkonferenz (DSK) und Standard-Datenschutzmodell 2.0b

Prozessschritt	Gefährdung	Bewertung	
[Prozessschrittnummer] Kurzbezeichnung Prozessschritt (Orientierung am Schema des Datenflusses)	Kurzbezeichnung Gefahr (z.B.: Widerrechtliche Weitergabe von und Einsicht unbefugter Personen in Behandlungsdaten)	Betroffene Gewährleistungsziele	Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit
		Risikoquelle/Angreifer	z.B.: interne und externe menschliche Quellen, technische Quellen
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig, überschaubar, substanziell, groß
		Schweregrad	geringfügig, überschaubar, substanziell, groß
		Risikokategorie	normal, hoch, sehr hoch
		Maßnahmen: Wird bei der Risikoanalyse ein hohes bzw. ein sehr hohes Risiko für die datenschutzrechtlich betroffene Person festgestellt (Risikokategorien hoch oder sehr hoch), müssen Maßnahmen zur Minimierung des Risikos (Risikokategorie normal) eingeleitet werden. Es erfolgt eine Kurzbeschreibung der entsprechenden Maßnahme mit Verweis auf Kapitel zu den technischen und organisatorischen Maßnahmen, dem Datenfluss und Rechtsrahmen im Datenschutzkonzept.	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig, überschaubar, substanziell, groß
		Schweregrad	geringfügig, überschaubar, substanziell, groß
		Risikokategorie	normal, hoch, sehr hoch

Tab. 2: Aufbau der Tabelle der Risiko- und Schutzbedarfsanalyse. Die Einteilungen der Eintrittswahrscheinlichkeit (geringfügig, überschaubar, substanziell, groß) und des Schweregrads (geringfügig, überschaubar, substanziell, groß) wurden dem Kurzpapier Nr. 18 der DSK entnommen. Die Risikokategorien (normal, hoch, sehr hoch) und Gewährleistungsziele entsprechen den Empfehlungen im SDM (Version 2.0b). Der Vorgang zur Risikoeinschätzung wird einmal ohne Berücksichtigung risikobezogener technischer und organisatorischer Maßnahmen und einmal mit einer entsprechenden Berücksichtigung vorgenommen, so dass eine Wirksamkeitsprüfung der Maßnahmen möglich wird.

ziel der Transparenz. Das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) beschlossene Standard-Datenschutzmodell (SDM) nennt darüber hinaus die Gewährleistungsziele der Datenminimierung, Nichtverkettung und Intervenierbarkeit [9]. Während die ersten beiden Ziele eigentlich Unterziele der Vertraulichkeit darstellen, adressiert die Intervenierbarkeit sowohl Teilziele der Transparenz (Benachrichtigung, Auskunft) als auch die Umsetzbarkeit weiterer Betroffenenrechte (z.B. Berichtigung, Löschung, Einschränkung). Die Einhaltung dieser Gewährleistungsziele gilt es mit geeigneten technischen und organisatorischen Maßnahmen zu garantieren.

Gemäß SDM sollte im Anschluss daran zur Festlegung der Höhe des Risikos eine »Schwellwert-Analyse« durchgeführt werden. Wird dabei entsprechend Art. 35 DS-GVO ein »voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen« festgestellt, müssen entsprechend nachprüfbare Maßnahmen zur Eindämmung dieses Risikos erfolgen. In diesem Zusammenhang sollte zunächst das identifizierte Risiko skalierbar transformiert werden. Dafür empfiehlt sich eine Einteilung der Risiken und der resultierenden Risikokategorien nach Eintrittswahrscheinlichkeit und Schweregrad mithilfe der Einteilungsbegrifflichkeiten des Kurzpapiers Nr. 18 der DSK bzw. nach dem SDM, wie sie in Abb. 1 dargestellt ist [10]. Dieser Vorgang zur Risikoeinschätzung wird einmal ohne Berücksichtigung risikobezogener technischer und organisatorischer Maßnahmen und einmal mit einer entsprechenden Berücksichtigung vorgenommen, so dass eine Wirksamkeitsprüfung der Maßnahmen möglich wird.

Die Auflistung der Ergebnisse der Risikoanalyse und der dazugehörigen technischen und organisatorischen Gegenmaßnahmen kann aus Gründen der Übersichtlichkeit in tabellarischer Form erfolgen. Um Redundanzen zu vermeiden bzw. die Übersichtlichkeit zu bewahren, werden die einzelnen technischen und organisatorischen Maßnahmen nicht in der Tabelle der Risiko- und Schutzbedarfsanalyse erläutert, sondern in einem gesonderten Kapitel des Datenschutzkonzepts detailliert beschrieben. Es werden lediglich gekürzte Inhalte mit Verweisen zu den entsprechenden Kapiteln formuliert. Eine Vorlage für diese Auflistung ist in Tab. 2 dargestellt. Bei der Verwendung der Tabelle ist für den jeweiligen Prozessschritt und die entsprechende Gefährdung eine Auswahl hinsichtlich der betroffenen Gewährleistungsziele und Risikoquellen sowie der Eintrittswahrscheinlichkeit, des Schweregrades und der Risikokategorie zu treffen. Wird eine DS-FA in dieser Form in ein umfassendes Datenschutzkonzept eingebettet, ist zu beachten, dass die DS-FA eine besondere gesetzlich geregelte Funktion hat. Entsprechend sollte sie klar und deutlich abgegrenzt und einfach auffindbar sein. Bei einer entsprechend transparenten Strukturierung des Datenschutzkonzepts kann eine solche Einbettung allerdings Redundanzen ersparen und zur Übersichtlichkeit und Pflegbarkeit der Dokumentation beitragen.

Einsatz eines Datentreuhänders zur Minimierung der datenschutzrechtlichen Risiken

Das Gewährleistungsziel der Vertraulichkeit ist typischerweise dann besonders gefährdet, wenn umfangreiche Gesundheitsdaten für längere Zeit und für viele verschiedene Forschungsanfragen vorgehalten werden sollen. In solchen Fällen ist dann auch regelmäßig die Durchführung einer DS-FA notwendig. Ein zentrales Instrument zur Sicherung der Gewährleistungsziele in solchen Szenarien ist die Einbindung eines möglichst unabhängigen Datentreuhänders. Im Datenschutzleitfaden der TMF wird der Datentreuhänder als Institution oder Person bezeichnet, die zum einen in spezieller Weise zwischen Forschungsdatengebern und der Nachfrageseite von Forschungsdaten agiert und zum anderen »rechtlich, räumlich und personell selbstständig und unabhängig ist« [11, S. 45-47 / 209]. Die Bundesdruckerei als Anbieter von Datentreuhänderdiensten ergänzt dazu, dass Vertrauen durch die Einbeziehung einer solchen Stelle entsteht, »wenn die Identitäten der Akteure sicher sind, die Datensouveränität erhalten bleibt und die Daten vor Manipulation und Diebstahl geschützt sind« [12]. Die Aufgaben bestehen zunächst in der Umsetzung des Prinzips der informationellen Gewaltenteilung. Diese sollte über geregelte

Zugangsberechtigungen auf verschiedenen Ebenen der Datenbestandsverwaltung gewährleistet werden. Insbesondere sollten die für die Forschung relevanten medizinischen Daten von den die Patienten oder Probanden direkt identifizierenden Daten getrennt und unabhängig voneinander verwaltet werden. Dabei spielt die elektronisch geführte und beim Datentreuhänder verortete Patientenliste, in der der Bezug der identifizierenden Patientendaten (IDAT) zu Pseudonymen (PID) hinterlegt ist, eine entscheidende Rolle. Sie kann als zentrale Einheit betrachtet werden, wo u.a. Prozessschritte zu Patienteneinwilligungen und -widerrufen (Einwilligungsmanagement) sowie zur (De-) Pseudonymisierung und Anonymisierung administriert werden. Der Zugang und die Verwaltung dieser Liste sollten unabhängig, verfahrenstransparent und vertrauenswürdig realisiert werden.

Die Verarbeitung von personenbezogenen Daten in der medizinischen Forschung erfordert im Regelfall eine zweckgebundene, informierte und auf dem freien Willen der Betroffenen basierende Einwilligung (Informed Consent, Art. 6 Abs. 1 a, Art. 9 Abs. 2 a DS-GVO). Ergänzend dazu muss jederzeit ein Widerruf der Einwilligung umsetzbar sein, so dass resultierend daraus die personenbezogenen Daten keine Weiterverarbeitung erfahren und nach Ablauf einer gesetzlichen Frist aus dem Forschungsdatensatz entfernt werden. Gemäß Art. 7 Abs. 3 DS-GVO sollte der Widerruf so einfach wie die vorher erteilte Einwilligung gestaltet werden. So wird der Verantwortliche dazu verpflichtet, passende Verfahren zur Entgegennahme und der Realisierung des Widerrufs festzulegen. Ein im Forschungsprojekt eingebundener Treuhänder kann auf Grundlage der Patientenliste z.B. notwendige widerrufsbedingte Interaktionen direkt vollziehen bzw. auslösen. Besonders bei der standortübergreifenden Analyse von medizinischen Forschungsdaten macht sich der Einsatz eines Datentreuhänders positiv bemerkbar: Durch die zentrale Verwaltung von idealerweise heutzutage elektronisch dokumentierten Patienteneinwilligungen werden diese in standardisierter Form übergreifend abfrag- und auswertbar [13,14]. Für die Erstellung einer Risiko- und Schutzbedarfsanalyse im Rahmen einer DS-FA im Format von Tab. 2 bedeutet dies, dass Gefährdungen der Gewährleistungsziele der Vertraulichkeit und Intervenierbarkeit in verschiedenen Prozessschritten mit der Einbindung von Datentreuhändern – zumindest für die getrennte Verwaltung von IDAT und MDAT und ggf. auch für ein zentrales Einwilligungsmanagement – begegnet werden kann.

Im Gegensatz zur – ggf. von einem Datentreuhänder durchgeführten bzw. unterstützten – Pseudonymisierung werden bei der Anonymisierung sämtliche Personenbezüge der Daten entfernt, so dass eine Verbindung der Daten zu einer Person technisch und inhaltlich nur noch mit höchsten Anstrengungen möglich ist [11, S. 198]. Letzteres ist aber nicht in jedem Fall einfach einzuhalten, da »eine valide Anonymisierung – je nach Art der zu anonymisierenden Daten und Kontext der Verarbeitung – eine Herausforderung für den jeweiligen Verantwortlichen bedeuten kann und nicht vorschnell von einer hinreichenden Anonymisierung ausgegangen werden darf« [15]. Weiterhin wird in einem aktuellen Positionspapier des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Anonymisierung empfohlen, dass beim Vorgang der Anonymisierung eine DS-FA gemäß Art. 35 Abs. 1 DS-GVO durchgeführt werden sollte. Dabei wird angenommen, dass ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, weil zum einen oft »neue Technologien« zum Einsatz kommen und zum anderen der Aufbau eines anonymen Daten-

Glossar

AG	Arbeitsgruppe
AMG	Gesetz über den Verkehr mit Arzneimitteln – Arzneimittelgesetz
BayLfD	Bayerischer Landesbeauftragter für den Datenschutz (www.datenschutz-bayern.de)
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (www.bfdi.bund.de)
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesministerium für Gesundheit
BMWI	Bundesministerium für Wirtschaft und Energie
CTR	Clinical Trials Regulation
DS-FA	Datenschutz-Folgenabschätzung (nach Art. 35 DS-GVO)
DS-GVO	Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (www.datenschutzkonferenz-online.de)
EDPB	European Data Protection Board (https://edpb.europa.eu)
EDSA	Europäischer Datenschutz Ausschuss
ePA	elektronische Patientenakte
EuGH	Gerichtshof der Europäischen Gemeinschaften (http://curia.europa.eu)
FDZ	Forschungsdatenzentrum
GDPR	General Data Protection Regulation
gICS	generic Informed Consent Service der Universitätsmedizin Greifswald
gnomDE	Plattform für genomische Medizin
IDAT	Identifizierende Daten (eines Patienten)
IP	Internet Protocol
MDAT	Medizinische Daten (eines Patienten)
MII	Medizininformatik-Initiative des BMBF (www.medizininformatik-initiative.de)
NAKO	ehemals Nationale Kohorte
NFDI	Nationale Forschungsdateninfrastruktur
NUM	Netzwerk der Universitätsmedizin
n.d.	no date
PDSG	Patientendatenschutzgesetz
PID	(pseudonymer) Patientenidentifikator
Privacy Shield	EU-US Privacy Shield: Von der EU-Kommission und den USA ausgehandelter Datenschutzstandard für US-Unternehmen, der gemäß Beschluss der EU-Kommission von 2016 den Datenschutzvorgaben der EU entspricht (Angemessenheitsbeschluss). Der EuGH hat diesen Beschluss 2020 für ungültig erklärt.
SDM	Standard-Datenschutzmodell, von der DSK verabschiedetes Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele
TK	Telekommunikation
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)
ToolPool	ToolPool Gesundheitsforschung, von der TMF betriebenes Web-Portal zur Bereitstellung von und Informierung zu Unterstützungsangeboten für IT-Infrastrukturen in der medizinischen Forschung (www.toolpool-gesundheitsforschung.de)

bestandes eine komplexe Aufgabe des Verantwortlichen darstellt und hierbei viele mögliche Fehlerquellen zu berücksichtigen sind. Bezüglich der Risiko- und Schutzbedarfsanalyse kann geschlussfolgert werden, dass beide Verfahren – die Pseudonymisierung und die Anonymisierung – insbesondere der Gewährleistung der Vertraulichkeit dienen. Zumindest bei der Pseudonymisierung muss aber zusätzlich beachtet werden, dass das Schutzziel der Integrität dadurch nicht außer Acht gerät.

Ausblick

In der Digitalisierungsstrategie der Bundesrepublik sind für die kommenden Jahre relevante nationale Projekte für das Gesundheitswesen verankert, welche insbesondere eine bessere Nutzung medizinischer Daten für die medizinische Forschung und die Verbesserung der Patientenversorgung adressieren. Bereits bestehende nationale Aktivitäten wie die NaKo-Gesundheitsstudie und die Medizininformatik-Initiative (MII) werden um Initiativen wie die Nationale Forschungsdateninfrastruktur (NFDI), das Netzwerk der Universitätsmedizin (NUM) zu COVID-19, das Forschungsdatenzentrum (FDZ) beim BfArM nach § 303a-e SGB V und die kommende Plattform für genomische Medizin (genomDE) [16] ergänzt und erweitert. Eine besondere Rolle wird zudem die elektronische Patientenakte (ePA) einnehmen, für die durch das jüngst verabschiedete Patientendatenschutzgesetz (PDSG) [17] gemäß § 363 SGB V eine Nutzungsmöglichkeit für die Forschung vorgesehen ist – auf zweierlei Wegen: zum einen auf dem Antragswege über das Forschungsdatenzentrum nach Ausleitung aus der ePA in das FDZ (§ 363 Abs. 1-7 SGB V), zum anderen bei Vorliegen einer eigenen Rechtsgrundlage und bei Erfüllen erforderlicher Sicherheitskriterien direkt im Kontext zum Patientenkontakt (§ 363 Abs. 8 SGB V). Gemein ist nahezu all diesen Initiativen, dass für die betreffende Datenverarbeitung von Patientendaten eine Einwilligung der Patienten als Rechtsgrundlage vorgesehen ist. Dabei werden die Herausforderungen an die Patienteneinwilligung wachsen, die erforderliche Informierung über breite Nutzungszwecke in der Nachnutzung wie über Datenverarbeitungsprozesse wird notgedrungen deutlich komplexer. Über neue Modelle der Patientenautonomie und Verfahren der Patienteneinwilligung im Rahmen einer »Datenspende« muss zwangsläufig – gemeinsam mit den Patientenvertretungen – nachgedacht werden. Zum anderen steigen die Kritikalität und die Anforderungen an IT-Sicherheit und Datenschutzmaßnahmen bei nahezu bevölkerungsweiten Plattformen. Nachvollziehbarer und technisch verlässlicher Datenschutz dient als Fundament für eine bleibende Akzeptanz in der Bevölkerung für diese neuen Infrastrukturen und für »Datenspenden« zugunsten der Forschung. Eine sichere Beherrschung der Instrumente Datenschutzkonzept und Datenschutz-Folgenabschätzung werden vor diesem Hintergrund notwendiger denn je. ■

Hinweis:
Datentreuhänder sowie Werkzeuge zur Umsetzung des Einwilligungs- und Widerrufsrechts, der Pseudonymisierung und Anonymisierung in der medizinischen Forschung sind im TMF-Portal »ToolPool Gesundheitsforschung« gelistet und beschrieben (https://www.toolpool-gesundheitsforschung.de/).

Quellen

[1] Artikel-29-WP. Guidelines on the right to data portability. Adopted on 13 December 2016. As last Revised and adopted on 5 April 2017. Brussels: Article 29 Data Protection Working Party; 2017.
[2] EuGH. Schlussanträge des Generalanwalts Manuel Compos Sánchez-Bordona in der Rechtssache C-582/14, Patrick Breyer gegen Bundesrepublik Deutschland. Europäischer Gerichtshof; 2016.
[3] Dierks C, Roßnagel A. Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen. Vol. 1. Berlin: MWV; 2019.
[4] EDPB. Guidelines 05/2020 on consent under Regulation 2016/679. Brussels: European Data Protection Board; 2020.
[5] Mustereinwilligungserklärung der Medizininformatik-Initiative des BMBF n.d. https://www.medizininformatik-initiative.de/de/mustertext-zur-patienteneinwilligung (accessed October 13, 2020).
[6] EDPB. Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)). Brussels: European Data Protection Board; 2019.
[7] Bischoff C, Wiencke J. Datenschutzrechtliche Voraussetzungen klinischer Prüfungen. Das Verhältnis von AMG und DS-GVO. ZD 2019;2019:8–13.
[8] Guidelines 07/2020 n.d. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en (accessed October 13, 2020).
[9] DSK. Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder; 2019.
[10] DSK. Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkonferenz (DSK); 2018.
[11] Pommerening K, Drepper J, Helbing K, Ganslandt T. Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0. Vol. 11. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft; 2014.
[12] Der Datentreuhänder n.d. https://www.bundesdruckerei.de/system/files/dokumente/pdf/BDR.de_Datentreuhaender.pdf (accessed October 12, 2020).
[13] Rau H, Geidel L, Bialke M, Blumentritt A, Langanke M, Liedtke W et al. The generic Informed Consent Service gICS®: implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research. J Transl Med 2020;18. https://doi.org/10.1186/s12967-020-02457-y.
[14] Bialke M, Penndorf P, Wegner T, Bahls T, Havemann C, Piegsa J et al. A workflow-driven approach to integrate generic software modules in a Trusted Third Party. J Transl Med 2015;13. https://doi.org/10.1186/s12967-015-0545-6.
[15] BfDI. Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche. Bonn: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit; 2020.
[16] Daten helfen heilen – Innovationsinitiative »Daten für Gesundheit«: Roadmap für eine bessere Patientenversorgung durch Gesundheitsforschung und Digitalisierung. BMBF, BMG, BMWi, 2020 n.d. https://www.bmbf.de/upload_filestore/pub/Daten_helfen_heilen.pdf (accessed October 15, 2020).
[17] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG), Bundesrat Drucksache 470/20, 2020. n.d.

Köpfe im BVMI
Priv.-Doz. Dr. Günter Steyer

Berufliches Tätigkeitsfeld
Seit 2006 Inhaber von eHealth Consulting und Berater für Digitalisierung, IT-Strategie, Planung und Einführung von KIS und Subsystemen, Systemintegration, Standards, Interoperabilität sowie Gesundheitstelematik; 2010 bis 2019 Lehrbeauftragter an der Hochschule für Wirtschaft und Recht (HWR) in Berlin, 2012 HWR-Gastaufenthalt am Universitätsklinikum Shengjing/China

Beruflicher Werdegang
Studium der Kerntechnik und Chemie an der TU Dresden; 1970 Promotion zum Dr. rer. nat. und Wechsel ans Universitätsklinikum Dresden; seitdem auf dem Gebiet der Healthcare IT-Anwendung tätig: Themenleiter für Laborsysteme, Institutsleiter für Medizinische Informatik, Produktmanager für klinische Informationssysteme (SOKRATES, MEDIK, i.s.h.med); 1997 bis 2006 »Director Healthcare CE« bei SeeBeyond (jetzt zu Oracle)

Weiterbildungen
1981 Fachanerkennung »Medizinische Informatik und Biomathematik«, 1982 Habilitation in Medizinischer Informatik, 1987 Lehrbefähigung an der Humboldt-Universität zu Berlin, 1991 Facultas docenti an der Universität Rostock

BVMI-Mitgliedschaft
Mitglied seit 1990, 1991 bis 2007 Vorsitzender der Landesvertretung Berlin/Brandenburg, 2003 bis 2004 Vizepräsident, 2004 bis 2007 BVMI-Präsident. Seit 2008 Ehrenmitglied, 2003 bis 2018 mdi-Redaktions-Mitglied, 2008 bis 2015 BVMI-Vertreter bei der Entscheiderfabrik (u.a. für IHE Europe), 2009 bis 2017 Leitung der AG »IKT-Beratung für die Gesundheitswirtschaft«, seit 2005 im Beirat von ITeG, conhIT und DMEA

Der BVMI ist mir wichtig, weil…
- der BVMI wie kein anderer Verband die ehemaligen DDR-Medizininformatiker bei der beruflichen Integration in die HealthCare-IT der BRD unterstützt hat.
- der BVMI viele Weiterbildungsveranstaltungen, nicht nur in Berlin organisiert und unterstützt.
- der BVMI von 1996 bis 2017 Mitveranstalter und bis 2009 Träger der erfolgreichen TELEMED war.
- der BVMI als einziger berufsständischer Verband die Interessen der Medizinischen Informatiker und vergleichbarer Berufsgruppen wahrnimmt.
- ich durch den BVMI toll unterstützt wurde und viele kompetente Mitstreiter kennengelernt habe.

Köpfe im DVMD
Andrea Großer

Berufliches Tätigkeitsfeld
Med. Dokumentarin/DataManager, Referentin
Seit 1994, Universitätsklinikum Hamburg-Eppendorf, Institut für Medizinische Biometrie und Epidemiologie

Beruflicher Werdegang
- MTA Fachrichtung Labor
- MDA Hamburg

Weiterbildungen
Zahlreiche Weiterbildungen in Statistik (Uni Hamburg), Klinische Studien, Data Management, Didaktik, Lehre, u.a.
Regelmäßige Tagungsteilnahme DVMD und GMDS.

DVMD-Mitgliedschaft
- Seit 1994 Mitglied
- Im Vorstand: Schriftführerin 2002-2004,
- stellvertr. Vorsitzende 2005-2011, Vorsitzende 2011-2014
- Organisatorin Hamburger Doku-Stammtisch 1997-2015, Aktive des DVMD im Rahmen von Tagungsorganisation (1997-2012), Tagungsbegleitteam, Team Schulpatenschaft u.a.

Der DVMD ist mir wichtig, weil…
- ich so am Ball bleibe außerhalb meines Fachbereiches und über meinen fachlichen Tellerrand hinausschauen kann.
- die Vernetzung mit Kollegen durch den DVMD super klappt und sehr spannend ist.
- die Tagungen/Fortbildungsangebote des DVMD mir sehr wichtig sind.
- Und natürlich auch, weil der DVMD für mich die optimale Interessenvertretung auf fachlicher und berufspolitischer Ebene ist.
- Das möchte ich durch meine Mitgliedschaft unterstützen. In meiner jahrelangen ehrenamtlichen Aktivenzeit habe ich außerdem viel gelernt und sehr viel Spaß und Freude erlebt!
- es mir persönlich eine bessere Vorstellung für den Beruf der medizinischen Dokumentation und andere Berufsfelder ermöglicht, damit ich mich nach meinem B.Sc. besser orientieren kann

DVMD startet mit neuer Veranstaltungsreihe

Detaillierte Informationen finden Sie auf www.dvmd.de, die genauen Termine im DVMD-Eventkalender. DVMD-Mitglieder nehmen selbstverständlich kostenfrei teil.

Die andauernde Pandemie zwingt auch den DVMD, geplante Veranstaltungen abzusagen oder neu zu denken. Von Beginn an haben wir dies als Chance gesehen, denn eine Ergänzung unseres Veranstaltungsprogramms auf digitale Formate war schon lange in unseren Köpfen. Nun haben wir diese Chance ergriffen und zur Abrundung unserer Angebote eine neue Veranstaltungsreihe ins Leben gerufen, den DVMD-Fokus. Der DVMD-Fokus soll im Gegensatz zu unseren Tagungen und Symposien nicht an ein oder zwei vollen Tagen, sondern in regelmäßigen Abständen den »Fokus« auf Teilbereiche des Medizinischen Informationsmanagements lenken. Diese Teilbereiche bilden wir in 1,5- bis 3-stündigen Sessions und Tutorien ab. Aus Erfahrung wissen wir, dass kürzere Zeitblöcke nicht nur für die Informationsaufnahme, sondern auch für das Einbinden in den Arbeitsalltag besser geeignet sind als ganztägige Angebote. Beginnen werden wir im Februar 2021 und bieten dann regelmäßig bis Mitte Mai Sessions und Tutorien zu bestimmten Themenschwerpunkten an.

Termine

- 25.02.2021 Aus- und Weiterbildung
- 11.03.2021 Datenmanagement
- 12.03.2021 Grundlegende Datenstandards in der klinischen Forschung (Tutorial)
- 25.03.2021 Datenzugriff und -bereitstellung
- 26.03.2021 FHIR Basiswissen (Tutorial)
- 15.04.2021 Rechtliche Rahmenbedingungen
- 16.04.2021 Dokumentationspflichten unter der DS-GVO (Tutorial)
- 29.04.2021 Tumordokumentation
- 20.05.2021 Klinische Dokumentation

DVMD bietet neue Plattformen für die Branche

Veröffentlichung auf beiden Plattformen sind einfach und kostengünstig und stehen allen Personen und Institutionen offen.

Mit einigem Stolz beobachten wir, dass der DVMD mehr und mehr zur festen Instanz und etablierten Organisation für alle Fragestellungen rund um das medizinische Informationsmanagement geworden ist. Aufgrund unserer Fachexpertise und sinnvollen Leistungen sind wir zu gefragten Akteuren in der Branche geworden. Unsere MEDDOK-Mailingliste ist ein einmaliger Service, der wie kein anderes Medium geeignet ist, zielgruppengenau Events der Branche sowie Stellenanzeigen im medizinischen Informationsmanagement zu veröffentlichen. Um dieses Angebot abzurunden, haben wir nun eine Stellenbörse sowie einen Eventkalender entwickelt. Mit der DVMD-Stellenbörse bieten wir eine Plattform für Stellen- und Praktikumsangebote sowie für Stellengesuche. Hierbei fokussieren wir uns auf alle Jobs aus dem Bereich Informationsmanagement und Informatik in der Medizin. Auch als Praktikumsplattform für Schüler/-innen und Studierende dient die Stellenbörse. Im DVMD-Eventkalender zeigen wir gebündelt, was in der gesamten Branche los ist. Neben DVMD-Veranstaltungen finden hier auch Events aus den Bereichen Messen, Tagungen, Workshops, Schulungen externer Anbieter Platz. ■

Impressum

Charakteristik:
medizin://dokumentation/informatik/informationsmanagement/ (mdi) ist eine praxisorientierte Zeitschrift mit Fachartikeln zur Thematik der Medizinischen Dokumentation und des DV-Einsatzes im Gesundheitswesen und damit angrenzenden organisatorischen Fragen. Sie transportiert Erfahrungsberichte zu Top-Themen sowie aktuelle Entwicklungen direkt in die Praxis. Zielgruppe sind die ca. 2.600 tätigen Mitglieder der beteiligten Verbände, Entscheidungsträger im Management und DV-Management von Gesundheitsversorgungseinrichtungen und bei einschlägigen Industrie-Unternehmen wie Software-Häusern, Pharma-Firmen, CROs sowie leitende Mitarbeiter, Ärzte, Pflegekräfte und Therapeuten.

Verlag und Vertrieb:
Eigenverlag und Eigenvertrieb

ISSN: 1438-0900

Auflage: 1.600 Stück

Erscheinungsweise:
4-mal jährlich, jeweils zum Quartalsende

Herausgeber:
mdi GbR
c/o BVMI Berufsverband Medizinischer Informatiker e.V.
Oberlinstr. 26
41239 Mönchengladbach
Tel.: 02166 2171148
Fax: 02166 134545
info@bvmi.de | www.bvmi.de

c/o DVMD Der Fachverband für Dokumentation und Informationsmanagement in der Medizin e.V.
Lobdengaustraße 13
69493 Hirschberg
Tel.: 06201 4891884
Fax: 06201 4890459
dvmd@dvmd.de
www.dvmd.de

Nachdruck und Kopien:
Nur mit Genehmigung der Redaktion und unter Angabe der genauen Quelle

Manuskripte:
Zuschriften, die den Inhalt der Zeitschrift betreffen, sind direkt an die Redaktionsanschrift zu senden. Für unverlangte Manuskripte wird keine Haftung und keine Verpflichtung zur Veröffentlichung übernommen. Beiträge, die anderweitig parallel eingereicht wurden, werden nicht angenommen. Die Redaktion behält sich vor, aus technischen Gründen Kürzungen vorzunehmen. Namentlich gekennzeichnete Beiträge geben die Meinung des Verfassers wieder.

Redaktionsteam:
Prof. Dr.-Ing. Oliver J. Bott, Hannover | Prof. Dr. Andreas J. W. Goldschmidt, Frankfurt | Angelika Händel, Erlangen | Markus Stein, Berlin (Leitung) | Prof. Dr. Paul Schmücker, Mannheim

Redaktionsanschrift:
Siehe Verbandsanschrift des BVMI

Autorenrichtlinien:
unter www.forum-mdi.de

Bestellungen:
Über die Verbandsanschrift des BVMI. Abbestellungen sechs Wochen zum Jahresende

Bezugspreis:
Jährlich 49 Euro inkl. MwSt., inkl. Versandkosten. Ausland plus Versandkosten, für BVMI- und DVMD-Mitglieder frei

Anzeigenpreisliste:
Nr. 21 vom Januar 2020

Anzeigenverwaltung:
DVMD e.V.
Katharina Mai
Lobdengaustraße 13
69493 Hirschberg
Tel.: 06201 489-1884, Fax: -0459
dvmd@dvmd.de

Layout:
Fleck · Zimmermann, Berlin

Titelfoto:
Shutterstock, Juergen Faelchle

Druck:
Kössinger AG, Schierling

Semantische Analyse von Routine- und Forschungsdaten mit ID LOGIK®

Standardisierte Medikationsressourcen per FHIR®

Literatur:

König M, Sander A, Demuth I, Diekmann D, Steinhagen-Thiessen E. Knowledge-based best of breed approach for automated detection of clinical events based on German free text digital hospital discharge letters. PLOS ONE. 2019 Nov 27, https://doi.org/10.1371/journal.pone.0224916

Sander A, Wauer R. Integrating terminologies into standard SQL: a new approach for research on routine data. J Biomed Semantics. 2019 Apr 24;10(1):7

Sander A, Wauer R. From single-case analysis of neonatal deaths toward a further reduction of the neonatal mortality rate. J Perinat Med. 2018 Dec 19;47(1):125–133

// Gut aufgestellt für Ihre digitale MD-Kommunikation.

// Einfach. Sicher. Effizient.

Mit Archivar 4.0 inside ist DMI Ihr zukunftsorientierter Lösungspartner, mit dem Sie den neuen Qualitätsansprüchen an die MD-Prüfung und der geforderten digitalen Kommunikation gerecht werden.

Vertrauen Sie wie bereits 850 deutsche Krankenhäuser auf den IT-Spezialisten DMI. Über 50 Jahre Kompetenz in Sachen informationsbasierter Prozessoptimierung sprechen für sich!

Ihr 24 h Kontakt
Tel 02534 8005-888 (Stichwort: MD21)
md21@dmi.de | www.dmi.de/md-kommunikation

D·M·I
ARCHIVIERUNG