www.krankenhaus-it.de ISSN 1619-0629 Preis: 17,50 Euro

Ausgabe 3 / 2023

Krankenhaus-IT JOURNAL

Fakten und Perspektiven der IT im Gesundheitswesen

Compliance:
Alle mit ins Boot holen

Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V.
ENTSCHEIDERFABRIK
IHE DEUTSCHLAND Integrating the Healthcare Enterprise
KRITIScher Stammtisch IT-Sicherheit im Sektor Gesundheitswesen

PRO-KLINIK

KRANKENHAUSBERATUNG

WIR MACHEN KLINIKEN ERFOLGREICHER !

Digitalisierungs-Strategien für Krankenhäuser

Elektronische Patientenakte und digitale Archivierung

Optimierung vorhandener IT-Lösungen

Beschaffung neuer IT-Systeme

www.pro-klinik.de

Förderung von oben

Wolf-Dietrich Lorenz

In der Gesundheitspolitik und von Krankenkassen wird immer wieder betont, dass es eine übermäßige Anzahl von Krankenhausbetten gibt und dass Kostensenkungen notwendig sind. Dies deutet auf einen Paradigmenwechsel im Krankenhauswesen hin, da Krankenhäuser einem starken Wettbewerbs- und Kostendruck ausgesetzt sind. Gesundheitsminister Karl Lauterbach hat sogar von einer "Pleitewelle deutscher Kliniken" gesprochen.

Um den Bedürfnissen von Patienten, Mitarbeitern und der Öffentlichkeit gerecht zu werden, gewinnt die Regulierung stetig an Bedeutung. Die Einhaltung von internen Vorgaben sowie von Recht und Gesetz, also die Compliance, wird in der täglichen Arbeit immer wichtiger. Fehler in der internen Organisation eines Krankenhauses sind besonders relevant für die Compliance, wenn sie zu Schäden bei den Patienten führen oder den Schutz von Patientendaten, die als äußerst sensible Informationen gelten, beeinträchtigen.

Dagmar Finlayson

Im Zeitalter der digitalen Disruption stehen Krankenhausunternehmen vor der Herausforderung, Schritt zu halten mit den neuen Technologien und gleichzeitig die geltenden Compliance-Anforderungen zu erfüllen. Die technologische Entwicklung im medizinischen Bereich, wie beispielsweise KI Large Language Models (LLM), verändert sich rapide. Bei der Gestaltung digitaler Compliance-Strategien sollten insbesondere ethische Aspekte berücksichtigt werden, vor allem im Hinblick auf den verantwortungsvollen Umgang mit Patientendaten und die Transparenz von Richtlinien.

In einem Umfeld mit hohem wirtschaftlichem, intellektuellem und ethischem Wettbewerbsdruck gestaltet es sich schwierig, alle Regeln einzuhalten. Daher wird die Implementierung von Compliance-Strukturen umso wichtiger. Angesichts des zunehmenden Regulierungsdrucks und des anhaltenden Wettbewerbsdrucks ist es nicht überraschend, dass das Thema Compliance weiter an Bedeutung gewinnt.

Kim Wehrs

Compliance muss als integraler Bestandteil der digitalen Transformationsstrategie betrachtet werden. Dafür ist eine enge Zusammenarbeit zwischen Bereichen wie Medizin, IT, Datenschutz und anderen relevanten Abteilungen erforderlich. Zudem sollten Krankenhäuser regelmäßige Schulungen und Überprüfungen durchführen, um sicherzustellen, dass ihre Prozesse und Systeme den Compliance-Anforderungen entsprechen.

Die Unterstützung der Unternehmensführung ist für den Erfolg von Compliance unverzichtbar. Die Auseinandersetzung mit Compliance ist eine sensible kommunikative Aufgabe, da die Förderung von compliantem Verhalten auf Akzeptanz stoßen muss. Compliance wird oft skeptisch betrachtet, daher muss die Unternehmensführung die notwendige Akzeptanz für Compliance fördern.

Herzliche Grüße, Ihr Krankenhaus-IT Journal Team

P.S.: Für eine bessere Lesbarkeit wird im Text des Krankenhaus IT-Journals weitgehend auf gegenderte Sprache verzichtet; in allen entsprechenden Formulierungen sind weibliche, männliche und weitere Geschlechtsidentitäten mitgemeint.

Impressum
Antares Computer Verlag GmbH,
Gießener Straße 4, D-63128 Dietzenbach
E-Mail: info@krankenhaus-it.de, www.krankenhaus-it.de
Verlagsleitung und Herausgeber **Kim Wehrs (kw)**,
Stellvertr. **Kai Wehrs (kaw)**. Tel.: 0 60 74/25 35 8, Fax: 0 60 74/2 47 86
Redaktion, Chefredakteur **Wolf-Dietrich Lorenz (wdl)** (verantwortlich)
Mitglied der Chefredaktion **Dagmar Finlayson (df)**, Freier Journalist **Ralf Buchholz**, **Michael Reiter**
Redaktionelle Mitarbeit **Kai Wehrs** (Fotos und Onlineredaktion) **(kaw)**
Anzeigen + Verkauf **Kim Wehrs**, D-63128 Dietzenbach, Tel.: 0 60 74/2 53 58 **(kw)**
Layout, Grafik, & Satz **Nebil Abdulgadir**
Lektorat **Maike Buchholz**
Druck und Versand: Westdeutsche Verlags- und Druckerei GmbH,
Mörfelden-Walldorf
Erscheinungsweise 6 x jährlich Einzelpreis EUR 17,50 zzgl. Versand ab 01.01.2023
Abonnement: Bitte beim Verlag erfragen.
Verbandsorgan des Bundesverbandes der Krankenhaus - IT Leiterinnen/Leiter e. V.
Mitglied im Börsenverein des Deutschen Buchhandels (VK Nr. 14815 Verlag, 32320 Buchhandel)

Fotonachweis
Adobe Stock:
1,3,6, 10,15,22,28,30,36,38,40,42,
53,68,72,75,78

Titelthema

Gesundheitsanwendungen

IT Management

Compliance:
Alle mit ins Boot holen

Healthcare ohne Compliance ist nicht mehr denkbar. Die organisatorischen Rahmenbedingungen im Gesundheitswesen sollen Compliance-Verstöße verhindern. Zu den Sorgfaltspflichten der Krankenhausleitung gehören angemessene Maßnahmen zur Kontrolle von Compliance-Risiken – und alle mit ins Boot zu holen. Die integere Compliance-Organisation kann wesentlich den Behandlungserfolg bestimmen.

Bei der digitalen Transformation sind verschiedene Compliance-Anforderungen zu beachten, um die rechtlichen und regulatorischen Vorgaben einzuhalten. Zu den Aspekten zählen Datenschutz, die Einhaltung von Datenschutzgesetzen wie der EU-Datenschutz-Grundverordnung (DSGVO) ist von zentraler Bedeutung. Unternehmen müssen sicherstellen, dass personenbezogene Daten angemessen geschützt und verarbeitet werden.

Digitale Compliance-Strategien von Krankenhäusern

Dies umfasst die Implementierung von Sicherheitsmaßnahmen, die Einholung der erforderlichen Zustimmung der Betroffenen und die Gewährleistung der Rechte der betroffenen Personen. Patientendaten, insbesondere elektronische Gesundheitsdaten, sind angemessen geschützt. Dazu gehören Maßnahmen wie die Verschlüsselung sensibler Daten, Zugriffskontrollen, Firewall-Schutz, regelmäßige Überprüfungen der Sicherheitsinfrastruktur und Schulungen für das Personal zur Sensibilisierung für Datenschutzbestimmungen.

Ebenso bedeutsam ist IT-Sicherheit. Mit der digitalen Transformation steigt die Bedeutung der IT-Sicherheit. Unternehmen müssen angemessene Sicherheitsmaßnahmen implementieren, um ihre Systeme, Daten und Netzwerke vor Bedrohungen zu schützen. Dies umfasst den Einsatz von Firewalls, Verschlüsselungstechnologien, Zugriffskontrollen und regelmäßigen Sicherheitsaudits.

Angesichts der zunehmenden Bedrohungen durch Cyberkriminalität müssen Krankenhäuser robuste IT-Sicherheitsmaßnahmen implementieren, um sich vor Angriffen und Datenverlust zu schützen. Dies umfasst regelmäßige Überprüfungen der IT-Infrastruktur, Aktualisierung von Software und Systemen, Schulungen für Mitarbeiter zur Erkennung von Phishing-Angriffen und die Entwicklung eines Notfallplans für den Fall von Sicherheitsvorfällen.

Prof. Dr. iur. Alexandra Jorzig, Rechtsanwältin, Fachanwältin für Medizinrecht

Trotz unterschiedlicher Zwecke können Compliance- und Service-Level-Agreements (SLAs) integriert werden. Wenn ein Unternehmen bestimmte Compliance-Standards einhalten muss, kann es diese Anforderungen in den SLAs mit seinen Dienstleistern festlegen. Auf diese Weise wird sichergestellt, dass die Dienstleister die erforderlichen Compliance-Maßnahmen implementieren und einhalten.

Konformität mit gesetzlichen Vorschriften

Compliance im Cloud Computing bedeutet, für die digitale Transformation sicherzustellen, dass die Nutzung solcher Dienste mit den geltenden Compliance-Anforderungen vereinbar ist. Dies beinhaltet die Auswahl vertrauenswürdiger Cloud-Anbieter, den Schutz von Daten in der Cloud und die Beachtung von länder- oder branchenspezifischen Vorschriften.

Konformität mit gesetzlichen Vorschriften veranlasst Krankenhäuser, die einschlägigen gesetzlichen Vorschriften im Gesundheitswesen einzuhalten, wie zum Beispiel die Datenschutz-Grundverordnung (DSGVO) in Europa oder das Health Insurance Portability and Accountability Act (HIPAA) in den USA. Sie müssen Richtlinien und Verfahren entwickeln, um sicherzustellen, dass sie alle rechtlichen Anforderungen erfüllen.

Unternehmen werden ständig mit neuen gesetzgeberischen Anforderungen konfrontiert. So haben der Deutsche Bundestag und Bundesrat am 11. bzw. 12. Mai 2023 das Hinweisgeberschutzgesetzt (HinSchG) verabschiedet, welches die EU-Richtlinie 2019/1937 („Whistleblower-Richtlinie“) zukünftig in nationales Recht umgesetzt. Dann müssen viele Unternehmen ein Meldesystem zum Schutz von Personen vorhalten, die einen Verstoß gegen geltendes Recht melden wollen. Christoph Naucke, Associate Partner, Rödl & Partner, Compliance Officer, stellt heraus: „Bislang wurde relativ wenig wahrgenommen, dass in der Neufassung des IDW PS 980 zahlreiche Anforderungen deutlich verschärft wurden, ganz besonders hinsichtlich des Compliance-Risikomanagements und der Risikobewältigung, der Compliance-Organisation und -Dokumentation.“

Digitale Disruption und Compliance-Anforderungen

Disruption beinhaltet neuere Technologien wie künstliche Intelligenz, mobile Technologie, Analysen und Cloud. Sie verändern die Art und Weise, wie Menschen, Organisationen und Regierungen interagieren. Diese disruptiven Innovationen sorgen für eine nie dagewesene Vernetzung zwischen Menschen und für eine stärkere Verbraucherorientierung. Im Zuge der Weiterentwicklung des Gesundheitswesens wird eine stärkere Integration von Gesundheitssystemen digitale Funktionen oder Prozesse, die zuvor getrennt waren, in Unternehmen zusammenführen.

Im Kontext der digitalen Disruption stehen Unternehmen vor der Herausforderung, mit den neuen Technologien Schritt zu halten und gleichzeitig die geltenden Compliance-Anforderungen einzuhalten. Compliance bezieht sich auf die Einhaltung von Gesetzen, Vorschriften und internen Richtlinien, um ethisches und rechtlich korrektes Verhalten sicherzustellen.

Bei rechtlichen Rahmenbedingungen in der Medizin für Patienten und Kliniken kommen KI Large Language Models (LLM) z.B. ChatGPT für den ärztlichen Kontext in den Blick.

Prof. Dr. iur. Alexandra Jorzig, Rechtsanwältin, Fachanwältin für Medizinrecht: „Aus rechtlicher Sicht gilt es bei ChatGPT vor allem den Datenschutz zu beachten. ChatGPT speichert und nutzt die eingegebenen Daten. Sofern also personenbezogene Daten eingegeben (geprompted) werden, ist der Anwendungsbereich der DSGVO eröffnet.“

Die digitale Disruption kann Compliance-Anforderungen auf verschiedene Weise beeinflussen. Dies erfordert eine sorgfältige Überprüfung und Anpassung bestehender Compliance-Richtlinien.

Digitale Disruption führt oft zu einer erhöhten Menge an Daten, die gesammelt, gespeichert und verarbeitet werden. Unternehmen müssen sicherstellen, dass sie angemessene Maßnahmen ergreifen, um die Sicherheit und den Schutz dieser Daten zu gewährleisten. Dies umfasst die Einhaltung von Datenschutzgesetzen, wie der DSGVO (Datenschutz-Grundverordnung) in der Europäischen Union. Regulierungsbehörden passen ihre Vorschriften erfahrungsgemäß an die digitale Disruption an, um den Schutz der Verbraucher und die Integrität des Marktes sicherzustellen. Unternehmen müssen die sich ändernden regulatorischen Anforderungen beobachten und ihre Geschäftspraktiken entsprechend anpassen, um Compliance zu gewährleisten.

Christoph Naucke, Associate Partner, Rödl & Partner, Compliance Officer

Dipl.-Ing. Gabriele Münker, DGQ Qualitätsmanagerin/-Auditorin, Risikomanagementbeauftragte Medizinprodukte, Münker YASKO Consulting

Ebenso gehören regelmäßige Überprüfung und Aktualisierung von Richtlinien dazu. Krankenhäuser müssen ihre Compliance-Richtlinien regelmäßig überprüfen und an die sich ändernden Anforderungen anpassen. Dies umfasst die Berücksichtigung neuer Technologien und Geschäftsmodelle.

Risikominimierung und Notfallvorsorge

Die digitale Disruption bietet Chancen für Gesundheitsdienstleister, erfordert aber auch eine sorgfältige Auseinandersetzung mit Compliance-Anforderungen. Compliance und B3S (Business Strategy, Security & Safety) sind wichtige Aspekte im Krankenhausumfeld, um die Einhaltung von Vorschriften, Richtlinien und Sicherheitsstandards zu gewährleisten. Risikominimierung und Notfallvorsorge sind Teil des B3S-Ansatzes. Krankenhäuser müssen Risiken identifizieren, bewerten und geeignete Maßnahmen ergreifen, um diese zu minimieren. Dies kann die Erstellung von Notfallplänen, Schulungen für das Personal, die regelmäßige Überprüfung von Sicherheitssystemen und die Zusammenarbeit mit externen Organisationen umfassen, um im Notfall schnell und effektiv reagieren zu können.
Compliance-Management und Risikomanagement gehören zusammen und aufeinander abgestimmt. Das Compliance-Management erweitert den Blick des Risikomanagements.

Compliance Management ist Bestandteil des Risikomanagements. Dipl.-Ing. Gabriele Münker, DGQ Qualitätsmanagerin/-Auditorin, Risikomanagementbeauftragte Medizinprodukte, Münker YASKO Consulting, und Dr. Udo Jendrysiak, Medizininformatiker, merken an: „Der Risikomanager sollte insbesondere Wissen und Erfahrungen im Risikomanagement besitzen, da er die erforderlichen Grundlagen zusammenstellt sowie die Risikoanalyse vorbereitet und moderiert. Das Fachwissen wird im Team von den unterschiedlichen Teammitgliedern bereitgestellt." Die beiden Experten betonen: „ Risikomanagement ist immer Teamarbeit, da nur so eine umfassende und fundierte Analyse möglich ist, indem die unterschiedlichen Themen aus mehreren Blickwinkeln betrachtet werden." Risiken sind zu minimiert und zu beherrschen sowie Leistung und Effizienz zu steigern.

Ein interdisziplinäres Team

Eine wichtige Komponente der digitalen Compliance-Strategie ist die Schulung des Krankenhauspersonals. Mitarbeiter sollten über die relevanten Gesetze, Vorschriften und Richtlinien informiert sein und in der Lage sein, ihre täglichen Aufgaben im Einklang mit den Compliance-Anforderungen auszuführen. Bewusstseinsbildungskampagnen können auch dazu beitragen, das Verständnis für Datenschutz und Sicherheitsrisiken zu verbessern.

Zu den ersten Schritten gehört, seitens der Geschäftsführung ein interdisziplinäres Team mit der Vorbereitung zu beauftragen, einen - internen oder externen - Informationssicherheitsbeauftragten zu benennen, das Informationssicherheitsmanagement organisatorisch zu verankern und im Unternehmen zu kommunizieren. Dazu zählt die Bestellung eines Informationssicherheitsbeauftragten (ISB). Der ISB besitzt eine unabhängige und organisatorisch herausgehobene Stellung. Er ist in dieser Rolle direkt der Klinikleitung unterstellt und berichtet direkt an diese. Die Klinikleitung trägt weiterhin die Gesamtverantwortung für alle Belange der Informationssicherheit. Risikomanagement delegieren? Aufgaben ja – Verantwortung nein. Die Geschäftsführung muss die Verantwortlichkeit für die Kontrolle der Zielerreichung des Informationssicherheitsmanagements sowie für die Umsetzung der im IT-Sicherheitsprozess abgestimmten Maßnahmen eindeutig zuweisen.

IT-Projekte im Krankenhausumfeld werden von zahlreichen externen und internen Compliance-Anforderungen begleitet, deren Einhaltung integraler Bestandteil des jeweiligen Projekterfolgs ist.

Paul Haag, Sector Manager Healthcare, KPMG AG Wirtschaftsprüfungsgesellschaft: „Oftmals werden diese Compliance-Aspekte allerdings erst spät oder am Ende der Digitalisierungsprozesse bedacht, was zum Teil umfangreiche Veränderungen und damit einen erhöhten Ressourcenaufwand nach sich zieht."

Dr. Udo Jendrysiak, Medizininformatiker

Paul Haag, Sector Manager Healthcare, KPMG AG Wirtschaftsprüfungsgesellschaft

Ein Hinweisgeberkanal macht noch kein Compliance Management System

Hinweisgeberschutzgesetz, neuer Prüfungsstandard: Die Anforderungen an ein „feuerfestes" Compliance Management System (CMS) steigen erheblich. Verantwortliche in Krankenhäusern sind gut beraten, ihr CMS daher auch jenseits des gesetzlich geforderten Hinweisgebersystems einem weiter gefassten, kritischen Review und „Aktualitäts-Check" zu unterziehen.

Von Christoph Naucke, Associate Partner, Rödl & Partner

Am Schluss ging es dann doch überraschend schnell: Am 5. Mai 2023 einigte sich der Bund mit den Ländern auf einen Kompromiss zum Hinweisgeberschutzgesetz (HinSchG), und schon am 12. Mai 2023 war das Gesetz durch Bundestag und Bundesrat verabschiedet. Es soll zum weit überwiegenden Teil einen Monat nach der Verkündung in Kraft treten – voraussichtlich also bereits Mitte Juni 2023.

Die unmittelbaren Folgen sind weithin bekannt. Unternehmen mit mehr als 250 Beschäftigten, das dürfte auf Krankenhäuser generell zutreffen, müssen das Gesetz zum Datum des Inkrafttretens befolgen. Auf Grund der weit gefassten Definition des Begriffs „Beschäftigungsgeber" gilt das Gesetz für alle juristischen Personen des öffentlichen und des privaten Rechts, soweit diese mindestens einen Beschäftigten haben.

Informationskanäle, die auch externen Menschen offenstehen, sind in Krankenhäusern schon jetzt fester Bestandteil des Qualitätsmanagements. Es muss allerdings bezweifelt werden, dass diese zugleich auch bereits die Anforderungen des Hinweisgeberschutzgesetzes erfüllen. Insoweit ist auch hier eine HinSchG-konforme interne Meldestelle noch kurzfristig einzurichten. Wichtig dabei: Die interne Meldestelle kann auch ausgelagert werden, wie Rödl & Partner dies anbietet. (1)

Die Frage, ob ein anonymer Kanal angeboten werden muss, ist die falsche Frage.

Eine Rechtspflicht zur Bereitstellung eines anonymen Meldekanals ist mit dem Hinweisgeberschutzgesetz nicht gekommen – nun doch nicht, anders als ursprünglich von der Ampel geplant. Wenn man nicht gezwungen ist, richtet man also keinen anonymen Meldekanal ein? Der Gedanke liegt nahe, könnte aber eine Sackgasse sein. Denn für das Krankenhaus insgesamt besteht in Bezug auf tatsächlich eingetretene Rechtsverstöße nur insoweit eine Chance, den Umgang damit selbst zu gestalten, als dass die Verantwortlichen selbst es sind, die als erste davon erfahren und ihrerseits ggf. Strafverfolgungsbehörden einschalten können. Im anderen Fall wird man zum Objekt und verliert entscheidende Möglichkeiten zur aktiven Mitwirkung an der Aufklärung.

Fest steht: Je dramatischer der Rechtsverstoß, umso weniger sind die Zeugen bereit, diesen mitzuteilen, wenn sie nicht anonym bleiben können. Der rein intern über das Intranet zugängliche Kanal wird dabei subjektiv meist als nicht wirklich anonym wahrgenommen, auch dann nicht, wenn keine persönlichen Daten abgefragt werden. Hinzu kommt, dass dieser auch keinen Zugang für Personengruppen wie ehemalige Beschäftigte bietet, denen jedoch nach der Vorgabe des HinSchG die Meldemöglichkeit gegeben werden muss. Vor allem aber: Wer aufklären soll, braucht meist die Möglichkeit zur Rückkommunikation mit dem Hinweisgeber. Das wird schwierig, wenn dieser anonym bleibt. Deswegen ist eine externe Meldeplattform mit Login-Möglichkeit für den Hinweisgeber unbedingt empfehlenswert. Sie leistet nämlich beides: Echte technische Anonymität bei gleichzeitiger Möglichkeit, Rückfragen zu stellen und mit dem Hinweisgeber Kontakt zu halten.

Bitte nicht verwechseln: Hinweisgebermeldekanal ? Compliance Management System

In der öffentlichen Wahrnehmung wird ein Hinweisgebersystem oft vereinfacht als „das Compliance-System" oder ähnlich bezeichnet. Auch wenn ein wirksames Compliance Management System (CMS) ohne geeigneten Hinweisgeberkanal nicht denkbar ist, wäre eine solche Gleichsetzung nicht nur falsch, sondern auch riskant. Eine tatsächlich haftungsreduzierende Wirkung, die in der Regel angestrebt wird, erreicht das CMS nur durch die nachweisliche Einrichtung aller erforderlichen Komponenten, von

denen eben der Hinweisgeberkanal lediglich eine darstellt.

Parallel zum Hinweisgeberschutzgesetz verschärfen sich auch die qualitativen Ansprüche, die an ein CMS gestellt werden.

Als eine maßgebliche Norm für die Frage nach der tatsächlich umfassenden Wirksamkeit eines CMS hat sich der IDW Prüfungsstandard 980 für die Prüfung von CMS seit vielen Jahren etabliert. Das IDW hat diesen Standard im Jahr 2022 neu aufgelegt. Obwohl die Grundstruktur in Form der sieben Grundelemente unverändert blieb, liegt ein umfassend erneuerter, deutlich verschärfter und nicht lediglich revidierter Prüfungsstandard vor.

Die darin geforderte, bewährte Grundstruktur eines CMS fordert nachweisliche Managementhandlungen zur Schaffung eines CMS in Form von sieben Grundelementen:

1. **Compliance-Kultur**
2. **Compliance-Ziele**
3. **Compliance-Risiken**
4. **Compliance-Programm**
5. **Compliance Organisation**
6. **Compliance-Kommunikation**
7. **Compliance-Überwachung und -Verbesserung**

In der Beschreibung des sechsten Bausteins „Compliance-Kommunikation" heißt es: „Im Unternehmen wird festgelegt, wie [...] Hinweise auf mögliche und festgestellte Regelverstöße an die zuständigen Stellen im Unternehmen [...] berichtet werden." Eine von drei Anforderungen zum vierten Element „Compliance-Programm" lautet: „Das Compliance-Programm umfasst auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen."
Ein Hinweisgebersystem bedeutet für diese geforderten Funktionalitäten also eine notwendige Voraussetzung, nicht mehr, nicht weniger. Bislang wurde relativ wenig wahrgenommen, dass in der Neufassung des IDW PS 980 zahlreiche Anforderungen deutlich verschärft wurden, ganz besonders hinsichtlich des Compliance-Risikomanagements und der Risikobewältigung, der Compliance-Organisation und -Dokumentation. Angesichts dessen tun Verantwortliche in Krankenhäusern gut daran, ihr CMS auch jenseits des nunmehr gesetzlich geforderten Hinweisgebersystems einem weiter gefassten, kritischen Review und „Aktualitäts-Check" zu unterziehen.

(1) WhistleClue

Christoph Naucke, Associate Partner, Rödl & Partner, Compliance Officer (TÜV), IT-AuditorIDW, GRC-Experte mit Schwerpunkt Gesundheits- und Sozialwirtschaft, Buchautor „Einrichtung von CMS im Krankenhaus" (Kohlhammer Verlag 2020) und „Der neue Compliance-Prüfungsstandard IDW PS 980" (Haufe Lexware 2022)

Krankenhäuser und Service-Level-Agreements (SLA)

Krankenhäuser stehen vor der Herausforderung, sich an die fortschreitende digitale Transformation anzupassen, um effizientere und qualitativ hochwertigere medizinische Dienstleistungen anzubieten. Bei diesem Prozess können Service-Level-Agreements (SLAs) eine wichtige Rolle spielen. Innovative Service-Level-Agreements (SLAs) im Krankenhaus können dazu beitragen, die Qualität zu steigern. Es ist wichtig, klare und messbare Kriterien festzulegen, um die Leistung zu überwachen und gegebenenfalls Anpassungen vorzunehmen. Nicht zuletzt ist die Frage der Verantwortung für SLA von Bedeutung.

Ein Service-Level-Agreement ist eine Vereinbarung zwischen einem Dienstleister (in diesem Fall das Krankenhaus) und einem Kunden (z. B. eine andere Abteilung im Krankenhaus oder ein externer Partner), in der die Erwartungen und Leistungskriterien für den angebotenen Service festgelegt werden. SLAs können helfen, die Erbringung von Dienstleistungen zu standardisieren, die Verantwortlichkeiten zu klären und die Erwartungen beider Parteien zu erfüllen.
Im Kontext der digitalen Transformation in Krankenhäusern können SLAs verschiedene Aspekte abdecken Verfügbarkeit von IT-Systemen: SLAs können die Verfügbarkeit von elektronischen Patientenakten, medizinischen Geräten, Kommunikationssystemen usw. festlegen. Dies umfasst beispielsweise die maximale zulässige Ausfallzeit oder die Reaktionszeit bei Störungen.

Datensicherheit und Datenschutz: Krankenhäuser müssen sicherstellen, dass Patientendaten vertraulich behandelt und vor unbefugtem Zugriff geschützt werden. SLAs können daher Sicherheitsmaßnahmen und Datenschutzstandards definieren, die eingehalten werden müssen.

Support und Wartung: Digitale Systeme erfordern regelmäßige Wartung, Updates und technischen Support. SLAs können den Umfang und die Reaktionszeit für Support-Anfragen festlegen, um eine reibungslose Funktion der Systeme sicherzustellen.

Schulung und Weiterbildung: Die Einführung neuer digitaler Technologien erfordert oft Schulungen und Weiterbildungen für das medizinische Personal. SLAs können den Umfang der Schulungsmaßnahmen und die erforderlichen Qualifikationen definieren.

Performance und Effizienz: SLAs können auch Leistungskennzahlen enthalten, um die Effizienz und Qualität der digitalen Dienste zu messen. Dies kann beispielsweise die Reduzierung von Wartezeiten, die Verbesserung der Genauigkeit von Diagnosen oder die Steigerung der Effizienz von Arbeitsabläufen umfassen.

Bei der Gestaltung von SLAs sollten Krankenhäuser die Bedürfnisse ihrer internen und externen Kunden berücksichtigen und realistische Ziele setzen. Es ist wichtig, klare und messbare Kriterien festzulegen, um die Leistung zu überwachen und gegebenenfalls Anpassungen vorzunehmen.

Die digitale Transformation im Gesundheitswesen ist ein komplexer Prozess, und SLAs können dazu beitragen, die Umsetzung zu erleichtern, indem sie klare Vereinbarungen treffen und die Verantwortlichkeiten definieren. Durch die effektive Nutzung von SLAs können Krankenhäuser ihre digitale Infrastruktur verbessern, die Patientenversorgung optimieren und die Zufriedenheit der Patienten und Mitarbeiter steigern.

Service-Level-Agreements (SLA) bei der digitalen Transformation und Risiken

Bei der digitalen Transformation können Service-Level-Agreements (SLAs) bestimmte Risiken mit sich bringen. Hier sind einige potenzielle Schwellen zu beachten:

Missverständnisse bei der Definition von SLAs: Es kann zu Missverständnissen kommen, wenn die Anforderungen und Erwartungen nicht klar definiert sind. Dies kann zu Konflikten zwischen den beteiligten Parteien führen und die Umsetzung der digitalen Transformation beeinträchtigen.

Komplexität der SLAs: SLAs können aufgrund ihrer Komplexität schwer zu verstehen und zu verwalten sein. Es erfordert eine sorgfältige Planung und Überwachung, um sicherzustellen, dass alle Parteien die SLAs verstehen und in der Lage sind, sie einzuhalten.

Unvorhersehbare technische Herausforderungen: Bei der digitalen Transformation können unvorhersehbare technische Herausforderungen auftreten, die die Einhaltung der SLAs erschweren. Beispielsweise können unvorhergesehene Systemausfälle oder technische Störungen auftreten, die die vereinbarten Service-Level beeinträchtigen.

Abhängigkeit von Dritten: Oftmals ist die digitale Transformation mit der Nutzung von Dienstleistungen Dritter verbunden, z. B. Cloud-Service-Providern oder Software-Anbietern. In sol-

chen Fällen besteht das Risiko, dass die Leistung dieser Dritten die vereinbarten SLAs nicht erfüllt, was sich negativ auf die digitale Transformation auswirkt. Veränderungen im Geschäftsumfeld: Das Geschäftsumfeld kann sich während des digitalen Transformationsprozesses ändern. Neue Technologien, Wettbewerbsumfeld oder regulatorische Anforderungen könnten auftreten und die SLAs beeinflussen. Es ist wichtig, flexibel zu bleiben und bei Bedarf Anpassungen an den SLAs vorzunehmen. Um diese Risiken zu minimieren, ist es ratsam, bei der Gestaltung und Umsetzung von SLAs Folgendes zu beachten:

Klarheit und Transparenz bei der Definition der SLAs. Regelmäßige Überprüfung und Aktualisierung der SLAs, um auf Veränderungen reagieren zu können.

Klare Kommunikation zwischen allen beteiligten Parteien, um Missverständnisse zu vermeiden.

Einrichtung von Überwachungs- und Berichtssystemen, um die Leistung und Einhaltung der SLAs zu überwachen. Alternative Lösungen und Backup-Pläne für den Fall unvorhergesehener Ereignisse. Eine rechtliche und vertragliche Absicherung, um im Falle von Vertragsverletzungen angemessen reagieren zu können. Es ist wichtig, dass SLAs als Instrument zur Zusammenarbeit und zur Verbesserung der Leistung betrachtet werden, anstatt als starre Vorschriften, die den Fortschritt behindern könnten. Durch eine sorgfältige Planung und Überwachung können viele der potenziellen Risiken im Zusammenhang mit SLAs bei der digitalen Transformation gemildert werden.

Verantwortung für Service-Level-Agreements im Krankenhaus

Im Krankenhaus liegt die Verantwortung für Service-Level-Agreements (SLAs) in der Regel bei der Geschäftsleitung oder der Verwaltung des Krankenhauses.

Diese sind dafür verantwortlich, die SLAs zu entwickeln, zu überwachen und sicherzustellen, dass sie eingehalten werden. Die SLAs im Krankenhaus können verschiedene Bereiche abdecken, wie zum Beispiel die Qualität der medizinischen Versorgung, die Wartezeiten für bestimmte Behandlungen, die Verfügbarkeit von medizinischen Geräten oder die Reaktionszeiten des Krankenhauspersonals in Notfällen. Die Verantwortung für die Erstellung der SLAs liegt oft bei einem interdisziplinären Team, das aus Vertretern der medizinischen Fachbereiche, der Verwaltung und der IT-Abteilung besteht. Dieses Team definiert die spezifischen Service-Level-Ziele und legt die Messgrößen fest, anhand derer die Zielerreichung gemessen wird.

Die Geschäftsleitung oder Verwaltung ist dafür verantwortlich, dass die SLAs implementiert und kommuniziert werden. Dazu gehört auch die Sicherstellung der erforderlichen Ressourcen, um die vereinbarten Ziele zu erreichen. Sie überwachen regelmäßig die SLA-Kennzahlen und treffen Maßnahmen, falls die Ziele nicht erreicht werden.

Zusätzlich können SLAs auch mit externen Dienstleistern oder Partnern des Krankenhauses abgeschlossen werden, wie beispielsweise mit medizinischen Laboren oder Lieferanten von Medizingeräten. In solchen Fällen liegt die Verantwortung für die SLAs sowohl beim Krankenhaus als auch beim entsprechenden externen Partner.

Insgesamt ist die Verantwortung für die Service-Level-Agreements im Krankenhaus eine gemeinsame Aufgabe der Geschäftsleitung, der Verwaltung und anderer relevanten Abteilungen, um sicherzustellen, dass die medizinische Versorgung effektiv und effizient bereitgestellt wird und die vereinbarten Standards erfüllt werden.

Innovative Service-Level-Agreements im Krankenhaus

Innovative Service-Level-Agreements (SLAs) im Krankenhaus können dazu beitragen, die Qualität der Patientenversorgung zu verbessern und die Effizienz der Krankenhausabläufe zu steigern. Hier sind einige Beispiele für innovative SLAs im Krankenhaus:

Reaktionszeit: Ein SLA könnte eine definierte Reaktionszeit für verschiedene Situationen festlegen, z.B. die Zeit, die benötigt wird, um auf einen Notruf zu reagieren oder die Zeit, die benötigt wird, um auf eine Anfrage nach zusätzlicher medizinischer Versorgung zu antworten.

Wartezeiten: Ein SLA könnte festlegen, dass bestimmte Wartezeiten für Patienten eingehalten werden müssen, z.B. die maximale Wartezeit in der Notaufnahme oder die Wartezeit für geplante Operationen.

Behandlungsqualität: Ein SLA könnte Qualitätsindikatoren definieren, die erfüllt werden müssen, z.B. eine bestimmte Erfolgsrate bei chirurgischen Eingriffen oder die Einhaltung bestimmter medizinischer Standards.

Kommunikation und Informationsaustausch: Ein SLA könnte die Kommunikation zwischen den verschiedenen Abteilungen und Fachkräften im Krankenhaus regeln, um sicherzustellen, dass Informationen effektiv ausgetauscht werden und die Patientenversorgung nahtlos erfolgt.

Ressourcenmanagement: Ein SLA könnte festlegen, wie Ressourcen im Krankenhaus verwaltet werden sollen, z.B. die Verfügbarkeit von Betten, medizinischen Geräten und Fachkräften.

Patientenzufriedenheit: Ein SLA könnte die Messung der Patientenzufriedenheit beinhalten und festlegen, dass bestimmte Zufriedenheitsziele erreicht werden müssen.

Datenverfügbarkeit und -sicherheit: Ein SLA könnte sicherstellen, dass Patientendaten sicher gespeichert werden und bei Bedarf schnell verfügbar sind.

Innovative Service-Level-Agreements (SLAs) im Krankenhaus können dazu beitragen, die Qualität der medizinischen Versorgung zu verbessern, die Patientenzufriedenheit zu steigern und die Effizienz der Krankenhausabläufe zu erhöhen. Einige probate Merkmale von innovativen SLAs können die Richtung für das Krankenhaus weisen.

Patientenzentrierter Ansatz: Innovative SLAs sollten den Fokus auf den Patienten legen und sicherstellen, dass die Bedürfnisse und Erwartungen der Patienten erfüllt werden. Dies kann beispielsweise durch die Festlegung von Zielen für kurze Wartezeiten, eine persönliche Betreuung oder die Verfügbarkeit von Informationen und Kommunikationskanälen erreicht werden.

Messbare Leistungsindikatoren: SLAs sollten klare, messbare Leistungsindikatoren enthalten, die eine objektive Bewertung der erbrachten Leistungen ermöglichen. Dies können beispielsweise Indikatoren wie die Behandlungszeit, die Erfolgsrate von Operationen, die Patientenbewertungen oder die Einhaltung von Qualitätsstandards sein.

Technologieeinsatz: Innovative SLAs können den Einsatz von Technologie vorsehen, um die Effizienz und Qualität der Dienstleistungen zu verbessern. Dies kann die Nutzung von elektronischen Patientenakten, Telemedizin oder anderen digitalen Lösungen zur Unterstützung der Diagnose und Behandlung umfassen.

Flexibilität und Anpassungsfähigkeit: Krankenhäuser stehen vor einer Vielzahl von Herausforderungen und Veränderungen. Innovative SLAs sollten daher flexibel sein und es den Krankenhäusern ermöglichen, ihre Leistungen an sich ändernde Umstände und Bedürfnisse anzupassen. Dies kann beispielsweise durch regelmäßige Überprüfungen und Aktualisierungen der SLAs oder die Möglichkeit zur Implementierung neuer Technologien und Behandlungsmethoden erfolgen.

Partnerschaften und Zusammenarbeit: SLAs können auch Partnerschaften zwischen Krankenhäusern, medizinischen Fachkräften und anderen Akteuren im Gesundheitswesen fördern. Durch eine enge Zusammenarbeit und den Austausch von Informationen können Synergien geschaffen werden, um die Qualität der Versorgung zu verbessern und die Effizienz zu steigern.

Anreizsysteme: Innovative SLAs können Anreizsysteme enthalten, um Mitarbeiter und Krankenhäuser zur Erreichung der vereinbarten Ziele zu motivieren. Dies kann beispielsweise die Bereitstellung von finanziellen Anreizen, Anerkennung oder Weiterbildungsmöglichkeiten umfassen.

Insgesamt können innovative SLAs im Krankenhaus dazu beitragen, eine qualitativ hochwertige, patientenzentrierte Versorgung zu gewährleisten und gleichzeitig die Effizienz und Zusammenarbeit zu fördern. Durch klare Ziele, messbare Indikatoren und den Einsatz von Technologie können Krankenhäuser ihre Leistungen verbessern und den sich wandelnden Anforderungen des Gesundheitswesens gerecht werden.

Routineaufgaben bei KI – Letztverantwortung beim Arzt

KI-Algorithmen besitzen eine enorm hohe Rechenleistung. Das Zusammenspiel KI – Mensch kann zu einer erheblichen Qualitätssteigerung in der Gesundheits- und Pflegeversorgung führen. Doch Vorsicht ist geboten, wenn es sich wie bei ChatGPT um einen (unwissenschaftlichen) Textgenerator handelt. Diesbezüglich bleibt es dabei, dass auch bei Nutzung von KI-Algorithmen die Letztverantwortung beim Arzt liegt und auch dort verbleiben muss. Im Interview mit dem Krankenhaus IT Journal erörtert die Rechtsanwältin Professorin iur. Alexandra Jorzig klinische Einsatzmöglichkeiten, rechtliche Rahmenbedingungen in der Medizin und Perspektiven und für KI-Sprachmodelle.

Prof. Dr. iur. Alexandra Jorzig, Rechtsanwältin, Fachanwältin für Medizinrecht, Professorin für Gesundheitsrecht/Digital Health, IB Hochschule für Gesundheit und Soziales Berlin, JORZIG Rechtsanwälte, Düsseldorf

Welche rechtlichen Rahmenbedingungen in der Medizin für Patienten und Kliniken sind durch KI Large Language Models (LLM) z.B. ChatGPT für den ärztlichen Kontext zu definieren?

Prof. Jorzig: Aus rechtlicher Sicht gilt es bei ChatGPT vor allem den Datenschutz zu beachten. ChatGPT speichert und nutzt die eingegebenen Daten. Sofern also personenbezogene Daten eingegeben (geprompted) werden, ist der Anwendungsbereich der DSGVO eröffnet. Die Verwendung personenbezogener Daten ist nach Art. 6 I DSGVO nur unter besonderen Bedingungen möglich. Liegen diese Bedingungen nicht vor, stehen nicht nur Sanktionen nach der DSGVO, sondern auch eine Strafbarkeit wegen der Verletzung der ärztlichen Schweigepflicht (§ 203 StGB) im Raum. Wichtig zu betonen ist noch, dass die personenbezogene DSGVO nur bei Anonymisierung der Daten nicht eingreift. Eine Pseudonymisierung, bei der unter Zuhilfenahme zusätzlicher Daten Rückschlüsse auf die Person möglich sind, ist demnach nicht ausreichend.

Wie weit können rechtliche Rahmenbedingungen bei textbasierten Dialogsystemen wie ChatGPT Entscheidungsfindungen der Therapie oder Behandlung Mediziner und Patienten rechtlich absichern? Welche Optimierung ist nötig, um rechtliche Rahmenbedingungen an evidenzbasierte, patientenzentrierte Medizin zu entsprechen?

Prof. Jorzig: Durch rechtliche Rahmenbedingungen ist dies nur schwerlich möglich, denn gerade dort liegt das Problem von ChatGPT. Das Tool ist nicht evidenzbasiert und patientenzentriert. Die zur Verfügung stehenden Daten werden gerade nicht nach wissenschaftlicher Relevanz unterschieden. Zudem kann das Programm nicht zwischen Fakt und Fiktion unterscheiden, es konfabuliert. OpenAI, der Betreiber von ChatGPT, spricht diesbezüglich von hallucinations. Zwar hat OpenAI kürzlich eine Strategie vorgelegt, um gegen diese hallucinations von ChatGPT vorzugehen. Noch sollte der Fokus hingegen darauf gerichtet werden, dass es sich bei ChatGPT um einen (unwissenschaftlichen) Textgenerator handelt.

Prof. Jorzig: Wie weit kann KI - Algorithmen, im klinischen Kontext angewendet - die ärztliche Rolle und die damit verbundenen Aufgaben verändern? Wie sollte sich die Ärzteschaft im Sinne rechtlicher Rahmenbedingungen darauf vorbereiten?

Prof. Jorzig: Im Zusammenhang mit Künstlicher Intelligenz wird oftmals die Frage aufgeworfen, ob KI uns nicht irgendwann (oder sogar in naher Zukunft?) alle ersetzen wird. Für den Beruf des Arztes gilt es, die unterschiedlichen KI-Algorithmen als Werkzeug und nicht als Substitution anzusehen. Die Gründe, warum ChatGPT den Arzt nicht ersetzt, habe ich bereits angerissen. Als Textgenerator kann ChatGPT aber bei administrativen Aufgaben hilfreich sein, z. B. bei der Erstellung von Arztbriefen. Generell können KI-Algorithmen Routineaufgaben übernehmen und zur Effizienz von Arbeitsabläufen beitragen. Ärzte hätten somit wieder mehr Zeit für ihre originäre Aufgabe, der medizinischen Behandlung von Patienten. Diesbezüglich bleibt es dabei, dass auch bei Nutzung von KI-Algorithmen die Letztverantwortung beim Arzt verbleibt und auch dort verbleiben muss!

Prof. Jorzig: Welche Potenziale liegen in der Kombination aus KI-basierten Diensten und menschlicher Korrektur? Welche Perspektiven für Arzt und Patienten sollten rechtliche Rahmenbedingungen eröffnen? Wo stehen wir?

Prof. Jorzig: Man sollte sich zunächst vor Augen führen, dass KI-Algorithmen eine enorm hohe Rechenleistung besitzen und das 24/7. Diese Algorithmen können bei vorhandener digitaler Infrastruktur Millionen von Daten miteinander verknüpfen und analysieren. Gerade das Zusammenspiel KI – Mensch kann zu einer erheblichen Qualitätssteigerung in der Gesundheits- und Pflegeversorgung führen, denn allein die KI-basierte Datenanalyse kann nicht ausreichen. Eine sich daran anschließende Behandlung greift auch immer in eine individuelle soziale Lebenssituation ein, die der behandelnde Arzt im Blick haben muss. Um die angesprochene digitale Infrastruktur auszubauen und Daten interoperabel miteinander verknüpfen zu können hat das Bundesgesundheitsministerium in seiner Digitalisierungsstrategie die Einführung eines Digital- und eines Gesundheitsdatennutzungsgesetzes (GDNG) angekündigt. Ein wichtiger Schritt, um der in Deutschland noch herrschenden fragmentarischen Datenlandschaft entgegenzuwirken.

Krankenhausbau und digitale Transformation: Eine Frage des Miteinanders

Um Krankenhäuser zukunftssicher aufzustellen, braucht es mehr als finanzielle Mittel. Die geplante Krankenhausreform zeigt wichtige Stellschrauben auf und auch die Digitalisierung bleibt ein zentraler Faktor. Soll sie ihr Potenzial entfalten, muss sie insbesondere im Kontext des Krankenhausbaus betrachtet werden. Ob die Synergien gehoben werden, hängt davon ab, wie die Verantwortlichen an diese Aufgabe herangehen und ob ein neues Miteinander entsteht. Von Katrin Thies, Partner bei EY Real Estate, und Florian Benthin, Partner bei EY Parthenon

4,3 Milliarden Euro Fördergelder für Digitalisierung werden durch das Krankenhauszukunftsgesetz (KHZG) mobilisiert. Gefördert werden insbesondere modernisierte Notfallkapazitäten und digitale Infrastruktur. Letzteres umfasst unter anderem Patientenportale, die elektronische Dokumentation von Behandlungen und digitales Medikationsmanagement. Sicherlich darf das an dieser Stelle als weitgehend bekannt vorausgesetzt werden. Wir betonen es dennoch, weil es erfolgsentscheidende ist: Die digitale Ertüchtigung von Gesundheitsbauten lässt sich nicht von weiteren baulichen Aspekten trennen. Erfreulich ist daher, dass der Gesetzgeber dies auch im KHZG berücksichtigt. Das meint nicht nur, dass Digitalisierungsprojekte auch bauliche Aspekte adressieren, sondern dass umgekehrt auch bauliche Maßnahmen mit dem Ziel der Digitalisierung anteilig auch über das KHZG gefördert werden.

Insbesondere wenn wir über Notfallkapazitäten sprechen, hat das sowohl personelle und organisatorische als auch bauliche und infrastrukturelle Implikationen. Etwas plastischer ausgedrückt: Der Weg und Zeitaufwand vom Krankenwagen oder Helikopterlandeplatz in die Notaufnahme ist ebenso zu berücksichtigen wie etwa die digitale Aufnahme der Patientendaten. Ein digitales Management der Medikation wiederum kann sich baulich insofern auswirken, dass etwa durch Echtzeitinformationen und automatische Bestellauslösung weniger Vorratshaltung und damit geringere Flächenkapazitäten für die Lagerfunktion erforderlich sind. Gleiches gilt für Archive für Patientenakten und Wartebereiche. Aus der baulichen Perspektive betrachtet, ist beispielsweise festzuhalten: kein Neubau ohne WLAN und keine Renovierung ohne Platz für Visitenwagen.

Zwischen Konsens und Differenzen

So einleuchtend die Zusammenhänge sind, so schwierig ist es, entsprechende Lösungen in den Krankenhausbau und -alltag zu übersetzen. Das meint nicht nur die Tatsache, dass es für jedes Krankenhaus individueller Lösungen bedarf, die zum Standort, zur Personalstruktur und zu den jeweiligen Prozessen passen. Mindestens genauso relevant ist die Frage, wie entsprechende Projekte aufgesetzt werden. Fakt ist: Soll das Ergebnis zur Organisation passen und im Krankenhausalltag gelebt werden, müssen alle Beteiligten gemeinsam daran arbeiten (können). Und genau an diesem Punkt kommt es oftmals zu Reibungen.

Vielen Kliniken fehlt neben personellen Kapazitäten und Know-how ein übergeordnetes Projektmanagement und damit eine umfassende Übersicht über alle anstehenden Themen und deren Priorisierung. Hinzukommende Projekte etwa werden ohne Rückkopplung mit den bisherigen Planungen neu priorisiert und drängen andere potenziell in den Hintergrund oder gar ganz ins Abseits. Das Ergebnis: Frust bei Beteiligten und Anwendern, Zeitverzug und Mehrkosten.

Geheimwaffe Projektmanagement

Der entscheidende Hebel, um dieses Spannungsfeld, das sich meist aus ungeklärten organisatorischen Fragestellungen, gelernten Herangehensweisen und nicht selten Kompetenzgerangel zwischen einzelnen Abteilungen ergibt, aufzulösen, ist eine übergeordnete Steuerungsstruktur (Governance). So sollte zunächst ein Rahmen geschaffen werden, zum Beispiel durch ein Projektmanagement-Team. Zu den ersten Schritten gehören die Klärung von Rollen, Pflichten und Beziehungen zwischen den Projektbeteiligten, die Definition von Prozessen zur effektiven Konflikt- und Problemlösung sowie die Förderung von transparenten Kommunikationsprozessen. Ziel ist es ferner, auf diese Weise das Vertrauen von Projektsponsoren, Betroffenen und Beteiligten zu gewinnen. Das gelingt nicht zuletzt über einen interdisziplinären Ansatz, der verschiedene Kompetenzen zusammenbringt, insbesondere aus den Bereichen IT und Bauplanung. Zudem sollten klare Erfolgsfaktoren (KPIs) am Anfang des Projektes definiert werden, um die Zielerreichung zu messen. Zu viele Projekte laufen länger, weil das zu erreichende Ziel am Anfang nicht klar abgesteckt wurde.

Vernetzt denken und handeln

Kommunikation und Kooperation sind also zentral, um bereichs- und abteilungsorientiertes von prozessfokussiertem Denken und Handeln abzulösen, Ressourcen effizient zu steuern und die Motivation aufrechtzuerhalten. Gefragt ist jedoch nicht nur ein professionelles Projektmanagement, sondern auch ein gutes Portfoliomanagement. Für welche Projekte werden Gelder ausgegeben und lassen sich Digitalisierung und Bau dort kombinieren? Gerade beim Bau geht es um hohe Summen, die – verschiedene Fragestellungen verbindend – genutzt werden können. Auch strategische Themen wie Gesundheitsnetzwerke können bauliche Themen bedingen. So fördert die digitale Transformation in Kombination mit der Ambulantisierung Netzwerke, deren bauliche Umsetzung entsprechend geplant werden muss.

Ernst & Young Real Estate GmbH
Mergenthalerallee 3-5, 65760 Eschborn, Germany

Mobile: +49 160 93 9 15 66 4
Email: katrin.thies@de.ey.com
Website: www.de.ey.com

Katrin Thies | Partner | Architektin AKBW | Immobilienökonom IRE| BS | PMP | Strategy and Transactions

Die Sekundärnutzung im European Health Data Space

Der Verordnungsentwurf der Kommission der Europäischen Union (EU) über den European Health Data Space (EHDS) hat in den letzten Monaten für viel Aufmerksamkeit gesorgt. Und das zurecht: der Verordnungsentwurf hat das Potenzial, neben der Versorgung vor allem die medizinisch-psychologische Forschung auf ein ganz neues Niveau zu heben und europäische Innovation im Gesundheitsbereich voranzutreiben. Von Christian Teichter und Pauline Engels, Technologiekanzlei Schürmann Rosenthal Dreyer Rechtsanwälte

I. Chancen der Sekundärnutzung

Die von dem Entwurf vorgesehenen Änderungen sind allerdings so umfassend, dass sich die betroffenen Akteur:innen frühzeitig einen Überblick darüber verschaffen sollten.

Der Verordnungsentwurf differenziert zwischen zwei verschiedenen Arten der Nutzung von elektronischen Gesundheitsdaten, der Primärnutzung zu Versorgungszwecken auf der einen und der Sekundärnutzung zu Forschungszwecken auf der anderen Seite. Anknüpfend an den hier veröffentlichten Beitrag zur Primärnutzung, widmen wir in diesem Beitrag der Sekundärnutzung besondere Aufmerksamkeit.

II. Struktur der Sekundärnutzung

1. Verwendungszwecke und Datenarten

Die Sekundärnutzung von elektronischen Gesundheitsdaten wird in Kapitel IV des EHDS-Verordnungsentwurfs (EHDS-VO-E) geregelt. Dabei werden zunächst Zwecke festgelegt, für die die Daten im Rahmen der Sekundärnutzung verwendet werden dürfen. Insgesamt umfasst die erlaubte Sekundärnutzung Forschung, Innovation, Politikgestaltung, Regulierung und die Verbesserung der Patientensicherheit. Damit ist von den zulässigen Nutzungszwecken beispielsweise die Datenverarbeitung aus Gründen des öffentlichen Interesses und im Bereich der öffentlichen Gesundheit umfasst, wie der Schutz vor grenzüberschreitenden Gesundheitsgefahren. Weiter dürfen die Daten für die Entwicklung von Arzneimitteln und Medizinprodukten verwendet werden. Daneben aber auch, um Algorithmen zu trainieren, digitale Gesundheitsanwendungen (DiGAs) weiterzuentwickeln oder dazu beizutragen, die personalisierte Gesundheitsversorgung zu professionalisieren.

Der Verordnungsentwurf legt dabei auch unerlaubte Sekundärnutzungszwecke fest. Nicht verwendet werden dürfen die elektronischen Gesundheitsdaten beispielsweise für kommerzielle Werbung oder die Entwicklung von alkoholischen Getränken und Tabakerzeugnissen oder anderen gefährlichen Produkten.

Angefordert werden können sowohl elektronische Gesundheitsdaten, die im Rahmen der Primärnutzung gesammelt (beispielsweise in Patientenakten) als auch unmittelbar im Rahmen der Sekundärnutzung (etwa bei einer Befragung von Studienteilnehmer:innen) erhoben wurden

2. Akteur:innen

Der EHDS-VO-E unterscheidet zwischen Dateninhaber:innen (jede Stelle, die Gesundheitsdaten verarbeitet und künftig in pseudo- oder anonymisierter Form bereitstellen muss) und Datennutz:erinnen (jede Stelle, die Gesundheitsdaten zu einem in der EHDS-VO erlaubten Zweck verarbeiten will). Die Begriffe der Datennutzer:innen bzw. der Dateninhaber:innen sind dabei recht weit. Hierzu zählen beispielsweise sowohl Krankenhäuser und Kliniken (sowohl öffentliche, private als auch Universitätskliniken) und Betreiber Medizinischer Versorgungszentren (MVZ) aber auch Krankenkassen (GKV und PKV), Labore, DiGA-Hersteller, E-Health-Dienstleister, Hersteller/Anbieter von IT-Lösungen im Gesundheitsbereich, Arzneimittel- und Medizinproduktehersteller, als auch private und öffentliche Forschungsinstitute.

3. Infrastruktur und Governance

Um die kontrollierte Freigabe elektronischer Gesundheitsdaten von Dateninhaber:innen an Datennutzer:innen zu regeln, sieht der EHDS-VO-E eine grenzüberschreitende Infrastruktur unterdem Oberbegriff HealthData@EU vor, die von speziellen Governance-Mechanismen flankiert wird.

Christian Teichter ist Rechtsanwalt der Technologiekanzlei Schürmann Rosenthal Dreyer Rechtsanwälte und auf das Datenschutz- und IT-Recht spezialisiert.

Auf nationaler Ebene sollen die Mitgliedstaaten sog. Zugangsstellen für Gesundheitsdaten einrichten. Die entsprechende Zugangsstelle prüft dann, ob der/die Antragsteller:in die Anforderungen der EHDS-VO erfüllt und stellt – bei Vorliegen der jeweiligen Voraussetzungen – sogenannte Datengenehmigungen aus. Nach Erteilung der Genehmigung fordert sie die elektronischen Gesundheitsdaten bei dem/der Dateninhaber:in an und stellt sie dem/der Datennutzer:in bereit. Zu den Aufgaben der Zugangsstellen zählt auch die Bereitstellung einer sicheren Infrastruktur zur Bereitstellung und Aufbereitung der Daten. Entscheiden sich Mitgliedsstaaten dafür, mehrere Zugangsstellen einzurichten, muss eine der Stellen eine koordinierende Funktion haben.

Die zentrale Plattform, die den länderübergreifenden Datenaustausch zwischen den Mitgliedstaaten ermöglichen soll, wird dabei als zentrale Plattform für die Sekundärnutzung elektronischer Gesundheitsdaten bezeichnet und von der Kommission eingerichtet.

Überwacht werden soll die Umsetzung der Vorgaben im EHDS-VO-E von einer digitalen Gesundheitsbehörde, die die Mitgliedstaaten zusätzlich einrichten sollen. Diese kann wahlweise in bereits bestehende Behörden integriert werden; denkbar wäre in Deutschland z.B. eine Zusammenlegung mit dem Bundesgesundheitsministerium.

III. Fazit

Das Potenzial der Sekundärnutzung elektronischer Gesundheitsdaten, wie sie im EHDS-VO-E angedacht ist, ist nicht von der Hand zu weisen. Der fehlende Zugang zu Daten ist aktuell ein Grund für das Scheitern zahlreicher Forschungsprojekte; dieses Hemmnis könnte der EHDS beseitigen und endlich den Weg frei machen für die Entwicklung innovativer Arzneimittel und Medizinprodukte, die bessere Erforschung seltener Krankheiten und die Entwicklung effizienter Behandlungsmethoden. Auf dem Weg dahin gilt es aber, die noch bestehenden Unklarheiten zu beseitigen. Insbesondere scheut sich der europäische Gesetzgeber bisher leider davor, konkrete Anforderungen an die Anonymisierung der bereitzustellenden elektronischen Gesundheitsdaten zu regeln. Weiter bleibt aus praktischer Sicht unklar, wie die Dateninhaber:innen die umfangreichen Bereitstellungs- und Archivierungspflichten bewältigen können. Wichtig ist vor allem, dass diese Pflichten praxisnah- und tauglich umsetzbar bleiben, da Dateninhaber:innen hohe Bußgelder riskieren, wenn sie den Vorgaben im EHDS-VO-E nicht nachkommen. In den Schritten, die im parlamentarischen Prozess auf EU-Ebene noch folgen werden, ist außerdem zu erwarten, dass der Entwurf noch einige Anpassungen erfahren wird. Es bleibt zu hoffen, dass dabei eine Balance zwischen dem Potenzial der Sekundärnutzung und einem ausreichenden Schutz der besonders sensiblen Gesundheitsdaten gelingt.

www.srd-rechtsanwaelte.de

Digitale Disruption im „Unternehmen Krankenhaus"

Disruption setzt das „Unternehmen Krankenhaus" unter Druck, Leistungen digital zu optimieren, Verbesserung der organisatorischen Effizienz erzielen und durch disruptive Innovationen herbeizuführen und umzusetzen. Dr. Patrick Heiler, Director Healthcare bei IG&H, skizziert einige Kernpunkte.

Eines lässt sich vorneweg sagen: Digitalisierung im „Unternehmen Krankenhaus" existiert, das ist die gute Nachricht. Es gibt kaum einen Bereich, der keine digitalen Prozesse beinhaltet. Angefangen bei der Bettenreinigung, über das Gebäudemanagement und die dazugehörige Technik bis hin zu den klinischen Systemen selbst. Doch auch, wenn schon einiges passiert ist – Digitalisierung im Gesundheitswesen kann und sollte noch viel mehr. Disruptive Innovationen sind auch dringend notwendig. Nicht erst seit dem Ausbruch der Corona-Pandemie vor drei Jahren ist klar, dass unser Gesundheitssystem an einigen Stellen überholt werden muss.

Die eigene digitale Strategie kennen

Eine weitere gute Nachricht lautet: Es existieren bereits viele Innovationen an unterschiedlichen Stellen. Unterschiedlichen Schätzungen zufolge sind in einem Krankenhaus rund 100 bis 400 verschiedene Softwarelösungen im Einsatz. Das Problem liegt darin, dass viele dieser nicht miteinander kommunizieren, sodass viel Potential verschenkt wird. Es benötigt daher dringend Innovationen auf Basis digitaler Transformation. Eine Technologie, die dabei eine große Rolle spielt, ist Künstliche Intelligenz (KI). KI braucht Daten, um wiederum aus diesen zu lernen. Sie erkennt Strukturen und Prozesse, die in vielen Bereichen eines Krankenhauses – von der Abrechnung bis zur zentralen Notaufnahme – helfen können, zu besseren Entscheidungen zu kommen.

Ziel des Ganzen sollte eine hohe Interoperabilität sein. Dafür braucht es eine offene Haltung gegenüber der Implementierung und Nutzung neuer Systeme. Voraussetzung für eine Weiterentwicklung ist allerdings, dass Infrastruktur und Projektvorhaben zusammenpassen. Dabei sollten wichtige Fragen vorab geklärt werden: Cloud ja oder nein? Passt das Vorhaben zur digitalen Strategie des Krankenhauses? Wie sehr wird IoT (Internet of Things) eine Rolle spielen? Fakt ist: Es bringt nichts, eine pauschale IT-Lösung zu implementieren. Stattdessen empfiehlt sich ein Schritt-für-Schritt-Vorgehen, das die oben angeführten Fragestellungen individuell berücksichtigt.

Innovation muss beim Anwender beginnen

Spricht man von disruptiver Innovation im Gesundheitswesen, muss vor allen Dingen eines klar sein: Nämlich, dass es in erster Linie um den Mehrwert für den Anwender, sprich das Krankenhauspersonal sowie für den Patienten selbst, gehen muss. Denn eine Lösung kann noch so innovativ und zukunftsweisend sein – wenn sie keinen konkreten Nutzen hat und nicht in die gesamte Strategie passt, ist sie fehl am Platz. Ein Beispiel aus der Praxis: Über einen Telemedizinroboter könnten sich Ärzte mancherorts von einem anderen Krankenhaus zur Visite dazuschalten. Jedoch beobachten wir, dass diese Technologie oft nicht genutzt, da sich das Personal – so wie in der Vergangenheit – per Telefon zusammenruft. Hier stoßen also Tradition und Möglichkeiten aufeinander. Daher sollte immer der konkrete Prozess berücksichtigt werden: Welche Herausforderungen haben die Anwender? Welche Probleme müssen gelöst werden? Idealerweise arbeiten Anwender und Projektverantwortliche – sei es intern oder mit externen Partnern – zusammen. Dies wird nach wie vor zu wenig praktiziert, stellt aber einen wichtigen Katalysator für mehr anwenderorientierte Innovation dar.

Transformation braucht Use Cases und das Gesetz

Weichen für mehr disruptive Innovation im deutschen Gesundheitswesen können nur dann gestellt werden, wenn auch ein Bewusstseinswandel bereits im Gange ist. Dann setzt Transformation ein, sprich der Anwender beziehungsweise ein konkreter Prozess rückt in den Mittelpunkt der Betrachtung. Werden daraus gezielt Use Cases generiert, nimmt das Ganze seinen natürlichen Lauf. Eine wichtige Rolle nimmt hier der Staat ein. Denn gerade um Systemoffenheit zu erreichen, braucht es Standards, die definiert werden müssen. Und das kann mittels Gesetzgebung in die richtige Richtung gelenkt werden, um noch anwenderorientierter zu agieren und Innovation damit voranzutreiben.

Dr. Patrick Heiler ist Director Healthcare bei der Beratungs- und Technologiefirma IG&H.

Vom Potenzial zur Realität – die Digitalisierung des deutschen Gesundheitswesens

Der große potenzielle Nutzen von Künstlicher Intelligenz (KI) wird zunehmend deutlich, auch im Gesundheitswesen. Krankenhäuser dürfen diese Entwicklung nicht verpassen, sondern müssen die Technologie möglichst effektiv – für Patienten sowie Mitarbeiter – und sicher implementieren. Isabela Buhai, Endava, erklärt, worauf es dabei ankommt und wie Krankenhäuser die bevorstehenden Veränderungen meistern können.

Trotz aller Fortschritte in den letzten Jahren kommt die Digitalisierung in Deutschland generell nur schleppend voran. Auch im Gesundheitswesen ist das Potenzial digitaler Lösungen und Prozesse noch lange nicht ausgeschöpft. Dies muss sich ändern, denn alle Beteiligten profitieren von einer sicheren, vernetzten Medizin: Die Versorgungsqualität steigt, die Arbeitsbelastung sinkt, Kosten werden eingespart.

KI-Systeme sind in der Lage, große Mengen an Daten auszuwerten und dieses Wissen jederzeit abzurufen. Diese Fähigkeit wird heute schon in der Diagnostik zur (Früh-)Erkennung von Krankheiten genutzt, was den Diagnoseprozess enorm beschleunigen kann.

Isabela Buhai, Head of Healthcare Delivery für Europa bei Endava: „Eine Lösung kann in der Theorie noch so viele Vorteile bieten, wenn sie nicht genutzt wird, wird sie zu einem, oft teuren, Misserfolg."

Dadurch sinkt die Zeit, die Mitarbeiter hierfür aufwenden müssen. Zudem werden bereits Zimmer mit Sprachassistenten und Internet-of- Things-(IoT)-Geräten ausgestattet, damit Patienten in der Lage sind, beispielsweise die Höhe des Bettes selbstständig zu verändern, auch wenn sie bewegungsunfähig sind. Ein weiterer entscheidender Pluspunkt eines vernetzten Systems ist der schnelle Datenaustausch: Informationen über Patienten stehen in der elektronischen Patientenakte (ePA) in Echtzeit zur Verfügung, können mit Kollegen in anderen Häusern oder Gesundheitseinrichtungen geteilt und (anonymisiert) in der Forschung verwendet werden.

Sicherheit und Datenschutz als oberste Priorität

Diese Beispiele zeigen, dass Daten der Schlüssel für die Zukunft der Medizin sind. Doch gerade in Deutschland gibt es – angesichts der Sensibilität dieser Daten – große Bedenken hinsichtlich des Datenschutzes und der Datensicherheit. Dementsprechend müssen Krankenhäuser diesen Aspekten höchste Priorität einräumen. Die DSGVO konkretisiert dabei zum einen die Anforderungen, die für eine Verarbeitung von Gesundheitsdaten erfüllt sein müssen. Im Gegensatz zu einfachen personenbezogenen Daten ist dies nur in Ausnahmefällen überhaupt erlaubt und braucht eine entsprechende Rechtsgrundlage. Zum anderen müssen Krankenhäuser angemessene Maßnahmen treffen, um den digitalen und physischen Schutz der Daten zu gewährleisten. Dazu zählt zum Beispiel die Verschlüsselung von Daten bei der Speicherung und Übertragung sowie eine strenge Zugangskontrolle, um den Zugriff unberechtigter Dritter zu verhindern. Auch müssen die Rechenzentren, in denen die Daten gespeichert und verarbeitet werden, entsprechend geschützt sein – vor Einbruch und Vandalismus, aber auch Feuer, Überschwemmungen oder Stromausfällen.

Eine Möglichkeit, um Patientendaten gewinnbringend einzusetzen und gleichzeitig den Datenschutz zu gewährleisten, sind synthetische Daten. Solche „künstlichen" Daten werden auf Basis vorhandener Datensätze beispielsweise mithilfe von KI generiert. Besonders in den letzten Jahren ist Generative Adversarial Network (GAN) Modeling stark vorangeschritten. Dieses Verfahren erzeugt synthetische Daten, die durch ihre tiefe Vernetzung untereinander einen höheren Mehrwert für Analysen bieten. Dank derartiger Nachahmungen elektronischer Gesundheitsakten für nicht existierende Patienten können Forscher diese Informationen nutzen, ohne gegen Datenschutzgesetze zu verstoßen. Wichtig ist hierbei jedoch zu vermeiden, dass echte Patientendaten in die künstlichen einfließen. Synthetische Daten können somit Forschung nicht nur in einem größeren Maßstab ermöglichen, sondern sie auch beschleunigen.

Darüber hinaus hat auch die Entwicklung digitaler menschlicher Zwillinge sowohl Diagnostik und Forschung als auch mögliche Behandlungsmaßnahmen erheblich verbessert. Derartige Simulationen des menschlichen Körpers sind hochgradig präzise und geben medizinischen Fachkräften die Möglichkeit, genauere Empfehlungen auszusprechen, die auf die jeweiligen spezifischen Bedürfnisse ihrer Patienten zugeschnitten sind.

Ein gemeinsamer Weg zur Digitalisierung

Neben diesen sicherheitsrelevanten Faktoren kommen auf Krankenhäuser auch organisatorische Herausforderungen zu. Allen voran wird es hierbei um die Fragen gehen, welche neuen Tools und Anwendungen eingeführt werden sollen und wie sichergestellt werden kann, dass Mitarbeiter und Patienten sie akzeptieren. Denn eine Lösung kann in der Theorie noch so viele Vorteile bieten, wenn sie nicht genutzt wird, wird sie zu einem, oft teuren, Misserfolg. Daher sollten Krankenhaus- und IT-Verantwortliche, wenn möglich, gemeinsam mit der Belegschaft evaluieren, welche Lösungen den größten Nutzen versprechen. Ein solches Vorgehen kann auch etwaige Ängste vor dem Jobverlust nehmen, welche durch die Fortschritte bei KI-Systemen oft aufkommen, und klarstellen, dass Technologie eine Unterstützung, nicht Ersatz sein soll. Trainings sollten dabei immer Bestandteil der Einführung neuer Anwendungen sein, damit die Mitarbeiter Unterstützung bei der Einarbeitung erhalten und nicht überfordert werden.

Vor allem muss ein Krankenhaus am Ende aber ein Ort der zwischenmenschlichen Interaktion sein und bleiben. Die Digitalisierung kann einen wichtigen Beitrag leisten, um diese nicht nur zuverbessern, sondern auch mehr Zeit hierfür freizuräumen. Dafür darf aber nicht einfach um des Digitalisierens willen digitalisiert werden, sondern immer mit Blick darauf, was für die Menschen einen echten Mehrwert bringt.

Optimierung des Patientenworkflows: Herausforderungen und Chancen für die IT-Infrastruktur

Die Digitalisierung im Gesundheitswesen bietet zahlreiche Möglichkeiten zur Optimierung des Patientenworkflows und der organisatorischen Effizienz. Doch um diese Potenziale auszuschöpfen, müssen Krankenhaus-IT-Abteilungen entsprechend gerüstet sein und sowohl technische als auch organisatorische Voraussetzungen erfüllen. In diesem Fachartikel werden die wesentlichen Aspekte der Konzeption und Inbetriebnahme eines solchen Projekts beleuchtet, mögliche Vorbehalte diskutiert und Empfehlungen für eine erfolgreiche Umsetzung gegeben. Von Flynn Herbst ist IT-Berater bei terraconnect.

Konzeption und Inbetriebnahme

Eine sorgfältige Planung und Konzeption sind entscheidend für den Erfolg eines Projekts zur Optimierung des Patientenworkflows. Dabei sollten folgende Schritte berücksichtigt werden:

- Analyse der aktuellen Prozesse: Durch eine systematische Analyse der bestehenden Abläufe können Schwachstellen identifiziert und gezielte Verbesserungsmaßnahmen entwickelt werden.
- Definition von Zielen und Kennzahlen: Klare Zielsetzungen und messbare Erfolgskriterien sind notwendig, um den Fortschritt des Projekts zu überwachen und sicherzustellen, dass die gewünschten Ergebnisse erreicht werden.
- Auswahl der Technologien: Bei der Auswahl von Technologien zur Automatisierung und Selbstbedienung sollte darauf geachtet werden, dass sie herstellerneutral und interoperabel sind, um eine einfache Integration in die bestehende IT-Infrastruktur zu ermöglichen.
- Implementierung und Schulung: Um die Akzeptanz der neuen Prozesse und Technologien zu erhöhen, ist es wichtig, das Personal frühzeitig einzubeziehen und entsprechend zu schulen.

Voraussetzungen der Krankenhaus-IT und Aufgabenverteilung

Die Verbesserung der organisatorischen Effizienz hängt maßgeblich von der Fähigkeit der Krankenhaus-IT ab, die notwendige Infrastruktur und Unterstützung bereitzustellen. Dazu gehören:

- Datensicherheit und Datenschutz: Die IT-Abteilung muss sicherstellen, dass die Daten der Patienten und Mitarbeiter geschützt sind und die geltenden Datenschutzbestimmungen eingehalten werden.
- Integration und Interoperabilität: Die IT-Systeme sollten nahtlos miteinander kommunizieren können, um einen reibungslosen Informationsfluss zwischen den verschiedenen Abteilungen zu gewährleisten.
- Skalierbarkeit und Flexibilität: Die IT-Infrastruktur sollte in der Lage sein, sich an veränderte Anforderungen anzupassen, um zukünftige Erweiterungen und Anpassungen des Projekts zu ermöglichen.

Vorbehalte, Ablehnung und interdisziplinäre Verantwortung

Vorbehalte gegenüber der Automatisierung und Selbstbedienung können vielfältig sein, etwa aufgrund von Datenschutzbedenken, Sorgen um den Arbeitsplatzverlust oder mangelndem Vertrauen in die Technologie. Um diese Bedenken zu entkräften, sollten die Vorteile wie gesenkte Kosten, reduzierte Wartezeiten und verbesserte Patientenversorgung betont werden. Eine transparente Kommunikation und die Einbindung aller Beteiligten sind hierbei entscheidend.

Die interdisziplinäre Verantwortung für die Projektumsetzung liegt sowohl bei der Krankenhausleitung als auch bei den IT-Verantwortlichen und den beteiligten Fachabteilungen. Eine enge Zusammenarbeit und regelmäßiger Austausch sind unerlässlich, um die unterschiedlichen Perspektiven zu berücksichtigen und eine erfolgreiche Implementierung zu gewährleisten.

Steigerung der Effizienz und Patientenzufriedenheit durch Automatisierung im Krankenhaus

Die Optimierung des Patientenworkflows im Krankenhaus durch Automatisierung bietet große Chancen zur Steigerung der Effizienz und Patientenzufriedenheit. Um diese Potenziale zu nutzen, müssen Krankenhaus-IT-Abteilungen die notwendigen Voraussetzungen schaffen und in enger Zusammenarbeit mit den Fachabteilungen und der Krankenhausleitung agieren. Durch eine sorgfältige Planung, eine offene Kommunikation und die Berücksichtigung der Bedenken aller Beteiligten kann ein solches Projekt erfolgreich umgesetzt und nachhaltige Verbesserungen im Patientenworkflow erreicht werden.

Dieser Artikel enthält Teile der Erkenntnisse des Kongresses der AHIME/Entscheiderfabrik vom 24.05. – 25.05. in Neuss. Titel des Workshops war „Patientenpartizipation durch Self-Services als win-win-Situation für Patienten und Leistungserbringern“.

Flynn Herbst ist IT-Berater bei der terraconnect GmbH & Co. KG, wo er die Prozessoptimierung verantwortet.

When life
becomes digital.

the i engineers

Mit unseren Portalen haben Sie alles im Griff.

Mobile Portallösungen von *the i-engineers* unterstützen Patient*innen, Zuweisende und Krankenhauspersonal.

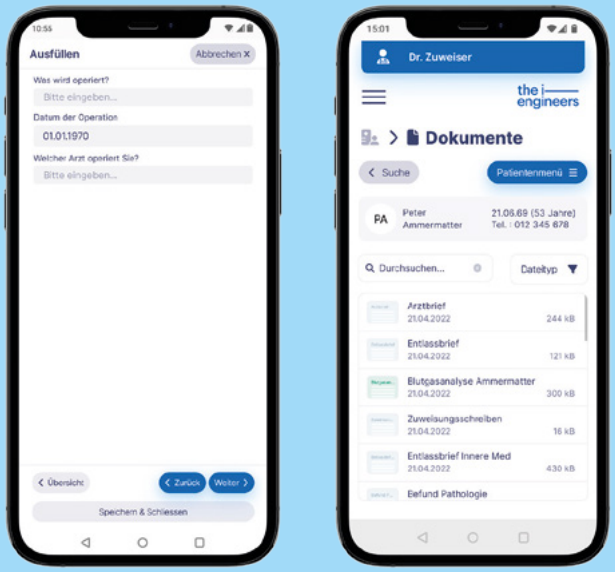
Unser Patientenportal ist ein nützlicher Begleiter vor, während und nach einem Krankenhausaufenthalt. Nicht nur die Patient*innen, sondern auch das Krankenhaus profitiert von der Einführung da vormals manuelle Prozesse im Bereich der Patient*innen Koordination effizient digitalisiert werden können.

Unser Zuweiserportal unterstützt die Kommunikation mit den niedergelassenen Ärzt*innen über einen gesicherten Kanal. Mit der App oder über den Browser können Sie Ihren wichtigsten Geschäftspartnerschaften digitale Services anbieten.

Unser Mitarbeiterportal erhöht die Zufriedenheit in der Belegschaft und schafft neue Wege zu mehr Effizienz und Transparenz. Ermöglichen Sie Ihren Teams den Zugang zu relevanten und persönlichen Informationen, wie zum Beispiel Schichtpläne, Lohnabrechnung, Urlaubsanträge und binden Sie Mitarbeitende in digitale Prozesse ein.

Überzeugen Sie sich selbst von unseren Portallösungen, testen Sie unsere Live Demos auf unserer Website und kontaktieren Sie uns unter sales@tie.ch

Beispielansicht Patientenportal & Zuweiserportal



health engine

Unsere Portale
Drei von 40+ Modulen

Hier geht's zur
Webseite & unseren
Live Demos

Klinische Entscheidungsunterstützung: Behandlungsteam aus zwei Welten

Klinische Entscheidungsunterstützungssysteme (KEUS) helfen medizinischem Personal bei Diagnosestellung und Therapie und können durch Fehlervermeidung erheblich zur Versorgungsqualität beitragen. Das Leistungsspektrum reicht von einfachen Warnhinweisen bis hin zu konkreten Diagnose- und Therapievorschlägen.

Der erfolgreiche Einsatz von KEUS hängt entscheidend davon ab, diese gut in den Arbeitsalltag der medizinischen Fachkräfte einzubinden. Dabei spielt unter anderem der Grad der Integration in bereits verwendete Systeme eine große Rolle. Von Dr. Florian Loga, Manager, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH, Ludwig Babl, Arzt & Informatiker, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH

Fehler im Krankenhaus müssen eingeplant und abgefangen werden

In jedem Krankenhaus passieren Fehler. Es werden falsche Diagnosen gestellt, falsche Therapien ausgewählt oder richtige Therapien falsch durchgeführt, z. B. durch Verabreichung einer falschen Medikation. Im Nachhinein und isoliert betrachtet, wirken solche Fehler oft unerklärlich. Wie kann es passieren, dass es nicht gelingt, die richtige Tablette zu verabreichen? Wieso wurde bei einem klassischen Lehrbuchfall die falsche Diagnose gestellt? Dabei wird übersehen, dass medizinisches Personal oft mit einem hektischen Arbeitsumfeld konfrontiert ist. Ständig klingelt irgendwo ein Alarm, ein Notfall muss sofort behandelt werden oder das Telefon läutet. Abgesehen davon sind lange Arbeitszeiten keine Seltenheit. Die menschliche Leistungsfähigkeit und Aufmerksamkeitsspanne sind jedoch begrenzt. Dass unter solchen Umständen Fehler passieren, muss eingeplant und so gut wie möglich abgefangen werden.

KEUS unterstützen beim Diagnostizieren und Therapieren von Krankheiten

Ein wichtiger Baustein zur Reduktion von menschlichen Fehlern können in Zukunft klinische Entscheidungsunterstützungssysteme sein. Dabei handelt es sich um Systeme, die auf unterschiedliche Art und Weise medizinische Fachkräfte beim Stellen von Diagnosen sowie Finden und Durchführen von Therapien unterstützen. Vergleichsweise einfache Hilfestellungen können darin bestehen, verordnete Medikamente auf ihre Plausibilität hin zu überprüfen. Widerspricht ein Medikament im System hinterlegten Allergien, passt ein potenziell besonders gefährliches Medikament nicht zu den Diagnosen oder liegen gravierende Wechselwirkungen mit anderen Medikamenten vor? In solchen Fällen kann ein Warnhinweis eine lebensrettende Hilfe sein. Deutlich komplexer ist die Situation, wenn vom KEUS auch Vorschläge zu Diagnosen oder Therapien geliefert werden. Es gibt aktuell solche Systeme beispielsweise für Brustkrebserkennung, zur Diagnose von diabetischer Retinopathie und für viele weitere Anwendungsfälle. Diese Systeme basieren oft auf der Auswertung riesiger Datenmengen und maschinellem Lernen und werden vermutlich in den nächsten Jahren noch deutlich besser werden.

Dr. Florian Loga, Manager, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH

Voraussetzungen für den Einsatz von KEUS

Die fachliche Korrektheit von Diagnose- und Behandlungsvorschlägen eines KEUS ist eine Grundvoraussetzung dafür, dass ihr Einsatz überhaupt in Betracht gezogen werden kann. Daneben hängt der erfolgreiche Einsatz entscheidend davon ab, diese gut in den Arbeitsalltag der medizinischen Fachkräfte einzubinden. Dazu muss schon bei der Entwicklung von KEUS darauf geachtet werden, welchen Arbeitsprozess diese später unterstützen sollen. Es reicht nicht, nur die richtige Information zu liefern. Sie muss auch genau zum richtigen Zeitpunkt kommen. Diagnosevorschläge sollten zum Beispiel genau dann geliefert werden, wenn Diagnosen gestellt und in die Patientenakte eingetragen werden. Es sehnt sich auch niemand im Krankenhaus nach einer zusätzlich zu bedienenden Anwendung, bei der man sich womöglich auch noch extra anmelden muss. Das Unterstützungssystem sollte also so tief wie möglich in bereits vorhandene Systeme integriert werden. KIS und PDMS bieten sich hier an, da dort ohnehin alle vom System benötigten Patienteninformationen hinterlegt sind. Ist ein KEUS nicht als fest in diese Systeme integriertes Funktionsmodul umgesetzt, sondern als extra Subsystem, so müssen die nötigen Schnittstellen bei KIS und PDMS vorliegen, damit die Patienteninformationen automatisiert vom KEUS verarbeitet werden können. Hierzu ist schon im Vorfeld bei der Anschaffung von KIS und PDMS darauf zu achten, dass die richtigen Schnittstellen im Lieferumfang enthalten sind. Besonders die ISIK und HL7 Standards werden hierbei in Zukunft vermutlich weiter an Bedeutung gewinnen. Des Weiteren sollten die Vorschläge zu Diagnosen oder Therapien des KEUS auch möglichst gut erläutert werden. Ein Minimum ist hier die Kenntlichmachung oder Auflistung von Daten, auf denen ein Vorschlag beruht. Die Vorschläge und Warnungen müssen auch in vernünftiger Anzahl ausgegeben werden. Es nützt nichts, wenn pro Patient 30 Empfehlungen erscheinen. Solch eine Flut würde im Arbeitsalltag sicher einfach ignoriert werden. Entscheidend ist auch, dass der Mensch immer das letzte Wort hat und Vorschläge vom KEUS auch ignorieren kann. Um Hemmschwellen auf Seiten des medizinischen Personals bei der Verwendung von KEUS abzubauen, sollten diese im Vorfeld genau über den Funktionsumfang sowie Stärken und Schwächen des Systems unterrichtet werden. Sehr hilfreich für spätere Nutzerinnen und Nutzer ist zudem die Möglichkeit, sich zuerst anhand von virtuellen Beispielpatienten in einer geschützten Umgebung mit dem KEUS vertraut machen zu können.

Ludwig Babl, Arzt & Informatiker, Curacon GmbH Wirtschaftsprüfungsgesellschaft und Sanovis GmbH

Mensch und Maschine ergänzen sich gegenseitig

KEUS sollen dabei das medizinische Personal nicht ersetzen. Mensch und Maschine können sich gegenseitig aber hervorragend ergänzen. Dieses Potential hat auch der Gesetzgeber erkannt und KEUS als Fördertatbestand 4 in das Krankenhauszukunftsgesetz aufgenommen. Computer machen keine Flüchtigkeitsfehler und verkennen niemals schon dagewesene Standardsituationen. Auf der anderen Seite haben sie Schwächen beim Erfassen und Analysieren von komplexen und unbekannten Situationen. Zahlreiche Menschen haben mehr als eine Krankheit und nehmen teilweise auch sehr viele Medikamente gleichzeitig. Selbst in riesigen Datenmengen finden sich dann nur wenige vergleichbare Fälle und ein Computersystem kommt an seine Grenzen. Auch die Kommunikation zwischen Mensch und Maschine ist nach wie vor ein großes Thema. Gerade im Zuge von medizinischen Behandlungen müssen inhaltlich und emotional sehr herausfordernde Gespräche geführt werden, wobei ein einfühlsamer Mensch unabdingbar ist.

Fazit

Ein Behandlungsteam aus Mensch und Unterstützungssystem kann das Beste aus beiden Welten vereinen. Flüchtigkeitsfehler werden stark reduziert und Standardfälle zuverlässig erkannt. Gleichzeitig kann mit neuen, komplexen Situationen und herausfordernden Gesprächen umgegangen werden. Diese Zusammenarbeit kann die Patientensicherheit erheblich erhöhen und somit die Behandlungsqualität nachhaltig steigern.

Infrastruktur und IT-Systeme für technologische Innovationen in Pflegearbeit

Um technologische Innovationen in der Pflegearbeit erfolgreich zu integrieren, ist eine solide Infrastruktur und entsprechende IT-Systeme erforderlich. Die Integration technologischer Innovationen erfordert eine umfassende Planung, Schulung und kontinuierliche Anpassung. Durch eine sorgfältige Integration können technologische Lösungen dazu beitragen, die Effizienz zu steigern, die Qualität der Pflege zu verbessern und die Arbeitsbelastung der Pflegekräfte zu verringern. Hier sind einige Aspekte, die bei der Einrichtung und Pflege der Infrastruktur und IT-Systeme berücksichtigt werden sollten.

1 Netzwerkkonnektivität: Eine zuverlässige Netzwerkkonnektivität ist entscheidend, um eine reibungslose Kommunikation und Datenübertragung zu gewährleisten. Pflegeeinrichtungen sollten über eine leistungsfähige und sichere Netzwerkinfrastruktur verfügen, die eine ausreichende Bandbreite für den Datenverkehr bietet.

2 Hardware-Ausstattung: Es ist wichtig, die richtige Hardware für die technologischen Anwendungen bereitzustellen. Dazu gehören beispielsweise Computer, Laptops, Tablets und mobile Geräte wie Smartphones. Die Hardware sollte den Anforderungen der Pflegearbeit gerecht werden und den Einsatz von Softwareanwendungen und elektronischen Systemen ermöglichen.

3 Elektronische Patientenakten (EPA): Die Implementierung von elektronischen Patientenakten erfordert ein geeignetes IT-System zur Erfassung, Speicherung und Verwaltung der Patientendaten. Es sollten angemessene Sicherheitsmaßnahmen getroffen werden, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

4 Softwarelösungen: Neben elektronischen Patientenakten können verschiedene Softwarelösungen zur Unterstützung der Pflegearbeit eingesetzt werden. Dazu gehören beispielsweise Terminplanungs- und Koordinationssysteme, Medikamentenverwaltungssysteme, Kommunikations- und Kollaborationstools sowie Datenanalyse- und Berichterstattungssysteme. Die Auswahl geeigneter Software sollte die spezifischen Anforderungen der Pflegeeinrichtung berücksichtigen.

5 Datenschutz und Sicherheit: Der Schutz von sensiblen Patientendaten ist von größter Bedeutung. Es sollten entsprechende Sicherheitsmaßnahmen ergriffen werden, um unbefugten Zugriff, Datenlecks und Cyberangriffe zu verhindern. Dies umfasst den Einsatz von Verschlüsselungstechnologien, Zugriffskontrollen, regelmäßige Sicherheitsaudits und die Einhaltung geltender Datenschutzbestimmungen.

6 Schulung und Support: Eine angemessene Schulung der Pflegekräfte im Umgang mit den IT-Systemen und technologischen Innovationen ist unerlässlich. Es sollten Schulungsprogramme angeboten werden, um das Verständnis für die Nutzung der Systeme zu fördern und die Pflegekräfte bei Fragen oder Problemen zu unterstützen.

Die Implementierung und Wartung einer robusten Infrastruktur und geeigneter IT-Systeme erfordert eine sorgfältige Planung, Ressourcenallokation und Zusammenarbeit mit IT-Experten. Durch eine solide technologische Grundlage können die Vorteile der technologischen Innovationen in der Pflegearbeit voll ausgeschöpft werden.

Souveränität durch ganzheitliches Datenmanagement.

Über 1.000 Krankenhäuser vertrauen auf
die Lösungen und Services der DMI Gruppe.

D·M·I gefyra Health·Comm

www.dmi.de

FHIR ist kein Zauberwort

Interoperabilität im Gesundheitswesen ist für Healthcare-Akteure mit Weitblick der Kernpunkt. Notwendig sind sektorenübergreifend einheitliche, verbindliche Vorgaben für alle. Herausforderungen der Digitalisierung sind allein mit dem Schreiben neuer Gesetze, Regularien und Spezifikationen nicht zu lösen, man muss sie auch implementieren. Die internationale FHIR-Community macht es vor. Aspekte für einen flächendeckend harmonisierten Datenaustausch erörtert Simone Heckmann, Geschäftsführerin / CEO, Gefyra GmbH, im Interview mit dem Krankenhaus IT Journal.

Bricht mit der Einführung von HL7 FHIR eine neue Ära der Interoperabilität im Gesundheitswesen an?

Simone Heckmann: Ja, davon bin ich überzeugt! Mit HL7 FHIR steht uns erstmals ein moderner internationaler Standard zur Verfügung, der das gesamte Gesundheitswesen berücksichtigt (ambulante und stationäre Versorgung, Forschung, öffentlicher Gesundheitsdienst, Kostenträger-Kommunikation, regulatorischer Datenaustausch etc.) alle gängigen Formen des Datenaustausches beherrscht (nachrichtenbasierte, dokumentenbasierte sowie abfragebasierte Kommunikation), aber auch das Bedürfnis der Industrie nach einfachen, modernen, webbasierten Lösungen erfüllt. Damit haben wir die Möglichkeit, den Datenaustausch im Gesundheitswesen flächendeckend zu harmonisieren und wegzukommen von kleinteiligen Insellösungen.

Wie weit akzeptieren Healthcare-Hersteller Interoperabilität? Welche Benefits gibt es für die Industrie?

Simone Heckmann: Es kommt drauf an. Es gibt immer Hersteller, die Daten haben und Hersteller, die Daten brauchen. Primärsystem-Hersteller, insbesondere diejenigen, die monolithische Systeme ("alles aus einer Hand") anbieten, sind der Interoperabilität gegenüber meist zurückhaltend, Subsystem-Hersteller hingegen sind auf Interoperabilität angewiesen und sehen in FHIR eine willkommene Lösung, die zu modernen Architekturen passt. Ich habe jedoch immer häufiger auch mit Monolithen zu tun, die für die interne Kommunikation zwischen ihren verschiedenen Modulen - die ja historisch betrachtet häufig auch nichts anderes sind, als Subsysteme von aufgekauften Herstellern - eine nachhaltige und flexible Lösung suchen und auf diesem Wege ebenfalls bei HL7 FHIR landen.

Simone Heckmann, Geschäftsführerin / CEO, Gefyra GmbH, Leiterin Technisches Komitee FHIR (HL7 Deutschland e.V.), FHIR Core Team Member: „Wir stehen bei der Digitalisierung des Gesundheitswesen vor enormen Herausforderungen, die allein mit dem Schreiben neuer Gesetze, Regularien und Spezifikationen nicht gelöst werden können; man muss sie auch implementieren!“

Muss Interoperabilität der Gesetzgeber vorschreiben? Oder regelt das der Markt?

Simone Heckmann: Ich stehe der Idee, so etwas den Markt regeln zu lassen, kritisch gegenüber. Oft hat dies zur Konsequenz, dass der Lösungsvorschlag des Herstellers mit der größten Marktmacht gewinnt, unabhängig davon, ob es sich dabei um die technisch ausgereifteste bzw. “beste” Lösung handelt (man denke an “Betamax vs. VHS”). Weiterhin stehen wir vor der Herausforderung, dass das Gesundheitswesen bei weitem nicht so stark globalisiert und internationalisiert wäre, als dass wir internationale Standards ohne weiteres Zutun in Deutschland nutzen könnten.

Ganz im Gegenteil: Flexibilität und Offenheit für (nationale) Anpassungen gehören zu den grundlegendsten Eigenschaften internationaler Standards. Dies wiederum erfordert jedoch eine nationale Vereinheitlichung dieser Anpassungen. Biegt sich jeder Hersteller den Standard nach eigenem Ermessen zurecht, kann die Interoperabilität innerhalb Deutschlands nicht gewährleistet werden.

Ich sehe es als ganz wichtige Aufgabe des Gesetzgebers, hier klare Zuständigkeiten zu schaffen, für bundesweit und sektorenübergreifend einheitliche Vorgaben zu sorgen und diese für alle verbindlich zu machen.

Wie weit sind Krankenhäuser technologisch, organisatorisch und personell auf Interoperabilität vorbereitet? Was ist zu optimieren?

Simone Heckmann: Kompetenz zum Thema FHIR aufzubauen, auch wenn aktuell in den Kliniken zum Teil noch keine FHIR-Schnittstellen im Einsatz sind, ist das Gebot der Stunde! FHIR ist kein Zauberwort, das - dreimal in den Kommunikationsserver gesprochen - alle Interoperabilitätsprobleme auf magische Weise löst. Wie eingangs gesagt: FHIR ist eine Technologie, die auf viele verschiedene Weisen genutzt werden kann und nicht alle davon sind untereinander kompatibel. Ein Hersteller muss wenig tun, um sein System als “FHIR konform” bezeichnen zu können. Für Entscheider in den Kliniken ist es wichtig, die richtigen Fragen stellen, Anforderungen präzisieren und Spezifikationen lesen zu können, um beurteilen zu können, ob ein System, das FHIR-Konformität verspricht, tatsächlich den eigenen Interoperabilitäts-Anforderungen genügt.

Welche neuen Risiken für Sicherheit und Datenschutz von Gesundheitsdaten bringt Interoperabilität? Wie lässt sich die Sicherheit von Gesundheitsdaten sicherstellen?

Simone Heckmann: Die Verwendung von HL7 FHIR hat beim Thema Datenschutz und Datensicherheit einen entscheidenden Vorteil: Das Rad muss nicht neu erfunden werden. FHIR setzt auf die Verwendung von etablierten und erprobten IT-Standards, wie zum Beispiel das HTTP-Protokoll mit TLS-Verschlüsselung, oder den OAUTH2-Standard zur Benutzerauthentifikation. Das hat den Vorteil, dass die Entwickler auf langjährige Erfahrungen anderer Branchen und fertige Softwarebibliotheken zurückgreifen können, die gegen Angriffe gehärtet sind.

Ist Interoperabilität als Standardisierungsprozess Innovationshemmnis oder Anschub für technische Weiterentwicklungen?

Simone Heckmann: HL7 FHIR basiert auf dem Baukastenprinzip. Es gibt verschiedene Informationsbausteine, um z.B. Patientenstammdaten, Diagnosen, Prozeduren oder Messwerte abzubilden. Diese können dann in unterschiedlichen Kontexten immer wieder verwendet werden, z.B. um die Diagnosen eines Patienten für ein Subsystem abrufbar zu machen oder die Patientenstammdaten an ein Messgerät zu übermitteln oder um daraus einen strukturierten Entlassbrief zu erstellen. Einmal implementiert, kann eine Vielzahl von Prozessen unterstützt werden, ohne dass dafür ein erheblicher Mehraufwand erforderlich ist.

Weiterhin ermöglicht die abfragebasierte Kommunikation erstmals die einfache Integration von leichtgewichtigen, webbasierten und mobilen Applikationen in die Krankenhaus-Umgebung. Zum Beispiel um wichtige Patienteninformationen auf die Smartphones der Ärzte zu bringen, oder um moderne, webbasierte Lösungen standardisiert in KIS-Systeme zu integrieren ("Fremdaufruf"). Damit sind Krankenhäuser künftig schneller in der Lage, innovative Lösungen in ihre bestehende Umgebung integrieren und den Anwendern zur Verfügung stellen zu können.

Wie ist „Kapitalismus – Sozialismus in der Datenwelt" zu verstehen? Welche Sichtweisen und Perspektiven zeigen sich?

Simone Heckmann: „Daten sind das neue Öl". Unterwirft man Daten den Gesetzmäßigkeiten des freien Marktes, dann werden sie auch wie Öl gehandelt, d.h. eine kleine, aber mächtige Elite derjenigen, die auf den Quellen sitzen, entscheidet über Zugang und Preis. Dabei gehören Gesundheitsdaten gar nicht den Systemen, in denen sie gespeichert sind, sondern dem Patienten, den Ärzten, der Solidargemeinschaft der Versicherten, dem Gesundheitswesen. Kein Hersteller sollte das Recht oder die Macht haben, den Zugang zu diesen Daten zu behindern. Ausgerechnet in den USA, denen man ja insbesondere im Gesundheitswesen gerne mal Turbokapitalismus unterstellt, ist man hier ein ganzes Stück weiter. Dort wurde mit dem 21st Century Cures Act von 2016 eine wichtige gesetzliche Grundlage geschaffen, die es Gesundheitsdienstleistern und Softwareherstellern untersagt, Patienten den Zugang zu ihren Gesundheitsdaten zu verweigern. Hierzulande fordert die DSGVO zwar ähnliches, aber weitaus weniger konkret als es in der "Information Blocking"-Richtlinie des Cures Act der Fall ist. (1)

Einen weiteren Grund, weshalb wir in der Gesundheits-IT "mehr Sozialismus wagen" müssen, ist ganz praktischer Natur: Wir stehen bei der Digitalisierung des Gesundheitswesen vor enormen Herausforderungen, die allein mit dem Schreiben neuer Gesetze, Regularien und Spezifikationen nicht gelöst werden können; man muss sie auch implementieren! Und dabei stehen wir sowohl vor dem Problem des Fachkräftemangels in der IT als auch den explodierenden Kosten, die von Softwareherstellern auf die Leistungserbringer, von den Leistungserbringern auf die Kostenträger, von den Kostenträgern auf die Versicherten umgelegt werden. Dabei gibt es in der IT-Branche längst ein etabliertes Prinzip, mit dem gemeinsame Probleme mit gemeinsamer Kraft gelöst werden können: Das Zauberwort heißt "Open Source". Anstatt dass hunderte von Entwicklern hundert mal dasselbe Problem lösen, können zehn Entwickler das gleiche Problem einmal gemeinsam lösen und allen anderen zur Verfügung stellen. Das Ergebnis geht schneller, benötigt weniger personelle Ressourcen, verursacht weniger Kosten, liefert eine bessere Softwarequalität und ist robuster als Einzelentwicklungen.

Die internationale FHIR-Community macht es vor und liefert einen großen Pool an frei verfügbaren Tools und Bibliotheken. Ich hoffe, dass es uns gelingt, den Solidaritätsgedanken auf die Deutsche Community zu übertragen und den Gesetzgeber dafür zu sensibilisieren, dass die Investition in Open Source-Lösungen einen wichtigen Beitrag leisten kann, die Kosten der Digitalisierung im Griff zu behalten.

(1) **www.healthit.gov/topic/information-blocking**

Teil 2: Umsetzung der 80001-1:2023-02

Risiken vernetzter Medizinprodukte

Nach Teil 1: „Gesetze und Standards“ beschreibt Teil 2 die Umsetzung anhand eines fiktiven PDMS-Projektes mit dem Aufbau der Risikomanagement-Akte und der Erstellung des Risikomanagementplans. In Teil 3 folgen Risikoidentifizierung, -Minimierung und -Bewertung, und in Teil 4 schauen wir auf Assurance Cases und Abschlussbericht.
Die Übergangsfrist zur Anwendung der DIN EN IEC 80001-1:2023-02 endet am 26.10.2024. Konformität ist nur noch durch aktive Beschlussfassung durch das TOP-Management der Gesundheitseinrichtung möglich. Für alle neuen Projekte sollte sie daher ab sofort beachtet werden. Von Dipl.-Ing. Gabriele Münker und Dr. Udo Jendrysiak

Die DIN EN ISO 80001-1 richtet sich an Gesundheitsorganisationen und unterstützt diese beim Aufbau eines nachhaltigen Risikomanagements, so dass über alle Lebenszyklen ihres medizinischen IT-Netzwerkes hinweg, angemessene Risikobewertungen durchgeführt und systematisch risikominimierende Maßnahmen festgelegt und umgesetzt werden.

Gründe für die Revision

In [1] beschreiben MacMahon, Cooper und McGaffery, dass international drei Problembereiche in der Umsetzung der IEC 80001-1 festgestellt wurden. Diese lagen im Top-Management der Gesundheitseinrichtung, der Zusammenarbeit von IT und Medizintechnik und zu hoher Komplexität. Die Neuausgabe hat diese Kritik aufgegriffen. Sie enthält nun ein Rahmenkonzept und erleichtert u.a. auch damit die Umsetzung.

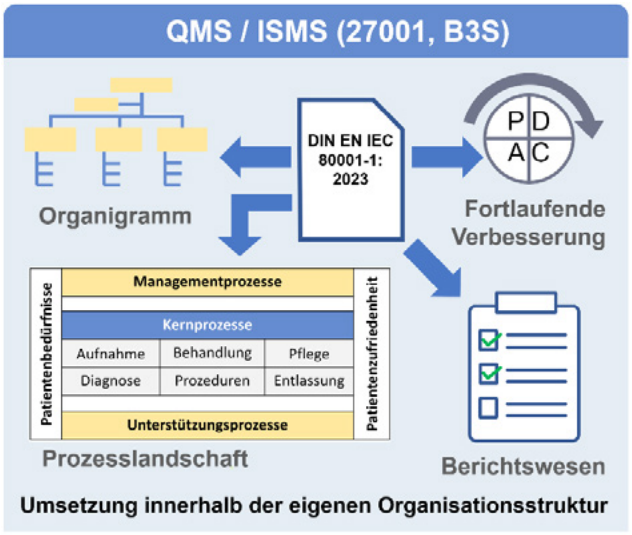
Vorteile der Neuausgabe aus unserer Sicht

- Bessere Verständlichkeit
- Gute Verknüpfbarkeit mit bestehenden organisatorischen Strukturen (Organigramm, Prozesse)
- Umfang der Risikoanalyse orientiert sich an den Lebenszyklen des medizinischen IT-Netzwerks
- Übersicht der Soll-Anforderungen
- Verbesserte Rechtssicherheit
- Rahmenkonzept (Framework)
- Genauere Vorgaben der Informationsbereitstellung von Herstellern und Lieferanten an den Betreiber
- Einige praktische Vorlagen

Unterschrift der Geschäftsführung

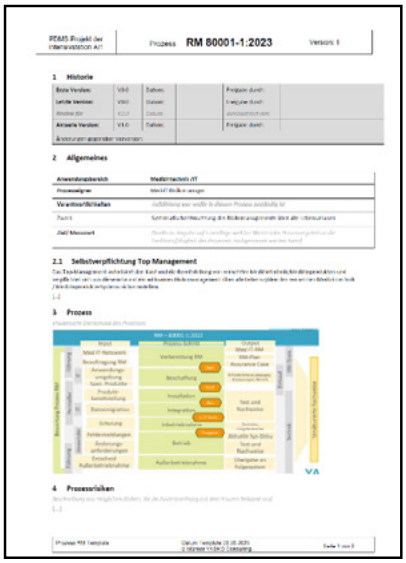
Die Norm beginnt mit dem Hinweis, „Gesundheitsversorgungsorganisationen sind auf sichere, effektive und geschützte Systeme als geschäftskritische Faktoren angewiesen.“ Das Rahmenkonzept (Kapitel 5) spricht daher zu allererst die oberste Führungsebene der Organisation an. Sie ist dafür verantwortlich, dass das Risikomanagement während des gesamten Lebenszyklus des vernetzten Systems umgesetzt wird.

Konkret bedeutet das:



Integration des Risikomanagements in QMS/ISMS

Autor Dr. Udo Jendrysiak



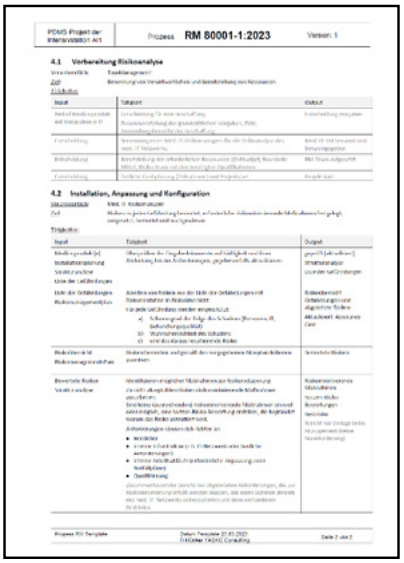


Abbildung: Auszug aus einem Risikomanagement-Prozess

Geschäftsführung/Vorstand des Krankenhauses müssen den Risikomanager einsetzen, beauftragen und mit den erforderlichen internen und externen Ressourcen ausstatten.

Abschließend ist es wieder die Geschäftsführung, die anhand von Risikoakte und Ergebnisbericht entscheiden muss, ob das Gesamtsystem in Betrieb genommen und etwaige Restrisiken in Kauf genommen werden. Diese Aufgaben können nicht einfach an die Linienmanager oder den Risikomanager delegiert werden.

Risikomanagementprozess

Der erste Schritt des frisch beauftragten „IT-Gesundheits-Risikomanagers" ist es, den Prozess zu starten und ein Team aufzustellen. Das in der 80001-1 beschriebene Risikomanagement basiert auf den grundlegenden Prinzipien der DIN EN ISO 31000. Bei erstmaliger Umsetzung eines Risikomanagements gemäß 80001-1, sollte unter Einbezug des Qualitätsmanagements zuerst ein Prozess „Risikomanagement" erstellt und mit den bestehenden Prozessen und Abläufen in der Gesundheitseinrichtung verknüpft werden, oder ein bereits bestehender Risikomanagementprozess an die Anforderungen der 80001-1:2023 angepasst werden. Der höchste Nutzen kann erzielt werden, wenn bereits in der Phase der Produktauswahl und Beschaffung das Projekt zur Durchführung der Risikoanalyse für das jeweilige med. IT-Netzwerk initiiert wird. So können risikominimierende Anforderungen an Hersteller im Rahmen von Ausschreibungen gestellt werden.

Zentraler Ausgangspunkt der Umsetzung der Norm-Anforderungen sind die bestehenden organisatorischen Randbedingungen in ihrer Gesundheitseinrichtung, die spezifische Situation auf den betroffenen Stationen und die vorgesehene Zweckbestimmung und Anwendung der vernetzten Medizinprodukte.

Risikomanagementteam

Entsprechend wird der Risikomanager ein Team von Mitarbeitenden aus den Fachbereichen IT, Medizintechnik, Qualitätsmanagement und vor allem den klinischen Anwendern aufsetzen: das Risikomanagement-Team, in dem bereichsübergreifend die Risikoanalyse und -Bewertung durchgeführt wird.

Für den Erfolg ihrer Risikobetrachtung sind die Qualifikation und Erfahrung des Risikomanagers und die Zusammensetzung des Risikomanagementteams von Bedeutung.

Der eingesetzte Risikomanager sollte insbesondere Wissen und Erfahrungen im Risikomanagement besitzen, da er die erforderlichen Grundlagen zusammenstellt sowie die Risikoanalyse vorbereitet und moderiert. Das Fachwissen wird im Team von den unterschiedlichen Teammitgliedern bereitgestellt.

Risikomanagement ist immer Teamarbeit, da nur so eine umfassende und fundierte Analyse möglich ist, indem die unterschiedlichen Themen aus mehreren Blickwinkeln betrachtet werden.

Sind erforderliche Qualifikationen in ihrer Einrichtung noch nicht vorhanden, ist es wichtig, den eingesetzten Risikomanager und gegebenenfalls das Team vorher zu qualifizieren oder für den ersten Durchlauf externe Beratung hinzu zu ziehen. Diese Beratung kann Schulungsanteile enthalten, ist aber im Wesentlichen eine Möglichkeit auf einen Erfahrungsschatz zuzugreifen und so die erforderlichen Tätigkeiten sicher und die Risikoanalyse im geplanten Zeitraum durchzuführen.

Risikomanagement-Akte und -Plan

Nun legt der Risikomanager die Risikomanagementakte an, in der alle zur Risikoanalyse gehörenden Dokumente abgelegt werden. Wie bei jedem Projekt wird im nächsten Prozessschritt eine Projektplanung erstellt, hier der sog. Risikomanagementplan.

Der Risikomanagementplan wird in der Akte als eines der ersten Dokumente abgelegt. Der Plan bildet die Grundlage für die Durchführung der Risikoanalyse und enthält alle hierzu erforderlichen Informationen oder verweist auf entsprechende Dokumente.

Zweckbestimmung vernetztes Gesamtsystem

Im fiktiven Beispiel PDMS für eine Intensivstation hat das PDMS natürlich eine Zweckbestimmung des Herstellers. Es fehlt aber die Zweckbestimmung bezogen auf die Anwendung beim Betreiber (z.B. Intensivstation vs. Notaufnahme). Es ist notwendig, diese insbesondere im Hinblick auf einzubindende Medizingeräte zu beschreiben und was mit den

durch die Vernetzung digital vorliegenden Medizingerätedaten geschehen soll – in der Neuaufnahme von Patienten, der Behandlung und auch in der Abrechnung.

Die geplante Anwendung und Zweckbestimmung des med. IT-Netzwerks wird im Risikomanagementplan dokumentiert, wie auch die sicherheitsrelevanten Merkmale, und die besonders wichtigen Leistungsmerkmale, als Grundlage zur anschließenden Ermittlung potentieller Gefährdungen.

Strukturanalyse

Jetzt geht es um den Ort und die Art und Weise der geplanten Nutzung. Es werden alle mit dem PDMS vernetzten Medizingeräte der Station erfasst, sowie die Verfahren und ggf. weitere Software-Anwendungen, die im Umfeld des medizinischen IT-Netzwerkes für die PDMS-Nutzung relevant sind. Dazu werden die Konformitätserklärungen und Schnittstelleninformationen der zu integrierenden Medizingeräte/Medizinprodukte und Medizinprodukt-Software benötigt. Wichtig sind außerdem der Raumplan der Station und eine Systemskizze des zukünftigen med. IT-Netzwerkes.

Mit dieser Strukturanalyse wird jetzt festgestellt, welche der gelisteten Komponenten (Werte = Assets) zum Anwendungsbereich der Risikoanalyse gehören, wie diese zueinander in Beziehung stehen und über welche definierten Schnittstellen die Werte im Anwendungsbereich mit dem Umfeld verbunden oder verknüpft sind. Diese Zusammenhänge sollten zweckmäßigerweise in einer Zeichnung vereinfacht dargestellt werden, auf die man in Workshops/Besprechungen zurückgreifen kann.

Jetzt werden noch Festlegungen zur Einstufung der Eintrittswahrscheinlichkeiten von Gefährdungssituationen und der Einstufung vom Schweregrad möglicher Schäden bei Patienten, Anwendern, sowie Auswirkungen auf die Zuverlässigkeit der Bereitstellung von Gesundheitsdienstleistungen im Risikomanagementplan dokumentiert. Aus der Kombination dieser Risikoakzeptanzkriterien ergibt sich das angenommene Risiko. Visualisiert in einer Matrix. wird festgelegt, welche Risiken als annehmbar eingestuft werden und zu welchen Risiken Maßnahmen zur Risikominimierung erforderlich sind.

Der Risikomanagementplan enthält grundlegende Informationen, Verweise auf relevante Dokumente und eine zeitliche Planung. Wenn der Risikomanagementplan fertiggestellt, genehmigt und gegenüber Vorstand und Risikomanagementteam verfügbar gemacht wurde, kann mit der Durchführung der Risikoanalyse begonnen werden. Hierüber berichten wir in Teil 3 dieser Reihe zur 80001-1:2023.

[1] MacMahon, Silvana Togneri and Cooper, Todd and McCaffery, Fergal (2018) Revising IEC 80001-1: Risk Management of Health Information Technology Systems. Computer Standards & Interfaces. ISSN: 0920-5489. https://eprints.dkit.ie/627/

Autorin Dipl.-Ing. Gabriele Münker

Risikomanagement delegieren: Aufgaben ja – Verantwortung nein

Derzeit werden im Rahmen der KHZG Förderprojekte zahlreiche Patientendatenmanagementsysteme PDMS neu implementiert. Geschäftsführung oder Vorstand eines Krankenhauses kann die Risikomanagement-Aufgaben an die Linienmanager oder den Risikomanager delegieren, nicht aber die Verantwortung. Allerdings haftet die Führung grundsätzlich dafür, dass alle notwendigen Aufgaben - dazu gehört auch das IT-Risikomanagement - ordnungsgemäß erledigt werden.

Die Geschäftsführung eines Krankenhauses kann die Risikomanagement-Aufgaben an die Linienmanager delegieren, indem sie einen strukturierten Ansatz verfolgt und klare Richtlinien und Verantwortlichkeiten festlegt. Einige Schritte machen das Vorgehen anschaulich.

Risikomanagementpolitik entwickeln: Die Geschäftsführung sollte eine klare Risikomanagementpolitik für das Krankenhaus entwickeln. Diese Politik sollte die Ziele, Grundsätze und Verfahren des Risikomanagements festlegen.

Risikomanagementprozess etablieren: Ein strukturierter Risikomanagementprozess sollte definiert werden. Dieser Prozess kann aus den folgenden Schritten bestehen: Risikoerkennung, Risikobewertung, Risikobewältigung und Risikoüberwachung.

Risikomanagement-Rollen und -Verantwortlichkeiten definieren: Die Geschäftsführung sollte klare Rollen und Verantwortlichkeiten für das Risikomanagement festlegen. Dies umfasst die Benennung von Linienmanagern als Risikomanager für ihre jeweiligen Bereiche.

Schulung und Sensibilisierung: Die Geschäftsführung sollte sicherstellen, dass die Linienmanager über die Grundlagen des Risikomanagements informiert sind und die erforderlichen Fähigkeiten und Kenntnisse besitzen. Schulungen und Schulungsmaterialien können verwendet werden, um die Sensibilisierung für Risikomanagementfragen zu fördern.

Kommunikation und Berichterstattung: Die Geschäftsführung sollte klare Kommunikationskanäle für das Risikomanagement etablieren. Linienmanager sollten in regelmäßigen Abständen über Risikomanagementaktivitäten berichten, um einen Überblick über den Status der Risiken in ihren Bereichen zu erhalten.

Überwachung und Bewertung: Die Geschäftsführung sollte den Fortschritt und die Wirksamkeit des delegierten Risikomanagements überwachen und bewerten. Regelmäßige Überprüfungen und Audits können durchgeführt werden, um sicherzustellen, dass die Risiken angemessen identifiziert und bewältigt werden.

Kontinuierliche Verbesserung: Die Geschäftsführung sollte ein System für kontinuierliche Verbesserung implementieren, um das Risikomanagement kontinuierlich zu optimieren. Dies kann die Überprüfung von Prozessen, die Identifizierung von Best Practices und die Implementierung von Verbesserungen umfassen.

Haftung für die Geschäftsführung bleibt bestehen

Befolgt die Geschäftsführung diese Schritte, kann sie die Risikomanagement-Aufgaben erfolgreich an die Linienmanager delegieren und sicherstellen, dass das Krankenhaus angemessen auf potenzielle Risiken reagiert.

Die Geschäftsführung des Krankenhauses haftet grundsätzlich dafür, dass alle notwendigen Aufgaben - dazu gehört auch das IT-Risikomanagement - ordnungsgemäß erledigt werden. Dieser Haftung kann sich die Geschäftsführung nicht entziehen.

Die Geschäftsführung kann Mitarbeiter des Hauses oder externe Fachleute mit der Wahrnehmung bestimmter Aufgaben und Verantwortlichkeiten beauftragen. Das sind dann die Beauftragten, über die ein Krankenhaus üblicherweise auch korrekt Buch führt. Soweit ich weiss sind die Beauftragten jeweils auch über die Webseite einsehbar.

Die Beauftragung einer Person (intern oder extern) als IT-Risikomanager muss formell und schriftlich durch die Geschäftsführung erfolgen. Kernaussage dieses kurzen, einseitigen Dokuments: die Einsetzung des Risikomanagers für ein konkretes, abgegrenztes Projekt, z.B. PDMS auf Intensivstation. Darin enthalten ist auch, dass diese Bestellung zum Risikomanager auf einem Organigramm erscheint und der Risikomanager hierfür direkt unter der Geschäftsleitung geführt wird, nicht als Teil von IT oder MT. Weiter steht darin, dass alle Mitarbeitende, die der Risikomanager in sein Team hinzuzieht, ihn zu unterstützen haben. Enthalten ebenfalls: Wenn Ausbildung oder Coaching/Externe Begleitung erforderlich sind, weil es die erste Umsetzung nach der neuen Norm ist, Bewilligung von Mitteln hierfür.

Wichtig: mit dieser Beauftragung entledigt sich die Geschäftsführung NICHT der Verantwortung für die korrekte Durchführung des Risikomanagements. Der beauftragte IT-Risikomanager muss allerdings - z.B. bei IT-Risikomanagement gemäß ISO 80001 - die in dem Standard vorgesehenen Prozesse durchlaufen und die Durchführung zusammen mit den Ergebnissen transparent dokumentieren.

Generell gilt somit: die Geschäftsführung hat am Ende immer die Verantwortung und haftet. Grobe Fahrlässigkeit auf der Ebene der Beauftragten oder auf Ebene der Geschäftsführung hat entsprechende Folgen - bei der Ebene Geschäftsführung soweit ich weiß auch die persönliche und private Haftung.

Zur Dokumentation: die Beauftragung muss immer schriftlich durch die Geschäftsführung erfolgen. Eine implizite Beauftragung ("Herr / Frau XY, kümmern Sie sich bitte um die Einführung des PDMS inkl. der damit verbundenen Risiken") ist keine formelle Beauftragung.

Kommunikationskanäle, Richtlinien und Schulungen

Die Geschäftsführung eines Krankenhauses kann die Verantwortung für das Risikomanagement grundsätzlich an die Linienmanager übertragen. Das Risikomanagement umfasst die Identifizierung, Bewertung und Steuerung von Risiken, um mögliche Schäden oder negative Auswirkungen auf das Krankenhaus und seine Patienten zu minimieren.

In vielen Organisationen, einschließlich Krankenhäusern, werden Risikomanagementaufgaben auf verschiedene Ebenen der Hierarchie delegiert. Die Geschäftsführung kann strategische Richtlinien und Ziele festlegen und die allgemeine Verantwortung für das Risikomanagement tragen. Sie können jedoch bestimmte Aufgaben und Verantwortlichkeiten an die Linienmanager delegieren.

Die Linienmanager, wie beispielsweise die Leiter der verschiedenen Abteilungen oder Kliniken, können dann für die Umsetzung der Risikomanagementmaßnahmen in ihren jeweiligen Verantwortungsbereichen zuständig sein. Sie identifizieren und bewerten Risiken, entwickeln Maßnahmen zur Risikominderung, überwachen die Wirksamkeit der Maßnahmen und berichten regelmäßig an die Geschäftsführung.

Es ist wichtig, dass klare Kommunikationskanäle, Richtlinien und Schulungen für das Risikomanagement vorhanden sind, um sicherzustellen, dass alle Linienmanager die erforderlichen Kenntnisse und Ressourcen haben, um ihre Aufgaben effektiv zu erfüllen. Die Geschäftsführung behält dabei in der Regel die übergeordnete Aufsicht und trägt letztendlich die Verantwortung für das Risikomanagement im Krankenhaus. Die Übertragung der Verantwortung für das Risikomanagement an die Linienmanager bedeutet jedoch nicht, dass die Geschäftsführung von ihrer Gesamtverantwortung entbunden wird. Sie bleiben weiterhin für die strategische Ausrichtung, Überwachung und Entscheidungsfindung im Zusammenhang mit Risiken im Krankenhaus verantwortlich.

B3S „Medizinische Versorgung“: Risikoobjekte und Risiko-Eigentümer - die Geschäftsführung ist in der Pflicht

Die Sicherheit der informationstechnischen Systeme in den Krankenhäusern muss dauerhaft gewährleistet werden, sie dient in letzter Konsequenz auch der Patientensicherheit. Dazu soll auch die Bereitstellung eines branchenspezifischen Sicherheitsstandards (B3S) im Sinne des § 8a BSI-Gesetzes dienen. Derzeit werden im Rahmen der KHZG Förderprojekte zahlreiche Patientendatenmanagementsystem PDMS neu implementiert. Geschäftsführung oder Vorstand eines Krankenhauses können die Risikomanagement-Aufgaben an Risikomanager delegieren, nicht aber die Verantwortung. Geht es hierbei um Risikoobjekte und Risiko-Eigentümer, ist die Geschäftsführung in der Pflicht.

Der Branchenspezifische Sicherheitsstandard (B3S) für die medizinische Versorgung hat als Zielgruppe insbesondere die für die Umsetzung von Informationssicherheit in den Krankenhäusern zuständigen Personen (Informationssicherheitsbeauftragten), die Geschäftsführungen als Verantwortliche für Informationssicherheit aber auch externe Dienstleister oder Dritte, welche die Umsetzung der Maßnahmen unterstützen wollen.

Zu den ersten Schritten gehört, seitens der Geschäftsführung ein interdisziplinäres Team mit der Vorbereitung zu beauftragen, einen - internen oder externen - Informationssicherheitsbeauftragten zu benennen, das Informationssicherheitsmanagement organisatorisch zu verankern und im Unternehmen zu kommunizieren. Dazu zählt die Bestellung eines Informationssicherheitsbeauftragten (ISB). Der ISB besitzt eine unabhängige und organisatorisch herausgehobene Stellung. Er ist in dieser Rolle direkt der Klinikleitung unterstellt und berichtet direkt an diese. Die Klinikleitung trägt weiterhin die Gesamtverantwortung für alle Belange der Informationssicherheit.

Risikoobjekte und Risiko-Eigentümer

Die Geschäftsführung MUSS für Bekanntgabe und Durchsetzung entsprechender Ziele der Informationssicherheit (z. B. durch Veröffentlichung einer Informationssicherheitsleitlinie, des B3S-Geltungsbereichs etc.) Sorge tragen und den Informationssicherheitsprozess initiieren.

Die Geschäftsführung MUSS sicherstellen, dass die Zuweisung von Rollen und Verantwortlichkeiten sowie die Bereitstellung von notwendigen organisatorischen, personellen und finanziellen Ressourcen zur Umsetzung des Informationssicherheitsmanagements im Krankenhaus erfolgen. Diese Rahmenbedingungen MÜSSEN geeignet sein, die Durchsetzung der hierfür notwendigen Maßnahmen zu gewährleisten. Die Zuweisung der organisatorischen Verantwortlichkeiten SOLL regelmäßig überprüft werden.

Die Geschäftsführung MUSS die glaubhafte und nachhaltige Vermittlung der Bedeutung der Informationssicherheit gegenüber Mitarbeitern, Patienten und Dritten (z. B. Aufsichtsbehörden etc.) sicherstellen.

Die Geschäftsführung MUSS die Überprüfung eines wirksamen Informationssicherheitsmanagements durch fortlaufende Kontrolle der Zielerreichung sicherstellen.

Die Geschäftsführung MUSS die Sicherstellung eines angemessenen Qualifikationsniveaus (erforderliche Kenntnisse und Erfahrungen) der Mitarbeiter entsprechend ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten sicherstellen.

Die Geschäftsführung MUSS für die Sicherstellung der Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche Sorge tragen, um das Risiko von Interessenkonflikten sowie unautorisierter oder versehentlicher Änderungen oder Missbrauch von Unternehmenswerten zu minimieren (Beispiel: Informationssicherheitsbeauftragter und IT-Leiter in einer Person birgt Interessenkonflikte).

Die Geschäftsführung MUSS die Verantwortlichkeit für die Kontrolle der Zielerreichung des Informationssicherheitsmanagements sowie für die Umsetzung der im IT-Sicherheitsprozess abgestimmten Maßnahmen eindeutig zuweisen.

ANF-0193 Informationswerte (Risikoobjekte) des Risikomanagements der Informationssicherheit MÜSSEN ermittelt, dokumentiert und verwaltet werden.

ANF-0194 Ein Risikoeigentümer MUSS festgelegt werden, der die Ergebnisse der Risikoanalyse und -behandlung verantwortet sowie alle nachfolgenden Überprüfungen zu Risikoanalysen und -behandlungen durchführt.

ANF-0195 Grundsätzlich SOLL der Verantwortliche des Informationssystems als Risikoeigentümer der Information auch die Informationsrisiken ermitteln.

ANF-0196 Für alle Informationswerte MÜSSEN einzelne Personen oder Personengruppen als Verantwortliche festgelegt werden.

Angemessenes Sicherheitsniveau etablieren

Der Anwendungsbereich dieses B3S umfasst nach der Rechtsverordnung die kritische Dienstleistung „stationäre medizinische Versorgung“, Teile davon (z. B. einzelne Prozessschritte) oder für die kritische Dienstleistung relevanten (Typen von) „Einrichtungen, Anlagen oder Teile[n] davon“. Der Begriff der „stationären medizinischen Versorgung“ wird im Krankenhaus in vor- und nachstationäre sowie teil- und vollstationäre Behandlungsformen differenziert.

Der B3S dient im Ergebnis der Etablierung eines angemessenen Sicherheitsniveaus i.S.v. § 8a (1) BSIG bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen.

Dabei ist nicht nur die Sicherheit der IT-Systeme und Medizingeräte, sondern – in Abhängigkeit von der Kritikalität der eingesetzten Systeme – auch die Sicherheit der hiermit verarbeiteten Informationen in der Gesundheitsversorgung von besonderer Bedeutung. Um diese zu schützen, bedarf es neben der Umsetzung technischer und organisatorischer Vorkehrungen auch eines bewussten Umgangs mit diesen Informationen seitens der hiermit betrauten Mitarbeitenden.

Quelle: Deutsche Krankenhausgesellschaft, Branchenspezifischer Sicherheitsstandard „Medizinische Versorgung“ Gesamtdokument 8.12.2022

Krankenhaus-IT-Management und Stakeholder gemeinsam strategische Ziele erreichen

Der Konflikt zwischen dem Krankenhaus-IT-Management und den Stakeholdern kann verschiedene Ursachen haben. Dazu kann mangelnde Transparenz über den IT-Wertbeitrag für die Patientenversorgung zählen oder innovative Impulse, wie IT-Investitionen zur Verbesserung der Ergebnisse beitragen können. Optimierung von Abläufen, Verbesserung der Patientenversorgung, Kostensenkung und Erfüllung von Vorschriften können relevanten Stakeholdern weiterführende Perspektiven für eine langfristig bessere Gesundheitsversorgung aufzeigen.

Durch Digitalisierung werden aber auch die Anforderungen an die klinikinterne IT-Abteilung immer höher. Auch die IT- und Medizintechnik-Abteilung muss sich zum vollumfänglichen IT-Dienstleister für das Krankenhaus weiterentwickeln. Die Administration der Systeme ist heute häufig geprägt von Ad-hoc-Prozessen und Verschwimmungen in den Bereichen. Es müssen jedoch eindeutige Rahmenbedingungen definiert werden, wie sich die IT zukünftig aufstellen sollte, um die Herausforderungen der Digitalisierung zu meistern. Das Krankenhaus-IT-Management im Clinch mit Stakeholdern lebt mit möglichen Problemen, die zu Spannungen führen können.

Für die Prozesse des Unternehmens Krankenhaus bieten sich potenzielle Lösungsansätze an.

Unterschiedliche Prioritäten: Das IT-Management konzentriert sich möglicherweise auf die Effizienz, Sicherheit und Kosteneinsparungen, während die Stakeholder möglicherweise den Schwerpunkt auf die Patientenversorgung und -zufriedenheit legen. In solchen Fällen ist es wichtig, eine offene Kommunikation zu fördern und die gegenseitigen Erwartungen zu klären. Das IT-Management sollte den Wertbeitrag seiner Arbeit für die Patientenversorgung deutlich machen und Stakeholdern zeigen, wie IT-Investitionen zur Verbesserung der Ergebnisse beitragen können.

Begrenzte Ressourcen: Oft stehen dem IT-Management begrenzte Ressourcen zur Verfügung, was zu Verzögerungen bei der Umsetzung von Projekten oder zur Priorisierung bestimmter Anforderungen führen kann. Es ist wichtig, transparent über die verfügbaren Ressourcen zu kommunizieren und gemeinsam mit den Stakeholdern Prioritäten zu setzen. Eine klare Kommunikation über die Ressourcenbeschränkungen und die daraus resultierenden Auswirkungen kann dazu beitragen, das Verständnis und die Zusammenarbeit zu verbessern.
Mangelnde Einbindung der Stakeholder: Wenn die Stakeholder nicht ausreichend in Entscheidungsprozesse einbezogen werden, kann dies zu Frustration und Widerstand führen. Das IT-Management sollte sicherstellen, dass die Stakeholder von Anfang an in den Planungs- und Entscheidungsprozess einbezogen werden. Regelmäßige Treffen, Feedbackschleifen und offene Kommunikation sind entscheidend, um sicherzustellen, dass die Bedürfnisse und Anliegen der Stakeholder gehört und berücksichtigt werden.

Komplexe Technologie: Die Komplexität der IT-Systeme und -Anwendungen kann zu Unverständnis und Fehlkommunikation zwischen dem IT-Management und den Stakeholdern führen. Es ist wichtig, die technischen Konzepte und Herausforderungen in verständlicher Form zu erklären und sicherzustellen, dass die Stakeholder die Auswirkungen und Vorteile der Technologie verstehen. Schulungen und Schulungsprogramme können dazu beitragen, das Verständnis und die Akzeptanz zu verbessern.

Sicherheits- und Datenschutzbedenken: Das IT-Management ist oft bestrebt, hohe Sicherheitsstandards und Datenschutzrichtlinien einzuhalten, was manchmal zu Einschränkungen in der Nutzung bestimmter Systeme oder Technologien führen kann. Die Stakeholder

können sich dadurch in ihrer Arbeit behindert fühlen. In solchen Fällen ist es wichtig, die Bedeutung von Sicherheit und Datenschutz zu erläutern und gemeinsame Lösungen zu finden, die die Anforderungen aller Beteiligten berücksichtigen.

Resilienz Management und Performanz: Diese Dimension erfasst die organisatorische und operative Sicherheit, Anpassungsfähigkeit und Belastbarkeit der Einrichtung, insbesondere vor dem Hintergrund sich ändernder Geschäftsbedingungen oder Störungen im Zusammenhang mit der Verfügbarkeit von technischen Systemen und digitalen Informationen. Für den Fall von geplanten oder ungeplanten Systemausfällen muss gewährleistet sein, dass sowohl die klinische Versorgung von Patient:innen als auch der allgemeine Geschäftsbetrieb aufrechterhalten werden kann (Business Continuity). Dafür müssen Regeln und Prozesse definiert sein, die bei Eintreffen eines Störfalles aktiviert werden können. Diese Pläne müssen zudem einer regelmäßigen Prüfung unterzogen werden.

Synergien minimieren - effektive Zusammenarbeit steigern

Ein effektives IT-Management im Krankenhaus erfordert eine enge Zusammenarbeit mit den Stakeholdern, um deren Bedürfnisse zu verstehen und auf sie einzugehen. Durch offene Kommunikation, Einbindung der Stakeholder in Entscheidungsprozesse und klare Erklärungen der IT-Strategie und -Maßnahmen können Konflikte minimiert und eine effektive Zusammenarbeit erreicht werden. Das Krankenhaus-IT-Management kann verschiedene Synergien mit seinen Stakeholdern erzielen.

Medizinisches Personal: Durch eine effektive IT-Infrastruktur und entsprechende Systeme kann das Krankenhaus-IT-Management das medizinische Personal dabei unterstützen, ihre Arbeit effizienter und sicherer zu gestalten. Dies umfasst die Bereitstellung von elektronischen Patientenakten, Labordatenmanagement, Bildgebungssystemen und anderen medizinischen Informations- und Kommunikationstechnologien. Durch den Zugriff auf aktuelle und umfassende Informationen können Ärzte und Pflegepersonal bessere Entscheidungen treffen, die Qualität der Patientenversorgung verbessern und potenzielle Fehler reduzieren.

Patienten: IT-Systeme im Krankenhaus können den Patienten viele Vorteile bieten, wie zum Beispiel die elektronische Patientenakte, die einen einfachen und sicheren Zugriff auf ihre medizinischen Daten ermöglicht. Dies fördert die Transparenz und ermöglicht es den Patienten, ihre Gesundheitsinformationen besser zu verstehen und aktiv an ihrer eigenen Versorgung teilzuhaben. Darüber hinaus können IT-Systeme Terminplanungen, Online-Kommunikation mit dem medizinischen Personal, Telemedizin und die Überwachung von Gesundheitsparametern unterstützen, was zu einer verbesserten Patientenerfahrung führt.

Verwaltung und Finanzen: Das Krankenhaus-IT-Management kann den Verwaltungs- und Finanzbereich unterstützen, indem es effiziente Systeme für die Abrechnung, das Bestandsmanagement, die Personalplanung und das Ressourcenmanagement bereitstellt. Durch die Automatisierung von Prozessen können Kosten gesenkt, Fehler reduziert und die Effizienz gesteigert werden. Darüber hinaus können IT-Systeme die Datenerfassung und -analyse verbessern, was wiederum die Entscheidungsfindung unterstützt und die Rentabilität des Krankenhauses optimiert.

Lieferanten und Partner: Das Krankenhaus-IT-Management kann eine engere Zusammenarbeit mit Lieferanten und Partnern ermöglichen, indem es elektronische Bestellsysteme, Kommunikationsplattformen und gemeinsame Datenzugriffe bereitstellt. Dies fördert eine effizientere Lieferkette, verbessert die Kommunikation und erleichtert die Zusammenarbeit bei der Entwicklung und Implementierung neuer Technologien oder Dienstleistungen.

Regulierungsbehörden und Aufsichtsgremien: Das Krankenhaus-IT-Management spielt eine wichtige Rolle bei der Einhaltung von Vorschriften und Richtlinien im Gesundheitswesen. Durch die Implementierung von Sicherheitsmaßnahmen, Datenschutzrichtlinien und Qualitätskontrollen trägt das IT-Management dazu bei, die Compliance-Anforderungen zu erfüllen und die Integrität des Gesundheitssystems zu wahren. Eine enge Zusammenarbeit mit Regulierungsbehörden und Aufsichtsgremien ist entscheidend, um die Einhaltung gesetzlicher Bestimmungen sicherzustellen und gemeinsame Ziele zu erreichen.

Durch Synergien kann das Krankenhaus-IT-Management eine wichtige Rolle bei der Optimierung von Abläufen, Verbesserung der Patientenversorgung, Kostensenkung und Erfüllung von Vorschriften spielen. Eine enge Zusammenarbeit mit allen relevanten Stakeholdern lasen sich langfristige strategische Ziele erreichen und eine bessere Gesundheitsversorgung gewährleisten.

Wie KI die IT-Administration innoviert

Künstliche Intelligenz (KI) hat das Potenzial, die IT-Administration auf vielfältige Weise zu innovieren. KI nicht ohne Herausforderungen ist. Die Implementierung von KI-Systemen erfordert eine sorgfältige Planung, Datensicherheit, Ethik und Datenschutz. Die Aussage, dass IT-Administratoren durch KI ihren Job verlieren, ist nicht zwangsläufig korrekt. Während KI-Technologien einige Aufgaben automatisieren und die Effizienz verbessern können, wird die Rolle des IT-Administrators weiterhin von großer Bedeutung sein.

Wenn in einem Unternehmen durch den digitalen Wandel grundlegende Veränderungen anstehen, betrifft das alle Mitarbeiter – auch die IT-Administratoren. Sie sollen vom „passiven Verwalter" zum „aktiven Gestalter" werden. Es ist wichtig anzumerken, dass KI nicht ohne Herausforderungen ist. Das hat Konsequenzen. Hier sind einige der Möglichkeiten, wie KI die IT-Administration vorantreiben kann.

1 Automatisierung von Routineaufgaben: KI-Systeme können repetitive und zeitaufwändige Aufgaben automatisieren, wie z.B. das Überwachen von Systemen, das Installieren von Updates oder das Erstellen von Backups. Dies ermöglicht den IT-Administratoren, sich auf anspruchsvollere Aufgaben zu konzentrieren und die Effizienz zu steigern.

2 Proaktive Wartung und Fehlererkennung: KI kann dazu eingesetzt werden, Probleme in IT-Systemen frühzeitig zu erkennen und proaktiv Maßnahmen zu ergreifen, um potenzielle Ausfälle zu verhindern. Durch die Analyse von Daten und das Erkennen von Mustern kann KI helfen, Engpässe, Sicherheitslücken oder Performance-Probleme vorherzusagen und rechtzeitig zu beheben.

3 Intelligente IT-Sicherheit: KI kann bei der Erkennung und Abwehr von Bedrohungen in Echtzeit helfen. KI-gestützte Sicherheitssysteme können Anomalien im Netzwerkverkehr, verdächtige Aktivitäten oder unbekannte Bedrohungen identifizieren und automatisch Gegenmaßnahmen ergreifen. Dies ermöglicht eine schnellere Reaktion auf Sicherheitsvorfälle und einen besseren Schutz der IT-Infrastruktur.

4 Effiziente Ressourcenverwaltung: KI kann bei der Optimierung der Ressourcennutzung in Rechenzentren helfen. Durch die Analyse von Daten über den Ressourcenverbrauch können KI-Systeme Vorhersagen über zukünftige Bedarfe treffen und die Ressourcen entsprechend zuweisen. Dies führt zu einer effizienteren Nutzung von Hardware und Energie und kann zu erheblichen Kosteneinsparungen führen.

5 Natürliche Sprachverarbeitung und Chatbots: KI-gesteuerte Chatbots können den IT-Support verbessern, indem sie Benutzern bei der Lösung von Problemen und der Beantwortung von Fragen in natürlicher Sprache helfen. Diese Chatbots können einfache Anfragen bearbeiten, häufig gestellte Fragen beantworten und bei der Fehlerbehebung unterstützen. Dies entlastet die IT-Mitarbeiter von repetitiven Support-Aufgaben und ermöglicht eine schnellere und effizientere Unterstützung für Benutzer.

Allerdings ist es wichtig anzumerken, dass KI nicht ohne Herausforderungen ist. Die Implementierung von KI-Systemen erfordert eine sorgfältige Planung, Datensicherheit, Ethik und Datenschutz. Dann bietet KI ein großes Potenzial, die IT-Administration zu verbessern und die Effizienz, Sicherheit und Benutzererfahrung zu steigern.

KI besitzt ein großes Potenzial, die Effizienz, Sicherheit und Benutzererfahrung in der IT-Administration zu verbessern. Künstliche Intelligenz (KI) hat das Potenzial, die IT-Administration auf vielfältige Weise zu innovieren. Hier sind einige Bereiche, in denen KI einen bedeutenden Einfluss hat:

1 Automatisierung von Routineaufgaben: KI kann eingesetzt werden, um repetitive und zeitaufwändige Aufgaben in der IT-Administration zu automatisieren. Beispielsweise können KI-Algorithmen verwendet werden, um die Überwachung und Wartung von IT-Systemen zu automatisieren, Patches und Updates zu verwalten oder sogar IT-Tickets zu bearbeiten und zu priorisieren.

2 Intelligente Analyse und Vorhersage: Durch die Analyse großer Datenmengen kann KI Einblicke in die Leistung und den Zustand von IT-Systemen liefern. KI-Algorithmen können Muster und Anomalien erkennen, um potenzielle Probleme frühzeitig zu identifizieren und vorherzusagen. Dies ermöglicht eine proaktive Wartung und Vermeidung von Ausfällen.

3 Verbesserung der Sicherheit: KI kann dabei helfen, Bedrohungen und Sicherheitsrisiken in Echtzeit zu erkennen. KI-gestützte Sicherheitssysteme können Anomalien im Netzwerkverkehr oder verdächtiges Verhalten von Benutzern identifizieren und sofort darauf reagieren. KI kann auch bei der Erkennung von Schwachstellen in IT-Systemen helfen und dabei unterstützen, diese zu beheben, bevor sie ausgenutzt werden.

4 Effizienteres Ressourcenmanagement: KI kann bei der Optimierung des Ressourcenmanagements in der IT-Administration unterstützen. Durch die Analyse von Nutzungsdaten und Leistungsmetriken kann KI helfen, Ressourcen wie Serverkapazitäten, Speicherplatz oder Netzwerkbandbreite effizienter zu verteilen und Engpässe zu vermeiden.

5 Verbesserung des Benutzererlebnisses: KI kann auch das Benutzererlebnis in der IT-Administration verbessern. Chatbots oder virtuelle Assistenten mit KI-Fähigkeiten können Benutzern helfen, ihre Probleme zu lösen, Fragen zu beantworten und Anfragen zu bearbeiten. Durch die Nutzung von natürlicher Sprachverarbeitung und maschinellem Lernen können diese Systeme lernen, Benutzeranfragen besser zu verstehen und effektive Lösungen bereitzustellen.

Es ist wichtig anzumerken, dass KI-Technologien in der IT-Administration auch einige Herausforderungen mit sich bringen, wie beispielsweise Datenschutzbedenken, ethische Fragen und den Bedarf an qualifiziertem Personal zur Verwaltung und Überwachung der KI-Systeme. Dennoch bietet KI ein großes Potenzial, die Effizienz, Sicherheit und Benutzererfahrung in der IT-Administration zu verbessern.

Warum der IT-Administrator durch KI seinen Job nicht verliert

Die Aussage, dass IT-Administratoren durch KI ihren Job verlieren, ist nicht zwangsläufig korrekt. Während KI-Technologien einige Aufgaben automatisieren und die Effizienz verbessern können, wird die Rolle des IT-Administrators weiterhin von großer Bedeutung sein. Hier sind einige Gründe:

1 Komplexität: Die IT-Infrastruktur von Unternehmen wird immer komplexer. Es erfordert ein tiefes Verständnis der Systeme, Netzwerke und Anwendungen, um sicherzustellen, dass sie effektiv funktionieren. Ein IT-Administrator ist in der Lage, diese Komplexität zu managen, Probleme zu erkennen und Lösungen zu implementieren.

2 Strategische Planung: IT-Administratoren spielen eine wichtige Rolle bei der Entwicklung und Umsetzung von IT-Strategien in Unternehmen. Sie analysieren die Geschäftsanforderungen, evaluieren neue Technologien und stellen sicher, dass die IT-Infrastruktur den Zielen des Unternehmens entspricht. Diese strategische Planung erfordert menschliches Fachwissen und Urteilsvermögen.

3 Sicherheit: Die IT-Sicherheit ist eine kritische Herausforderung für Unternehmen. IT-Administratoren sind dafür verantwortlich, die Infrastruktur vor Bedrohungen zu schützen, Sicherheitslücken zu identifizieren und zu schließen sowie Sicherheitsrichtlinien zu implementieren. Dies erfordert ein tiefes Verständnis für die aktuellen Bedrohungen und Angriffsmethoden, das kontinuierlich aktualisiert werden muss.

4 Anpassungsfähigkeit: Die IT-Landschaft verändert sich ständig, neue Technologien und Trends kommen auf den Markt. IT-Administratoren müssen sich kontinuierlich weiterbilden, um mit den neuesten Entwicklungen Schritt zu halten und neue Technologien erfolgreich zu implementieren.

Obwohl KI einige repetitive Aufgaben automatisieren kann, ist der menschliche Faktor in der IT-Administration immer noch unerlässlich. Die Zusammenarbeit von KI und IT-Administratoren kann zu effizienteren Prozessen, besseren Entscheidungen und einer optimierten IT-Infrastruktur führen. Es ist wahrscheinlicher, dass sich die Rolle des IT-Administrators durch KI verändert und er neue Fähigkeiten und Kenntnisse entwickeln muss, um mit den sich wandelnden Anforderungen Schritt zu halten.

dedalusgroup.de

Dedalus

Best of Digital Health

Gemeinsam mit unseren Anwendern treiben wir die Digitalisierung täglich voran.

Harmonisierung und Erschließung medizinisch-wissenschaftlicher Register: Herausforderungen für die IT

Im Fokus „Medizinisch-wissenschaftlicher Register – IT-Kooperation für Registeraufbau und -weiterentwicklung" beschreiben Sebastian C. Semler (TMF e. V.), und Dr. Anna Niemeyer (TMF e. V.) IT-Rahmenbedingungen für die Nutzung von Registerdaten im Bewertungsprozess neuer Therapien, das Reifegradmodell und den Status quo der Registerlandschaft und blicken auf IT-Instrumente für Registeraufbau und -weiterentwicklung zusammen mit Schnittstellen zu Vernetzung und Zusammenarbeit von Registern. Sie benennen last but not least Aspekte und Empfehlungen für die Registercommunity.

Medizinisch-wissenschaftliche Register nehmen in der datenbasierten Medizin neben Daten aus der primären Dokumentation der Behandlung, aus klinischen Studien sowie Daten aus medizinischen Abrechnungsvorgängen eine wichtige Rolle ein. In den Registern werden einrichtungsübergreifend zu bestimmten Indikationsgebieten mit behandlungs- oder produktbezogenen Fragestellungen Daten vieler Patientinnen und Patienten mit einem hohen Anspruch an Datenqualität und -sicherheit zusammengetragen und für künftige Forschungsauswertungen vorgehalten. Im Vergleich zu manchen europäischen Nachbarländern ist Deutschland bezüglich der Harmonisierung und Erschließung von Registern im Rückstand. Es gibt bei uns neben den Krebsregistern nur einige wenige gesetzlich geregelte Register. Die Register sind noch kein strategischer Baustein der E-Health-Strategie in Deutschland. Dies soll sich nach Willen des Koalitionsvertrages der aktuellen Bundesregierung ändern. Wie notwendig eine bessere und besser vernetzte Datenlage im deutschen Gesundheitswesen ist, hat nicht zuletzt die COVID-19-Pandemie aufgezeigt. Es ist deutlich geworden, dass Forschende, Innovatoren, öffentlichen Einrichtungen und die Industrie einen sicheren, kontrollierten Zugang zu Gesundheitsdaten von hoher Qualität benötigen, um die Verbesserung der Gesundheitsversorgung voranzubringen. Und nicht zuletzt die von der EU angekündigte europäische Gesundheitsunion mit dem Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) macht es erforderlich, dass Deutschland seine Digitalarchitektur und Akteure der Gesundheitsdatennutzung bündelt, um anschlussfähig an europäische Entwicklungen sein zu können.

Status quo der Registerlandschaft

Für das vom Bundesgesundheitsministerium in Auftrag gegebene Registergutachten[1] wurden in den Jahren 2020 und 2021 etwa 356 medizinisch-wissenschaftliche Register mit ihren Eigenschaften in einem Registerverzeichnis erfasst. Zwischenzeitlich wurde dieses Verzeichnis mit einer Suchfunktion online[2] zur Verfügung gestellt und zählt mittlerweile 402 Register. Im Hinblick auf ihre Ziele, die Laufzeit, den Datenkranz, die Registerpopulation und Größe des Registers (Anzahl der Datensätze und eingeschlossene Patienten und Patientinnen) sowie die gewählte Technologie für die Umsetzung und Erfassung der Daten sind die Register sehr vielfältig. Die Ziele und Aufgaben der Register reichen von der Abbildung der (Routine-)Versorgung über Qualitätssicherung bis hin zur Wahrnehmung von Pharmakovigilanzaufgaben und Post-Market-Surveillance. Vor diesem Hintergrund scheint ein für alle Register gleicher Kriterienkatalog zur Bewertung der Registerqualität wie die Quadratur des Kreises. Der Bedarf, Registerdaten für vielfältige Aufgaben der Versorgungsforschung zu nutzen und auch zur Ergänzung von registerbasierten randomisierten klinischen Studien heranzuziehen, steigt stetig. Um die Nutzbarkeit und die Nutzung von Registerdaten zu erhöhen und transparent darzustellen, werden nachvollziehbare und umsetzbare Standards für die Bewertung der Qualität von Registern benötigt. Die Anforderungen, die zur Bewertung von Registern herangezogen werden, müssen darüber hinaus praktisch umsetzbar, überprüfbar und eindeutig sein.

Das Reifegradmodell für Register

Das im Rahmen des Gutachtens entwickelte Reifegradmodell[3] ermöglicht es jedem Register, anhand eines Fragenkataloges das eigene Weiterentwicklungspotential zur Erreichung eines selbstgewählten Nutzungszwecks zu identifizieren. Zentrales Merkmal ist die Prozessorientierung, die der für Register wichtigen Anpassungsfähigkeit Rechnung trägt, da sich die Anforderungen und Aufgaben von Registern mit dem medizinischen Wissens- und Erkenntniszuwachs, aber auch durch sich verändernde Versorgungssettings und gesundheitspolitische Rahmenbedingungen kontinuierlich ändern. Die Heterogenität der Register fordert hier einen Ansatz, der den unterschiedlichen Nutzungsdimensionen Rechnung trägt und durch einen einheitlichen Kriterienkatalog eine übergreifende Vergleichbarkeit ermöglicht. Für jede der definierten Nutzendimensionen stellen sich unterschiedliche Anforderungen an Strukturen und Prozesse sowie deren Dokumentation. Sie werden in sogenannten Bewertungsdimensionen gebündelt, die zunächst einmal für alle Register gleich sind: Governance, ethische, gesetzliche und soziale Aspekte (ELSI), GWP (Gute wissenschaftliche Praxis), Datenmanagement, Datenqualität, IT-Betrieb, Identitäts- und Einwilligungsmanagement, Partizipation sowie Finanzierung und Verstetigung. Jede dieser Dimensionen wird durch verschiedene Aspekte und Merkmale

repräsentiert. Ob die Erfüllung des jeweiligen Merkmals unbedingt erforderlich oder lediglich wünschenswert ist, wird durch die betrachtete Nutzungsdimension bestimmt. Um als Grundlage für eine Überprüfung durch Dritte (im Sinne einer Auditierung) zu dienen, ist eine Weiterentwicklung und Validierung erforderlich.

Datenverknüpfung und das „Forschungspseudonym“

Die Verknüpfung von Registerdaten mit anderen Datenbeständen, z.B. mit Krankenkassendaten oder genomischen Daten stellt eine wichtige Erweiterung der Nutzung dar. Hierfür ist es freilich erforderlich, die richtigen Patientenfälle zusammen zu führen. Anders als nordeuropäische Nachbarländer hat Deutschland keine einheitlichen Identifikatoren im Gesundheitswesen, die dies einfach und fehlerfrei erlauben. Die Nutzbarkeit z.B. der Krankenversichertennummer zu diesem Zweck ist gesetzlich weitgehend ausgeschlossen. Koalitionsvertrag und Digitalstrategie des BMG haben hier nun Lösungen angekündigt. „Für die Verknüpfbarkeit von Daten aus unterschiedlichen Datenquellen sowie der Verknüpfung der Register untereinander ist ein bundesweit einheitlicher Identifikator entscheidend“, erläutert TMF-Geschäftsführer Sebastian C. Semler. „Wir begrüßen daher ausdrücklich, dass das Bundesgesundheitsministerium in seiner Digitalstrategie die Einführung eines „Forschungspseudonyms“ angekündigt hat.“

Interoperabilität und definierte Metadaten sind von entscheidender Bedeutung

In Deutschland gibt es bereits eine Reihe von Interoperabilitätsinitiativen, die sich mit den Herausforderungen der Harmonisierung von Gesundheitsdaten auseinandersetzen. Register werden hier bislang noch nicht ausreichend miteinbezogen. Im Fokus stehen in der Routineversorgung erhobene Daten in Bezug auf die Verwendung technischer Standards (FHIR) oder Terminologien. Metadaten bzw. Metadatenkataloge oder -Repositorien werden bislang nicht adressiert. Die umfassende Beschreibung der verwendeten Datenelemente und Wertebereiche stellt jedoch eine der zentralen Aufgaben beim Aufbau von Registern dar, ihre Weiterentwicklung im Betrieb ist ein wichtiger Prozess zur Sicherstellung der Auswertbarkeit und Nutzbarkeit von Registerdaten. Die eindeutige und präzise Definition von Metadaten ist aber von entscheidender Bedeutung und rückt zunehmend in den Fokus. Eine einheitliche, standardisierte Definition der Metadaten zur Beschreibung medizinischer Dokumentation gehört daher zu den dringendsten Aufgaben der Standardisierung im Gesundheitswesen und bildet eine der Grundlagen für den grenzüberschreitenden Austausch von Gesundheitsdaten.

Schnittstellen spielen aktuell nur eine sehr untergeordnete Rolle. Werden Schnittstellen angegeben, so dienen sie in der Regel dem automatisierten Import von Daten aus der Routineversorgung in das Register, zur Vernetzung und Zusammenarbeit von Registern werden sie bislang kaum eingesetzt. „Register müssen viel stärker in den Interoperabilitätsprozess einbezogen werden“, fordert Dr. Anna Niemeyer von der TMF. „Öffentlich verfügbare und gut beschriebene Metadaten aus den Registern im Registerverzeichnis wären zudem ein wichtiger Schritt.“

TMF AG Register unterstützt Registeraufbau und -weiterentwicklung

Die TMF Arbeitsgruppe (AG) Register beschäftigt sich damit, wie patientenbezogene Register vor dem Hintergrund sich verändernder gesundheitspolitischer Rahmenbedingungen und technologischer Möglichkeiten so weiterentwickelt werden können, dass sie noch nutzbringender für die Forschung eingesetzt werden können. Die AG wird nicht nur fachkundige Begleitung für Registerbetreibende anbieten, sondern aktiv zur Verbesserung der Qualität und Interoperabilität von Registern in Deutschland beitragen. Dafür wird die Arbeitsgruppe auch auf die Expertise bereits etablierter Arbeitsgruppen wie Datenqualität, Datenschutz und IT-Infrastrukturen zurückgreifen. Ein Fokus wird auf der Erprobung und Weiterentwicklung des Reifegradmodells liegen. Zentrale Aufgaben der Arbeitsgruppe sind darüber hinaus die Vernetzung und das Networking der Mitglieder untereinander und mit kooperierenden Initiativen und Vereinen. Mit dem zukünftigen Beratungsangebot für Registerprojekte zu allen Phasen des Register Lifecycle (von der Planung bis zur Abwicklung) will die AG zur Standardisierung und Weiterentwicklung der Registerlandschaft beitragen.

[1] https://www.bundesgesundheitsministerium.de/service/publikationen/details/gutachten-zur-weiterentwicklung-medizinischer-register-zur-verbesserung-der-dateneinspeisung-und-anschlussfaehigkeit-2.html
[2] https://registersuche.bqs.de/search.php
[3] https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/REG-GUT-2021-Anhang-K_Bewertungskatalog_Anwendung_Beispielregister_2021-....xlsx

Sebastian C. Semler, wissenschaftlicher Geschäftsführer, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.,

Dr. Anna Niemeyer, wissenschaftliche Mitarbeiterin der TMF und Erstgutachterin, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.,

Das Sommer-Camp des Eco Systems ENTSCHEIDERFABRIK – der eHealth Inkubator

ENTSCHEIDERFABRIK geht in die heiße Phase und zeigt auf dem Sommer-Camp2023 die Effizienzpotentiale von Digitalisierungsprojekten auf. Gastgeber des Sommer-Camps der ENTSCHEIDERFABRIK im Jahr 2023 war CompuGroup Medical - CGM Das Sommer-Camp fand am 12.-13.06.2023 bei CGM in Koblenz statt. Motto: „Krankenhauserfolg durch Nutzen stiftende Digitalisierungsprojekte".

eHealth Inkubator 2023, Sommer-Camp bei Industrie-Mitglied CGM, 12.-13.06.2023, Koblenz

Als Sommer-Camp Gastgeber begrüßten Peter Wegmann, Vertriebsleiter KIS DACH und Sarah Peuling, Head of Go-To-Market Management KIS DACH, CGM – CompuGroup Medical und Dr. Pierre- Michael Meier, CHCIO, Geschäftsführer ENTSCHEIDERFABRIK und EVP & CFO AHIME die TeilnehmerInnen.

In Vertretung von Peter Summermatter, Feedbackgeber 2023 und Verwaltungsratspräsident the i-engineers, gaben Volker Sobieroy, CHCIO und David Hofmann, die richtigen Impulse um die Ausarbeitungen der einzelnen Digitalisierungsprojekte auf die nächste Ebene zu heben.

Die Teilnahme am Sommer-Camp ist den Personen vorbehalten, die in einem der 5 Digitalisierungsthemen 2023 engagiert sind oder ein Thema für den Digitalisierungswettbewerb auf dem Entscheider-Event 2024 eingereicht haben.

Durch die Coaching Session für den Digitalisierungswettbewerb auf dem Entscheider-Event 2024 führten Dr. Meier, Dr. Silke Haferkamp, CIO, Uniklinik der RWTH Aachen, Dieter Padberg, AHIME Association Vice President Human Ressources, CIO, Universitätsklinikum Bonn und Michael Schindzierlorz, Vorsitzender Supervisory Board der AHIME.

Die betreuenden Berater der 5 Digitalisierungsthemen organisierten die Projektfortschritte, d.h. zu den Digitalisierungsthemen

(1) Managed Threat Response (MTR) – SOC und SIEM as a Service

(2) Optimierung des Patientenworkflows – Selfcheck-In & smarte Vitaldatenerfassung

(3) Klinische Entscheidungsunterstützung für Diabetes am PoC

(4) Identity Governance® - durch rollenbasierte Zugriffe eine qualitativ hochwertige Patientenversorgung gewährleisten

(5) Wo sind meine Patientinnen und Patienten?

Mit unserem digitalen Live Stream haben wir auch in 2023 die Möglichkeit eröffnet, Ausschnitte aus dem Sommer-Camp live zu erleben.

Die Tagungsvorsitzenden waren Dr. Meier Pierre- Michael, CHCIO, Vilker Sobieroy, CHCIO und David Hofmann.

Der Ehemalige Camp-Teilnehmer, der gegenüber den aktuellen „Camp-Teilnehmer" über seine Erfahrungen berichtete, war in diesem Jahr Frank Ebling, Stabsstelle Digitalisierung und Informationssicherheit Westpfalz-Klinikum.

Die ENTSCHEIDERFABRIK Medienpartner, d.h. Health & Care Management (Michael Klotz), Krankenhaus IT-Journal (Kim Wehrs) und Pflege Management (Markus Frings) präsentierten ihre Programme.

Die Teams der 5 Digitalisierungsthemen stellten den Stand ihre Ausarbeitungen zu Beginn des ersten Tages, zum Ende des ersten Tages und zur Mitte des zweiten Tages des Sommer-Camps vor.

Management Training on Digital Transformation

Seit 2006 hat das Eco System ENTSCHEIDERFABRIK als führender eHealth-Inkubator maßgeblich dazu beigetragen, die Chancen der digitalen Transformation im Gesundheitswesen zu realisieren. Insbesondere in Zusammenarbeit mit Entscheidern aus Krankenhäusern konnte das Eco System innovative Lösungen entwickeln und erfolgreich in die Praxis integrieren. Seit 2009 wurde zudem eine nachhaltige Beziehung zu amerikanischen Krankenhausträgern aufgebaut, um gemeinsam die Chancen der digitalen Transformation zu erforschen, zu diskutieren und zu adaptieren.

Der Besuch unserer Partnerkliniken in San Diego sowie die Teilnahme an unseren Workshops in Phoenix bieten die einmalige Gelegenheit, sich persönlich von den Fortschritten der digitalen Transformation zu überzeugen. Dort wird insbesondere das von unseren amerikanischen Freunden entwickelte Management Training zur digitalen Transformation im Gesundheitswesen Transforming Health Care in Disruptive Times" angeboten.

Management Training zur digitalen Transformation

Das Management Training besteht aus verschiedenen Modulen, die den Teilnehmern ein umfassendes Verständnis für die Herausforderungen und Chancen der digitalen Transformation vermitteln. Der Erfahrungsaustausch mit den US-amerikanischen Partnerkliniken in San Diego ermöglicht es den Teilnehmern, die Entwicklungen seit dem letzten Jahr nachzuvollziehen und die wichtigsten Schritte von der Vision über die Strategie bis hin zur Umsetzung und dem quartalsweisen Reporting kennenzulernen. Dabei wird deutlich gemacht, dass eine Vision ohne Umsetzung nur eine Illusion ist.

Erfahrungsaustausch mit Partnerkliniken

Ein weiteres Highlight des Trainings ist die Besichtigungstour, bei der der aktuelle Fokus im Detail beleuchtet wird. Darüber hinaus werden auf dem CHiME Fall Forum in Phoenix spezielle Workshops zu den Themen Leadership & Change Management sowie Digital Health & Health-IT angeboten. Diese Workshops geben den Teilnehmenden die Möglichkeit, ihre Organisation im Bereich Leadership & Management zu reflektieren und zu verbessern sowie die Auswirkungen von Digital Health & Health-IT auf ihre Organisation zu untersuchen.

Zertifikat für erfolgreiche Teilnahme

Am Ende des Management Trainings erhalten die Teilnehmer das Zertifikat "Strategic Health Information Management Executive (SH-I-ME)", das die erfolgreiche Teilnahme und die erworbenen Kenntnisse bescheinigt.

Zielgruppe und Interessen

Das Management Training richtet sich an Führungskräfte und Entscheidungsträger von Leistungserbringern, Industrie und Beratungsunternehmen. Von besonderem Interesse ist es für diejenigen, die sich mit den Auswirkungen der digitalen Disruption auf den regionalen und überregionalen Wettbewerb der Leistungserbringer auseinandersetzen wollen. Die Teilnehmer sollen auf die Herausforderungen vorbereitet werden, denen wir uns täglich stellen müssen: "Transforming Healthcare in disruptive Times". Ziel ist es, die Auswirkungen der digitalen Transformation auf den Wettbewerb der Leistungserbringer zu verstehen und konkrete Maßnahmen zu ergreifen, um im Wettbewerb erfolgreich zu sein.

Mehr Informationen unter

www.ENTSCHEIDERFABRIK.com

KH-IT-Frühjahrstagung 2023: Intelligenter Optimismus ist Pflicht

Die KH-IT-Frühjahrstagung 2023 am 22. und 23.05.2023 in Nürnberg informierte über „KI, Machine Learning, Automatisation und Verantwortung". Aus der Praxis für die Praxis gaben Experten über 200 Verantwortlichen der Krankenhaus-IT interdisziplinäre Impulse. Vor allem ging es um Konzeption, Umsetzung und Erfahrungen zukunftsweisender Lösungen. Von Wolf-Dietrich Lorenz

Der Anlass für die Themenauswahl der Frühjahrstagung „KI, Machine Learning, Automatisation und Verantwortung" ist hochaktuell. Im Moment herrscht große Aufmerksamkeit für das Thema „künstliche Intelligenz". Motiv für Prof. Dr. phil. Rouven Porz, Medizinethik und ärztliche Weiterbildung, Universitätsspital Bern, zu fragen: „Kann KI gut sein?" Manche meinen, dass die KI unsere ganze Welt revolutionieren kann, andere haben Angst, dass sie jetzt ihren Arbeitsplatz an KI verlieren. Wieder andere wissen gar nicht genau, was mit KI gemeint ist. Da kommt nun die Ethik ins Spiel. „Man hat nämlich Angst, dass im ganzen Rummel um die Möglichkeiten der KI vielleicht grundsätzliche ethische Regeln des guten menschlichen Miteinanders verloren gehen können," meinte der Referent. „Davon handelt die Ethik." Und davon handelte auch sein Vortrag. „Ich appelliere an Verantwortung, und daran, dass jeder und jede von uns diese Verantwortung auch selbst übernehmen muss." Der Einsatz von Systemen der künstlichen Intelligenz braucht Regeln. Nicht viele, aber zielorientierte und wirksame. Künstliche Intelligenz und Roboter sind Chance und Risiko zugleich, je nachdem, wofür sie eingesetzt werden. Anzustreben ist ein differenzierter Ansatz, der möglichst viel Raum für Innovation lässt und dank allgemeingültigen, technologieneutralen Regeln in der Lage ist, der raschen technischen Entwicklung Rechnung zu tragen. Hier kann ein Zitat von Philosoph Karl Popper die Richtung weisen: „Optimismus ist Pflicht." Es ist nämlich wahrscheinlicher, dass die Dinge besser werden, wenn man aktiv daran arbeitet, als sie ignoriert.

Potentiale Künstlicher Intelligenz

Digitalisierungsgewinne durch „KI, Machine Learning, Automatisation" sind für klinische Anwendungen, Telekommunikation und Medizintechnik zu erwarten. Wirtschaftliche, technische und organisatorische Auswirkungen auf Ressourcen finden sich täglich. Es kommen rasch weitere dazu.

Aktuell leiden immer mehr Krankenhäuser unter den Auswirkungen eines massiven Fachkräftemangels. Mittels automatisierter Prozesse und technischer Ansätze zur Entlastung der Mitarbeiter von Routinetätigkeiten werden Rationalisierungspotentiale gesucht, die häufig auch komplexe Verknüpfungen bisher erhobener Daten erfordern. Diese Potentiale lassen sich inzwischen meist nur noch mit Ansätzen Künstlicher Intelligenz heben, da einfachere Verfahren bereits ausgereizt sind. Auf der Tagung waren einige beispielhafte Ansätze und verschiedene Strukturen zu sehen, ihre Auswirkungen bzw. auch die erforderlichen Voraussetzungen wurden thematisiert. So will SVA System mit „Elastic Security: Sicherheit mit KI und Machine Learning“ die Herausforderungen der Digitalisierung angehen und einen Beitrag zur Wertschöpfung leisten.

Gewandelte Aufgaben und Anforderungen für Entscheider ergeben sich durch die Integration von KI, Machine Learning und Automatisation. Sie können erhebliche Zeitersparnis bei Routinetätigkeiten wie der Vorsortierung und Kategorisierung von DICOM-Bildern oder Entlastung bei Routinetätigkeiten im Rechenzentrum bringen. Außerdem können sie Erlösoptimierungen wie bei der intelligenten Verarbeitung von Leistungen der Krankenhausabteilungen zur automatischen Kodierung ermöglichen. Nebeneffekt: Damit kann dem akuten Mangel an Fachkräften entgegenwirkt werden.

Mit Machine Learning und KI sind Wissenspotenziale zu erschließen, wie Anett Müller, DMI, und Wilhelm Brinkmann, St. Vincenz-Kliniken, Paderborn, darstellten. Eine solche Roadmap für das digitale Datenmanagement zeigt Informationssicherheit, technische Kommunikationsfähigkeit, Prozessoptimierung und Wissensgenerierung auf mit der digital konsolidierten Patientenakte im Fokus. Verantwortliche, die ihren Krankenhausbetrieb erfolgreich managen möchten, müssen qualifiziert mit den Daten beim Einsatz neuer Technologien umgehen.

Künstliche Intelligenz in Gesamtheit verstehen

Künstliche Intelligenz (KI) ist eines der Technologiethemen, das ein hohes disruptives Potenzial aufweist. Um einen Mehrwert generieren zu können und KI erfolgreich in Unternehmen zu etablieren, müssen mehrere Aspekte betrachtet werden. Udo Würz, FUJITSU Technology Solutions GmbH Berlin, hinterfragte pointiert „Dr. KI – Künstliche Intelligenz im Gesundheitswesen“ und gab zu bedenken: "Ausgereift oder der Assistent im Hintergrund"? Um im Rennen datengesteuerter Unternehmen mithalten zu können, müssen sowohl die Datenqualität sichergestellt als auch die technischen Voraussetzungen geschaffen werden. KI-Technologien funktionieren nur dann gut, wenn die richtigen Daten vorliegen und Systeme auch die Fähigkeit haben, sich die relevanten Informationen zusammenzuziehen. Udo Würz: „Nur wer Künstliche Intelligenz in ihrer Gesamtheit versteht, kann einen klaren Wettbewerbsvorsprung erzielen.“

Europäischer Raum der Gesundheitsdaten

In der etablierten „Aktuelle Stunde“ ging es u.a. um europäische Rechtsvorschriften zur Digitalisierung im Gesundheitssektor. Werner Bachmann, rechtl. Beirat KH-IT e.V., ging auf den „Europäischen Raum der Gesundheitsdaten“ ein. Er wird voraussichtlich Anfang des kommenden Jahres verabschiedet. Im wesentlichen geht es um zwei Ziele: Einmal Portabilität von Gesundheitsdaten über die Grenzen der Mitgliedstaaten hinweg, dementsprechend jederzeit Zugang und Kontrolle der Gesundheitsakte durch den betroffenen Patienten, Öffnung grenzüberschreitender Gesundheitsleistungen und damit einen Binnenmarkt für solche Leistungen, um zweiten einen europäischen Pools von Gesundheitsdaten als nichtkommerzieller Datenraum zu schaffen, der für Forschung und Entwicklung zur Verfügung steht (d.h. Förderung datengetriebener medizinischer Verfahren für Diagnostik und Heilbehandlung.). Begleitet wird dies von einer behutsamen Revision der Datenschutzgrundverordnung und dem neuen Data Governance Act. Hören Sie das Interview mit Werner Bachmann, rechtl. Beirat KH-IT e.V., über IT Sicherheit des Gesundheitswesens, Beschaffung und Kooperation bei digitaler Infrastruktur sowie was daraus für den Berufsverband KH-IT folgt.

Digitalisierungsgewinn durch KI

Aspekte des Wissenstransfers aus der Praxis für die Praxis gehören zu „Digitalisierungsgewinnen“, gerade durch „KI, Maschine Learning, Automatisation“ für IT, Medizintechnik sowie für klinische Anwendungen. Wie sich Aufgaben und Anforderungen für IT-Entscheider durch Integration und Interoperabilität wandeln, zeigte die interaktive KI-Assistenz zur prädiktiven und flexiblen Steuerung im Entlass- und Überleitungsmanagement. „KI-basierte Entlassung“ ist ein Forschungsprojekt des Deutschen Forschungszentrums f. Künstliche Intelligenz (DFKI) zusammen mit der Empolis GmbH und der nubedian GmbH. Das Modell kann den Nachsorgeprozesse optimieren und dynamisch an die sich ändernden Anforderungen der anpassen. Ziel ist u.a. eine zeitgerechte Bedarfsermittlung, um die individuelle Versorgungsqualität zu verbessern.

Wegen fortschreitender Digitalisierung und Big Data führt kein Weg an dieser neuen Technologie vorbei. Das Themenfeld KI durchzog daher die Tagungsagenda. „ChatGPT oder wie?“ provozierte Prof. Dr. Thomas Jäschke, DATATREE AG. "Chatbot Generative Pre-trained Transformer" ChatGPT ist ein KI-Modell, das auf Basis von vorherigen Texten trainiert wurde. Obwohl es viele Aufgabenstellungen unterstützen könne, seien seine Antworten immer kritisch zu hinterfragen und zu überprüfen, da sie möglicherweise nicht immer fehlerfrei oder vollständig wären. Dann gilt für den Medizininformatiker und Professor für Wirtschaftsinformatik: „Der Nutzen ist höher als der Schaden“.

Weitere Themen und Referenten waren: „Der Weg zum autonomen Datencenter“, Markus Biesinger, NUTANIX GmbH, Andreas Lockau, Niels-Stensen-Kliniken, Osnabrück; Sprachbot für die Patientenkommunikation Maaike Sloof, aaron.ai, Andreas Lockau, Niels-Stensen-Kliniken, Osnabrück; „Wer soll das alles befunden?“ Miriam Haustein, SIEMENS Healthineers, Strukturierte, interoperable Versorgungsdaten und ihre Anwendung in einem KI-gestützten klinischen Entscheidungsunterstützungssystem Dr. Moritz Augustin, Leiter Maschinelles Lernen, Tiplu GmbH.

Rückblick und Ausblick

Im Blick der Frühjahrstagung 2023 in Nürnberg standen gewandelte Aufgaben und Anforderungen für IT-Entscheider durch Integration und Interoperabilität. Vor allem geht es um Konzeption und Umsetzung von zukunftsweisenden Lösungen. Neben dem intensiven Austausch über aktuelle Trends, Entwicklungen und Erfahrungen vermittelte die KH-IT-Frühjahrstagung einen Überblick über den Stand von Künstlicher Intelligenz im Einsatz. Zugleich diskutierten die Teilnehmer in einer konstruktiven Auseinandersetzung das Potenzial von KI-Systemen, die potentiellen Risiken, Transformationshürden und Erfolgsorientierung.

Den Ausblick auf die Herbsttagung 2023 gab Jürgen Flemming, KH-IT Vorstand e.V. Als Themen stehen am 20. und 21.9.2023 auf der Agenda: Services und Vernetzung intern, extern, interoperabel sowie Telematikinfrastruktur mit den Aspekten KIM und TIM. Die Tagung findet in Präsenz im Universitätsklinikum Dresden statt. Am 21.9.2023 ist die Mitgliederversammlung und die Wahl der neuen Vorstände und des Kassenprüfers angesetzt.

Bundesverband KH-IT – aus der Praxis für die Praxis

Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V. KH-IT ist der führende Berufsverband der Krankenhaus-IT-Führungskräfte. Das Motto der Konzepte, Projekte und Lösungen lautet dabei: Aus der Praxis für die Praxis. Ausgewählte Industrieaussteller haben die Gelegenheit, zum Wissenstransfer für Anwender beizutragen. Der KH-IT veranstaltet jährlich eine Frühjahrstagung und eine Herbsttagung. Der KH-IT steht allen leitenden und/oder verantwortlichen Mitarbeitern der Krankenhaus-IT offen. Hören Sie das Interview mit Horst-Dieter Beha, KH-IT-Vorsitzender, über Stellung und Würdigung der IT in der Klinik, Unterstützung der IT-Verantwortlichen durch den KH-IT und Akzente des KH-IT mit Blick auf die Zukunft der Krankenhaus-IT.

www.kh-it.de

Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V.
Jürgen Flemming
Vorstandsmitglied/Pressereferent
www.kh-it.de – flemming@kh-it.de

Die Inhalte der Verbandsseiten werden redaktionell erstellt und betreut vom KH-IT. Der Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V. kurz KH-IT ist der führende Berufsverband der Krankenhaus-IT-Führungskräfte. Der KH-IT steht allen leitenden und/oder verantwortlichen Mitarbeitern der Krankenhaus-IT offen.

Herbsttagung des KH-IT am 20./21.09.2023 in Dresden: Cloudcomputing, Telematik, vernetzte Medizintechnik
Seminare (Online, Anmeldung über die KH-IT-Webseite)
Fit für die Cloud, Online, **20./21.07.2023**
Motivationsmöglichkeiten für Führungskräfte & Projektleiter, Online, **25./26.07.2023**
ITIL®4 Foundation, Online, **06. – 08.09.2023**

Teilnahme an den Seminaren auch für Mitarbeiter unserer Mitglieder möglich !

Health-IT-Talk in Berlin-Brandenburg (nach Ankündigung Berlin-Brandenburg)
Health-IT in Baden-Württemberg (nach Ankündigung Region Stuttgart)
Regionalveranstaltungen in Bayern (nach Ankündigung, München)
Regionalveranstaltungen in Sachsen/Sachsen-Anhalt (in Planung)
Weitere Regionalveranstaltungen in Vorbereitung

Health-IT-Talk Rhein-Main jetzt im Web: Wegen der Corona-Pandemie erfolgen die Treffen derzeit an jedem dritten Dienstag im Monat, jeweils um 20:00 Uhr, als Web-Meeting.

Alle Termine und Inhalte finden Sie auf der Website des KH-IT (www.kh-it.de). Einladungen zu den Regionalveranstaltungen erfolgen über die teilnehmenden Verbände und Mailinglisten. Die Kooperationen sind regional unterschiedlich ausgeprägt.

KI-basierte Automatisierung: Potenzial, Expertise, Akzeptanz

Künstliche Intelligenzen (KI) beherrschen derzeit die Schlagzeilen und der Erfolg [1] von ChatGPT hat eine wahre Welle an neuen Lösungen bzw. deren Veröffentlichung ausgelöst. Künftig wird die Technologie immer mehr Einzug in Unternehmen erhalten, um Prozesse zu beschleunigen, die Produktivität zu steigern und Angestellte zu entlasten. KI-basierte Automatisierung ist hier das Stichwort. Jan Schütze, Senior Design Authority bei Endava in Berlin, skizziert, wie Unternehmen diese Ziele erreichen können.

Wie so oft bei neuen Technologien geht auch aktuell mit Blick auf KI die Angst um, dass sie unzählige Jobs, wenn nicht gar ganze Branchen überflüssig machen wird. Doch sollten Unternehmensverantwortliche und Angestellte sich von dieser Sichtweise nicht beirren lassen, denn der Einsatz von KI und Automatisierung kann große Vorteile bringen.

Die Vorteile von KI-basierter Automatisierung

Laut dem aktuellen Emerging Technologies Report [2] von Endava sind bereits 88 Prozent der Unternehmensentscheider aus Deutschland mit der Technologie zu einem gewissen Grad vertraut und fast genauso viele (86 Prozent) stufen sie als relevant für ihr Geschäft ein. Denn KI-basierte Automatisierung kann in zahlreichen Anwendungsfällen, Branchen und Abteilungen zum Einsatz kommen.

Folgendes versprechen sich die Befragten dabei in erster Linie von der Technologie:

- Eine höhere Produktivität (33 Prozent)
- Eine höhere geschäftliche Effizienz (30 Prozent)
- Eine Reduzierung der Kosten (30 Prozent)

Von vielen dieser Vorteile profitieren Unternehmen einiger Branchen schon heute. Doch das Potenzial KI-basierter Automatisierung reicht weiter. ChatGPT und andere KI-Tools sind zum Beispiel in der Lage, (einfachen) Code in verschiedenen Programmiersprachen zu schreiben. Diese Fähigkeit könnte Unternehmen nicht nur helfen, Zeit zu sparen, sondern auch die Folgen des IT-Fachkräftemangels ein Stück weit abzufedern.

Langfristiger Erfolg dank der richtigen Strategie

An diesem Punkt sind bereits vier von fünf Unternehmen: Während 39 Prozent die Technologie bereits implementiert haben, befinden sich 41 Prozent derzeit auf dem Weg dahin – sie treiben die Einbindung entweder systematisch und ganzheitlich oder nur punktuell voran.

Letzteres kann sich schnell als nachteilig herausstellen, und zwar auf mehreren Ebenen. Zum einen können nahezu alle Abteilungen von KI-basierter Automatisierung profitieren – das beste Beispiel ist hier die Unterstützung beim Erstellen von Inhalten aller Art, wie wir es gerade sehen. Zum anderen steigt der Aufwand, wenn sich jede Abteilung um ihre eigene Lösung kümmert. Potenzielle Synergien oder ein Wissensaustausch bleiben dann ungenutzt.

Wenn Unternehmen keine umfassende Strategie für den Einsatz KI-basierter Automatisierung – oder anderer Technologien – verfolgen, steigt darüber hinaus die Wahrscheinlichkeit, dass sie sich mit der einmaligen Umsetzung zufriedengeben. Die Lösung wird dann zwar (hoffentlich) genutzt, aber nicht kontinuierlich weiterentwickelt.

Angesichts der großen Fortschritte, die KI-Systeme heute schon machen und die wir in den kommenden Jahren erwarten können, wäre dies jedoch fatal und ein Wettbewerbsvorteil würde sich in einen -nachteil drehen. Dementsprechend sollten die Verantwortlichen eine Strategie entwickeln, in der sie auf alle Unternehmensbereiche und -abteilungen blicken und das Potenzial der Technologie evaluieren – dies ist natürlich auch im Nachhinein noch möglich, wenn sie bereits mit der Implementierung begonnen haben.

Bei der Strategieentwicklung sollten aber noch zwei weitere Aspekte eine Rolle spielen:

Expertise – Für den Einsatz und die kontinuierliche Weiterentwicklung von KI-Anwendungen sind Fähigkeiten in Bereichen wie Softwareentwicklung und Machine Learning notwendig. Unternehmen können diese durch Neueinstellungen, interne Weiterbildungen und/oder Unterstützung durch Dritte entwickeln, integrieren und stärken.

Akzeptanz – Eine Anwendung wird nur genutzt werden, wenn das Team einen Nutzen darin sieht. Daher ist es wichtig, es für KI und Automatisierung zu begeistern. Dies kann gelingen, wenn man die Angst vor einem möglichen Jobverlust nimmt und aufzeigt, welche Vorteile die Technologie für einen ganz persönlich bringt.

Die Strategie sollte nicht in Stein gemeißelt sein, sondern sich flexibel an neue Gegebenheiten anpassen lassen und generell regelmäßig überprüft werden, ob sie noch den Bedürfnissen des Unternehmens entspricht. So kann nicht nur der Einstieg, sondern auch die Nutzung von KI-basierter Automatisierung dauerhaft Erfolg bringen.

(1) 100 Millionen Nutzer in zwei Monaten: Hype um ChatGPT, Handelsblatt GmbH, 07. März 2023
(2) NEUE TECHNOLOGIEN AUSGEPACKT, https://info.endava.com/emerging-tech-unpacked

Jan Schütze, Senior Design Authority bei Endava in Berlin

Highlights vom 18. KRITISchen Stammtisch

Cybersecurity – Herausforderung für alle Krankenhäuser

Mit Vorträgen und Diskussionen zu IT-Sicherheit und Informationssicherheit wendet er sich inzwischen an alle Krankenhäuser: der KRITISche Stammtisch. Datenschutzbeauftragte (DSB), Informationssicherheitsbeauftragte (ISB), Krankenhaus-IT-Leiter sowie Vertreter von Verbänden, Behörden und der Industrie kommen online zusammen. Veranstalter sind das Universitätsklinikum Carl Gustav Carus der TU Dresden und die SHD System-Haus-Dresden GmbH. Auch die 18. Ausgabe im Frühjahr war wieder geprägt von aktuellen Informationen, Best Practice und Antworten auf drängende Fragen. Hier kommen ausgewählte Highlights.

Aus den DKG-Arbeitskreisen

Aktuelles aus den KRITIS-Arbeitskreisen zum B3S und OH-Systemen zur Angriffserkennung präsentierte beim Stammtisch Markus Holzbrecher Morys, DKG-Geschäftsbereichsleiter Digitalisierung und eHealth. So beschäftigt sich der Branchenarbeitskreis (BAK) „Medizinische Versorgung“ der Kooperation UP KRITIS mit der Verbesserung der Informationssicherheit in Krankenhäusern. Er bezieht sich auf die IT-Sicherheitsgesetze (BSIG) und den dort vorgeschriebenen „Stand der Technik“ (§ 8a BSIG, BGBl. 2015a, S. 1325). Der Branchenstandard B3S v1.2 adressiert die Anforderungen der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OH SzA) – also das „Was“, so Holzbrecher-Morys. Eine enorme Herausforderung sei die Umsetzung zum 1.5. der konkreten Anforderungen der geforderten SzA-Reifegradstufe 3. Daher hatte der BAK Hinweise zum „Wie“, zur Herangehensweise, veröffentlicht. Verantwortliche sollten die Anforderungen, so Holzbrecher-Morys, im Kontext der erwarteten Prüfungen einordnen. Beispielhaft beschrieb er das plausible Vorgehen anhand der SIEM-Einführung.

„Nach der Einreichung ist vor der Einreichung“ konstatierte der DKG-Vertreter zu den Aktivitäten der Arbeitsgruppe „B3S Überarbeitung“: Die Arbeiten zur Version 2.0 hätten bereits begonnen. Die AG beschäftige sich ferner mit einem Forschungs- und Entwicklungsprojekt mit dem Team um Prof. Pilgermann von der TH Brandenburg zu SzA. Die Anpassungshinweise, die noch nicht in Version 1.2 aufgegriffen worden waren, sollen in einer größeren, strukturellen Überarbeitung ihren Platz finden. Die Einreichung der Überarbeitung ist für Mitte / Ende 2024 geplant.

Die Einreichung des B3S zur Eignungsfeststellung sei im März 2022 beim BSI erfolgt, erinnerte Holzbrecher-Morys. Parallel habe eine Umorganisation innerhalb des BSI stattgefunden; die Zuständigkeit liege nun im Referat „Grundsatzfragen“. Noch vor Feststellung der Eignung des B3S erfolgte die Veröffentlichung der OH SzA; das BSI forderte die nachträgliche Berücksichtigung der neuen Vorgaben der OH SzA.

Die Feststellung der Eignung nach §8a Abs. 3 BSIG erfolgte nach umfangreichen Anpassungen im Januar dieses Jahres. Die Anforderungen der OH sind laut Holzbrecher-Morys in B3S v1.2 abgebildet.

Die DKG-Arbeitsgruppe zum § 75c SGB V hatte zum Zeitpunkt des Stammtisches die finale Bearbeitung einer Kostenstudie zur Umsetzung dieser gesetzlichen Vorgaben in Arbeit. Danach ist die Fortführung der Umsetzungshinweise der DKG zu folgenden Themen geplant: Anpassungen aufgrund der Fortschreibung des B3S; neue Arbeitshilfen und Vorlagen hinsichtlich Anforderungen an Dienstleister und Logistik sowie Assetmanagement. Eine zweite Informationsveranstaltung hierzu soll es im zweiten Quartal geben. Die Aktivitäten „B3S“ und „75c SGB V“ sollen zusammengeführt werden.

Als Ausblick aus der Sicht UP KRITIS, BMI und BSI nannte Holzbrecher-Morys, die allgemeine Bedrohungslage mit Blick auf den Ukraine-Krieg sei „abstrakt hoch“. Eine merkliche Verschärfung der behördlich organisierten Aufsichtsfunktion stehe an – durch Erhebung der Mängellisten alle drei Monate. Die Vakanz an der Spitze des BSI werde ab Juli 2023 durch Claudia Plattner besetzt. Das BMI habe die Resilienzstrategie des Bundes vorgestellt; und für unsere Branche sei die Krankenhaus Reform als „große Unbekannte“ zu betrachten, insbesondere mit Blick auf die Level 1i-Häuser.

Angriffsvektoren und Notfallmanagement

Über Best Practice bei typischen Angriffsvektoren und Notfallmanagement sprach Alexander Sparbrod. Er Leiter leitet die Stabsstelle Informationssicherheits- und Datenschutzmanagement am Universitätsklinikum Jena und baute dort das ISMS nach ISO 27001 auf. Zu den häufigsten Informationssicherheitsvorfällen Krankenhaus von extern zählen laut Sparbrod Phishing-E-Mails zum Abgreifen von Benutzerzugängen, Vireninfektion auf Endgeräten durch Downloads oder E-Mails, Vireninfektion auf Serversystemen, z.B. durch Ausnutzung von Schwachstellen sowie der Diebstahl von IT-Equipment, etwa Datenträgern.

Intern bedingte Vorfälle seien insbesondere der Missbrauch von Benutzerberechtigungen, Ausfall zentraler (kritischer) IT-Systeme und ungesperrte sowie verlassene Endgeräte, die eine unbefugte Einsichtnahme durch Externe ermöglichen. Im März, so der ISB, seien am UKJ insgesamt 9,3 Millionen E-Mails eingegangen, von denen nur rund sechs Prozent zugestellt wurden. Der E-Mail-Filter blocke Mails aufgrund definierter Eigenschaften.

Häufigste angriffe würden verursacht durch Schadsoftware und Trojaner, Bot-Netzwerke sowie CEO Fraud, Phishing und Social Engineering. Die potenziellen Folgen reichten von Schaden für Leib und Leben sowie für die Reputation bis hin zu finanziellen Schäden.

Der Mensch als Schwachstelle stehe im Fokus beim Social Engineering, führte Sparbrod aus. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität würden ausgenutzt, um Personen geschickt zu manipulieren. Je mehr persönliche Informationen Angreifern zur Verfügung stünden, desto eher hätten sie Erfolg. „Der Mensch ist das schwächste Glied der Sicherheitskette“, betonte der ISB.

Die Angriffsziele seien vielfältig. Zu ihnen zähle das Ausspähen wertvoller Firmeninformationen ebenso wie Identitätsdiebstahl für Internetbestellungen und Zahlungen, Erpressung von Geldmitteln oder politischen Entscheidungen oder das Ziel, Unternehmen in ein schlechtes öffentliches Licht zu rücken. Patientenakten seien hier ein spezielles Gut.

Der Handel mit Gesundheitsinformationen floriere, so Sparbrod: Gesundheitsinformationen seien auf dem Schwarzmarkt wertvoller als Kreditkartendaten oder „normale“ personenbezogene Daten. Eine Krankenakte könne auf dem Schwarzmarkt für bis zu 335 Euro verkauft werden, andere personenbezogene Daten hingegen nur für 1 bis 2 Euro. Dies liege daran, dass die persönliche Gesundheitsgeschichte im Gegensatz zu Kreditkarteninformationen oder Sozialversicherungsnummern nicht geändert werden könne. Gesundheitsdaten könnten beispielsweise zur Erpressung des Opfers genutzt werden, z.B. mit Androhung der Veröffentlichung der Daten, wenn eine bestimmte Summe nicht gezahlt werde. Gesundheitsdaten könnten auch verwendet werden, um gefälschte Versicherungsansprüche zum Kauf und Weiterverkauf medizinischer Geräte zu ermöglichen. Einige Kriminelle würden Gesundheitsdaten verwenden, um sich illegal Zugang zu Rezepten zu verschaffen.
Als Beispiel für CEO Fraud beschrieb der UKJ-ISB die vermeintliche Eröffnung einer neuen Geschäftsstelle eines Lieferanten. Betrüger würden so Zahlungen auf ein illegitimes Konto bewerkstelligen.

Mit einem Katalog an Maßnahmen gehe das UKJ gegen Social Engineering vor, beschrieb Sparbrod. Sensibilisierung in betroffenen Abteilungen (transparenter Umgang mit Vorfällen); Richtlinien zur Informationsklassifikation – welche Informationen dürfen nach außen gegeben werden; etablierte Kontrollen zur Absicherung bei Kontodatenänderungen und Änderungen im Zahlungsverkehr.

Ein beispielhaftes Angriffsszenario beschrieb der ISB so: Beim Risiko gehe es um das Abgreifen von User Accounts. Mögliche Auswirkungen seien das Ausspähen personenbezogener Daten und der Zugriff auf sensible Informationen. Als Schutzmaßnahme der IT beschrieb Sparbrod die Sperrung der Webseiten, Sensibilisierung der Mitarbeitenden im Intranet und Multifaktorauthentifzierung.

Eine wichtige Rolle für Angriffsvektoren spielten Webserver, E-Mail-Server, Webmail-Zugang und VPN-Zugang. Der ISB illustrierte dies anhand des Weges, den ein infizierter Excel-Anhang in einer Personalabteilung nehmen kann. Als top Sicherheitsmaßnahmen kämen infrage: Endpoint security, mindestens Endpoint Detection and Response, EDR; Netzwerksegmentierung / VLAN-Segmentierung; minimale Berechtigungen; Datensicherung mit Backupstrategie und Offline-Backups; ein Logging-/Monitoringsystem.

Die Bedrohung ist real, erklärte Sparbrod anhand einer umfangreichen Liste von Vorfällen an Krankenhäusern in Deutschland und im europäischen Ausland. Ein Notfallmanagement sei daher essenziell. Am UKJ sei noch kein großflächiger Ransomwarevorfall eingetreten, da die bisher etablierten Maßnahmen die Auswirkung von Schadsoftware eingedämmt hätten. Der Vorfall am UK Düsseldorf habe große Bereitschaft und Sensibilität beim UKJ-Vorstand ausgelöst; es sei investiert worden, um ein dokumentiertes IT-Notfallmanagement zu etablieren.

Erfahrungsberichte zeigten beispielsweise, dass ein Tag Ausfall in einem Klinikum mit ca. 1400 Betten und 55.000 stationären Fällen pro Jahr rund 1 Million Euro koste. Die Einbindung externer Forensiker, Firmen bzw. Behörden wie dem LKA führe zu etwa 12 bis 15 Tage Handlungsunfähigkeit. Solche Faktoren hätten zu einer Neubewertung des Risikos geführt.

Notfallpläne müssten IT- und Nicht-IT-Komponenten abzudecken, betonte Sparbrod. Anforderungen seien aus ISO 27001 (Annex A.17) und B3S (V1.2 Kapitel 6.4) abzudecken. Verantwortliche sollten ein Notfallhandbuch in der Version 1.0 beginnen und kleine Schritte verabschieden lassen. Prioritäten sollten liegen auf dem Festlegen von Rollen/Verantwortlichkeiten, dem Sammeln und Dokumentieren von Kontakten, der Definition der Lage – Störung oder Notfall, dem Kommunikationsablauf, den Sofortmaßnahmen und Wiederherstellungsplänen. Themen für Sofortmaßnahmen seien Stromausfall, Ausfall Telefonie, Ausfall Kälteversorgung, großflächige Virenifektion, Ausfall zentraler Netzwerkkomponenten, Ausfall medizinischer Applikationen und Ausfall des Internets.

„Übung macht den Meister!", unterstrich Sparbrod. Regelmäßige kleinere Übungen seien erfolgversprechend. Die Fachabteilungen müssten eingebunden werden, ein Drehbuch sei zielführend. Antworten müssten gefunden werden auf Fragen wie „Ist die Telefonie nach Netzwerktrennung noch funktionstüchtig? Wie und wo können neue Passwörter an alle Mitarbeiter ausgegeben werden?". Web-/Informationsseiten sollten nach extern verlagert werden, um alle Betroffenen informieren zu können. Im Fall von Ransomware sollten Server nicht heruntergefahren, sondern nur unverzüglich vom Netzwerk getrennt werden, so der ISB.

Systeme zur Angriffserkennung (SzA)

Zur Überführung von SzA in den B3S MV 2.0 sprach beim Stammtisch Prof. Dr. Michael Pilgermann. Er arbeitet in der Forschungsgruppe MedSec im Fachbereich Informatik der Technischen Hochschule Brandenburg. Kernpunkte des Sicherheits-Leitstandes in der Detektions-Infrastruktur / Security Operations (Netzwerksicherheit) lauten: prompte Erkennung & Behandlung von Sicherheitsvorfällen; SIEM-Kern, auch als Basis für forensische Analysen; die Einbindung von Sektor-Spezifika aus dem Gesundheitswesen, wie KIS, HL7 und mehr; Integration der Netzsicherheitssysteme, etwa Firewall und IDS; Leitstands- und Krisenstabs-Organisation; Resilienz der Prozesse.

Als regulatorischer und normativer Rahmen für Detektion beim Betrieb Kritischer Infrastrukturen, sagte Prof. Pilgermann, seien zu sehen: IT SiG 1.0, Kritische Infrastrukturen zum Stand der Technik und mit Meldepflichten; IT SiG 2.0 mit Auflagen zur Angriffserkennung (geltend seit Mai) sowie § 75c SGB V mit Ausweitung IT-Sicherheit zum Stand der Technik auf alle Krankenhäuser. Der Experte beschreib den Zeitplan für die Umsetzung der Vorgaben bis 2024. Anforderungen umfassen Protokollierung, Detektion und Reaktion; Nachweise sind zu erbringen, auch für den erreichten Grad im Umsetzungsgradmodell.

Die Umsetzung im Rahmen des Umsetzungsgradmodells sollte laut Prof. Pilgermann beinhalten: Grad 3 – Erfüllung aller „Muss"-Anforderungen für alle Bereiche. Idealerweise wurden „Sollte"-Anforderungen sind hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft, ein Verbesserungsprozess ist etabliert oder in Planung. Grad 4 – hierauf aufbauend: Alle „Sollte"-Anforderungen sind erfüllt, außer sie wurden stichhaltig und nachhaltig ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Als Vorgehensvorschlag für den Anteil SzA in der Fortschreibung des B3S fasste der Hochschulvertreter inhaltliche Handlungsfelder zusammen – nach der Erstanalyse der OH SzA hinsichtlich des Konkretisierungsbedarfs in der Branche. Zu ihnen zählen:

- Branchenspezifische Risikolage inkl. branchenspezifischer Bedrohungen
- Branchenspezifische Prozesseigenheiten und Abhängigkeiten
- IT-Systemarchitektur: branchenspezifische Strukturanalyse inkl. Netzplan
- Übersicht über eingesetzte Detektions-Technologien
- Branchenspezifische Regeln und Normen
- Anonymisierung/Pseudonymisierung von Protokoll(ierungs)daten
- Protokollierungsfähigkeit von Medizintechnik
- Automatisierungspotentiale für die Reaktion.

Als Arbeitsschritte stehen in der Projektlaufzeit bis April 2024 Bestandsaufnahme, Ableitung von Handlungsempfehlungen und Formulierungsvorschläge zur Überführung an. Betreiber von Krankenhäusern seien durch Workshops und bei der Entwicklung von Fragebogen eng eingebunden, sagte der Experte. Er regte alle Krankenhausvertreter zur Mitwirkung an.

Neuen Input zur „Neverending Story" von IT- und Informationssicherheit für Krankenhäuser bietet der nächste KRITISche Stammtisch am 28. Juni: Mehr unter https://kritischer-stammtisch.de/.

Enormes Interesse am RöKo 2023

Eindrücke vom 104. Deutschen Röntgenkongress

Wie im letzten Jahr, fand der Deutscher Röntgenkongress (RöKo) auch dieses Jahr vom 17. bis 19. Mai 2023, erneut in den Hallen und Sälen des RheinMain CongressCenters (RMCC) in Wiesbaden statt. Die diesjährige Kongresspräsidentin war Univ.-Prof. Dr. Christiane Kuhl und das Kongressmotto hieß „Abenteuer Forschung". In den Hallen und Sälen des RMCC wurden, außer dem vielfältigen wissenschaftlichen Angebot, auch die Produktneuigkeiten und -lösungen vorgestellt. Seine Eindrücke von diesjährigem RöKo in Wiesbaden schildert Dr. Aykut Uslu, Berater für Projektierung in der Medizintechnik und Medizin-IT.

KI kann nicht besser sein als der beste Radiologe

Die Eröffnungsveranstaltung des Präsenzteils des Kongresses am Mittwoch, 17. Mai 2023 widmete sich dem Thema „Möglichkeiten und Grenzen des Einsatzes künstlicher Intelligenz in der Radiologie". Hauptredner waren Prof. Jörg Debatin, bis Ende 2021 Leiter des Health Innovation Hub des Bundesgesundheitsministeriums, und Prof. Michael Forsting, Leiter des Institutes für Diagnostische und Interventionelle Radiologie und Neuroradiologie sowie des Instituts für KI in der Medizin (IKIM) an der Universitätsmedizin Essen. Sie vertraten beide übereinstimmend die Meinung: Der Einsatz künstlicher Intelligenz (KI) birgt für die medizinische Entwicklung großes Potenzial und kann etwa die Radiologie in der Diagnostik und bildgeführten Therapie unterstützen, besonders bei der Effizienz, Genauigkeit und Geschwindigkeit von Diagnosen. Bereits jetzt werden KI-gestützte Lösungen zum Beispiel im Lungenkarzinom-Screening oder in der Mammadiagnostik eingesetzt und dabei vor allem in der Früherkennung. Wenn es um Quantifizierung geht, wird KI das gut lösen können, ob sie etwa alle Differenzialdiagnosen am Ende sicher in eine richtige Diagnose umwandelt, ist noch nicht hinreichend belegt - KI kann auch nicht besser sein als der beste Radiologe.

Die Hauptredner der Eröffnungsveranstaltung waren Prof. Jörg Debatin und Prof. Michael Forsting – mit dem Thema „Möglichkeiten und Grenzen des Einsatzes künstlicher Intelligenz in der Radiologie". (Bildquelle: DRG / Thomas Rafalzyk)

Neues Gesundheits- und Berufspolitisches Format

Mit dem neugeschaffenen „Forum Beruf" will die Deutsche Röntgengesellschaft Debatten und Entwicklungen im Gesundheitssektor gestalten und versuchen, eigene Vorstellungen umzusetzen. Drängendste davon dürften die Themen Krankenhausreform, Ambulantisierung, Aufweichung der Fachgebietsgrenzen und Fachkräftemangel, sein – diese und viele weitere Themen bestimmen die Gegenwart und Zukunft der Medizin und auch der Radiologie. Die geplanten Veranstaltungen auf dem „Forum Beruf" umfassen unter anderem Themen rund um die Niederlassung in der Radiologie, zunehmende Aktivitäten von Finanzinvestoren sowie Themen der Weiterbildungsordnung und der Zertifizierung. Sprecher Gesundheitsstrategie des Vorstandes der DRG ist der Prof. Gerald Antoch aus Uni Düsseldorf fasste die Ziele des Forums mit „Das Forum Beruf versteht sich als Plattform für Themen der Gesundheitsstrategie und des Berufsrechts. Es soll die Teilnehmenden des Kongresses für diese Themen sensibilisieren und ihnen die Möglichkeit des Austausches geben".

Herz-CT als Kassenleistung

Die Computertomographie des Herzens (Herz-CT) ist eine nicht-invasive Methode und dient zur Quantifizierung des Koronarkalks in den Herzkranzgefäßen. Mit ihr kann eine schonende, schnelle und aussagekräftige Beurteilung der Herzkranzgefäße erfolgen. Bislang konnte die Diagnose einer koronaren Herzerkrankung (KHK) nur durch eine invasiv durchgeführte Herzkatheteruntersuchung gesichert werden. Kardio- oder Herz-CT wird zwar in Leitlinien bei diversen Herzerkrankungen als Diagnostik empfohlen, fand jedoch bislang keinen Eingang in den Regelleistungskatalog der gesetzlichen Krankenversicherung. Doch jetzt kommt Bewegung in die Sache: Beim RöKo 2023 gab Prof. Jörn Sandstede, Hamburg, während seines Vortrages bekannt, dass der Gemeinsame Bundesausschuss (G-BA) das Beratungsverfahren zur koronaren CT-Angiographie bei Patient:innen mit Verdacht auf chronische KHK, eingeleitet hätte. Er fügte hinzu: „Im Februar 2024 dürften die Voraussetzungen für die Vergütung der Herz-CT erfüllt sein". Und, möglicherweise kurz darauf, wird die kardiale CT eine Kassenleistung. Allerdings müssten bis dahin noch einige Fragen hinreichend geklärt werden wie z.B. wer die Untersuchung macht und wer zuweist. Die Höhe einer angemessenen Vergütung steht ebenfalls noch im Raum.

Juniorreporter auf dem RöKo

Ende Oktober letzten Jahres wurde in Remscheid-Lennep die Wilhelm Conrad Röntgen-Juniorakademie gegründet, um junge Menschen frühzeitig mit Forschungsthemen in Berührung zu bringen und ihre Leidenschaft für Medizin und Naturwissenschaften zu fördern. Das Pilotprojekt startete am 10. März 2023 im Deutschen Röntgen-Museum. 12 Schülerinnen und Schüler ausgewählter Remscheider Schulen im Alter von 8 bis 12 Jahren erarbeiten in einem dreimonatigen Programm ein selbst gewähltes Thema. Die Aktion „Juniorreporter auf dem RöKo 2023" war für den 18. Mai 2023 von ca. 10-17 Uhr geplant. Die Kinder wurden um 10 Uhr im Foyer / Eingangsbereich des RMCC in Empfang genommen, erhielten im Pressebereich nach einer kurzen Begrüßung eine allgemeine Einführung zum Kongress und zum Veranstaltungsort, gefolgt von einem Basic-Workshop zu Filmtechnik und allgemeinen journalistischen Fertigkeiten in Theorie und Praxis. Anschließend zog das Reporter-Team los und besuchte vorgegebene Orte im RMCC, um mit den jeweils anwesenden Personen kurze Interviews durchzuführen und interessante Momente/Perspektiven mit der Videokamera einzufangen.

Das Pilotprojekt „Wilhelm Conrad Röntgen-Juniorakademie“ startete am 10. März 2023 mit 12 ausgewählten Schülerinnen und Schüler im Alter von 8 bis 12 Jahren, in Remscheid-Lennep. (Bildquelle: DRG / Thomas Rafalzyk)

Weitere interessante Entwicklungen

- Fort- und Weiterbildungsangebot: Die Teilnehmenden des Präsenzteils des 104. Deutschen Röntgenkongresses sahen sich einem Überangebot an Fort- und Weiterbildungsangebot gegenüber. Dabei die richtige Wahl zu treffen, wurde außer dem parallelstattfinden interessanten Veranstaltungen, auch die Anziehungskraft der prallen Sonne, erheblich beeinflusst.
- Kleinere Ausstellungsflächen: Dem Anschein nach waren die Ausstellungsflächen insgesamt kleiner geworden, bei gleichzeitiger Zunahme der Ausstellenden. Außerdem waren beide Hallen, an allen Tagen, gut besucht.
- Kinderbetreuung auf dem RöKo: An allen Tagen während der Kongresszeiten konnten die Kongressteilnehmenden Eltern ihre mitgebrachten Kinder direkt im RheinMain CongressCenter (RMCC) betreuen lassen – von einem Team aus pädagogisch ausgebildeten Mitarbeiterinnen und Mitarbeitern. Angemeldet werden konnten Kinder ab ca. 12 Monaten. Für Kinder ab ca. 3 1/2 Jahren gab es ein erweitertes Ausflugsangebot. Für die Betreuung und Verpflegung im RMCC wurde ein Kostenbeitrag von € 5,- pro Tag und Kind erhoben.

Save The Date „08. - 10. Mai 2024“

Der 105. Deutsche Röntgenkongress / 10. Gemeinsamer Kongress der DRG und ÖRG findet voraussichtlich vom 06. März-22. Juni 2024 online und vom 08.-10. Mai 2024, in Präsenzform – erneut in den Hallen und Sälen des RheinMain CongressCenters (RMCC).

www.drg.de/
www.uslumedizininformatik.de/

Dieses Bild gab es öfter: Draußen pralle Sonne, drinnen prallvolle Säle. (Bildquelle: DRG / Thomas Rafalzyk)

Dr. Aykut M. Uslu, Berater Medizintechnik und Medizin-IT, www.uslumedizininformatik.de

DMEA 2023: Zum aktuellen Stand der Cybersicherheit im Gesundheitswesen

Bericht von Ingo Buck, Vorstand von OGiTiX, ein Imprivata-Unternehmen

Auch dieses Jahr war Imprivata, das Unternehmen für digitale Identitäten für systemrelevante Branchen, wieder auf der DMEA vertreten. Das mit über 16.000 Besuchern deutlich gestiegene Besucheraufkommen machte sich deutlich bemerkbar: Es herrschte reger Betrieb am Imprivata-Stand. Deutlich mehr Besucher als im letzten Jahr informierten sich in Live-Demos über die Produktpalette von Imprivata, die durch die Übernahme von OGiTiX erweitert wurde. Gemeinsam bieten Imprivata und OGiTiX das einzig umfassende und eng integrierte Lösungsportfolio für digitale Identitäten an, das Identity & Access Management, Single Sign-On, Privileged Access Management und mobile Lösungen umfasst. Zusammen werden dies die einzigen Lösungen mit einer dedizierten Integration mit Dedalus Orbis sein, dem vorherrschenden klinischen Informationssystem in der Region. Auch mobile Arbeitsabläufe stießen auf großes Interesse. Die Besucher interessierten sich dafür, wie ein SSO-Workflow für gemeinsam genutzte mobile Geräte es Krankenhäusern ermöglicht, das volle Potenzial mobiler Geräte auszuschöpfen, indem ein schneller, effizienter Arbeitsablauf für das Krankenhauspersonal gewährleistet und gleichzeitig die Sicherheit und Überprüfbarkeit beibehalten und verbessert wird.

Die DMEA 2023 war ein voller Erfolg. Doch welche Themen spielten dieses Jahr in den vielen Gesprächen mit Gesundheitsorganisationen und Partnern aller Art die wichtigste Rolle?

Cybersecurity ist in aller Munde

Cybersecurity ist ein zentraler Bestandteil des KHZG, denn gerade Krankenhäuser geraten zunehmend ins Visier von Cyberkriminellen.

Die gute Nachricht ist: Das Thema Cybersecurity ist im Gesundheitswesen definitiv angekommen. Imprivata befragte über 230 DMEA-Teilnehmer zur Cybersicherheit in ihren Einrichtungen. Die überwiegende Mehrheit (65 %) hält die Compliance- und Cybersecurity-Maßnahmen in ihrer Einrichtung für "sehr umfangreich". Beim Thema digitale Identitäten, das für die Cybersicherheit von zentraler Bedeutung ist, gibt etwa ein Drittel an, dass der Reifegrad ihrer Organisation bei der Verwaltung dieser "sehr ausgereift" sei, was bedeutet, dass digitale Identitäten über einen zentralen Hub verwaltet werden und flexible Integrationsmöglichkeiten bestehen.

KHZG zeigt Wirkung - jetzt geht es um die Umsetzung

Auch beim Thema KHZG geht es voran, wie die Umfrageergebnisse zeigen. Rund die Hälfte der Befragten gab an, dass dank des KHZG mehr in die IT investiert wurde. In direkten Gesprächen an Imprivatas Stand beklagen jedoch viele Gesundheitsorganisationen, dass trotz größerer finanzieller Mittel viele geplante IT-Projekte ins Stocken geraten. Grund dafür sind ein Mangel an Fachkräften und Partnerunternehmen. Um diese Lücke zu schließen, werden daher Managed Services immer wichtiger, bei denen der Evaluierungs- und Implementierungsprozess mit dem Softwareprodukt mitgeliefert wird.

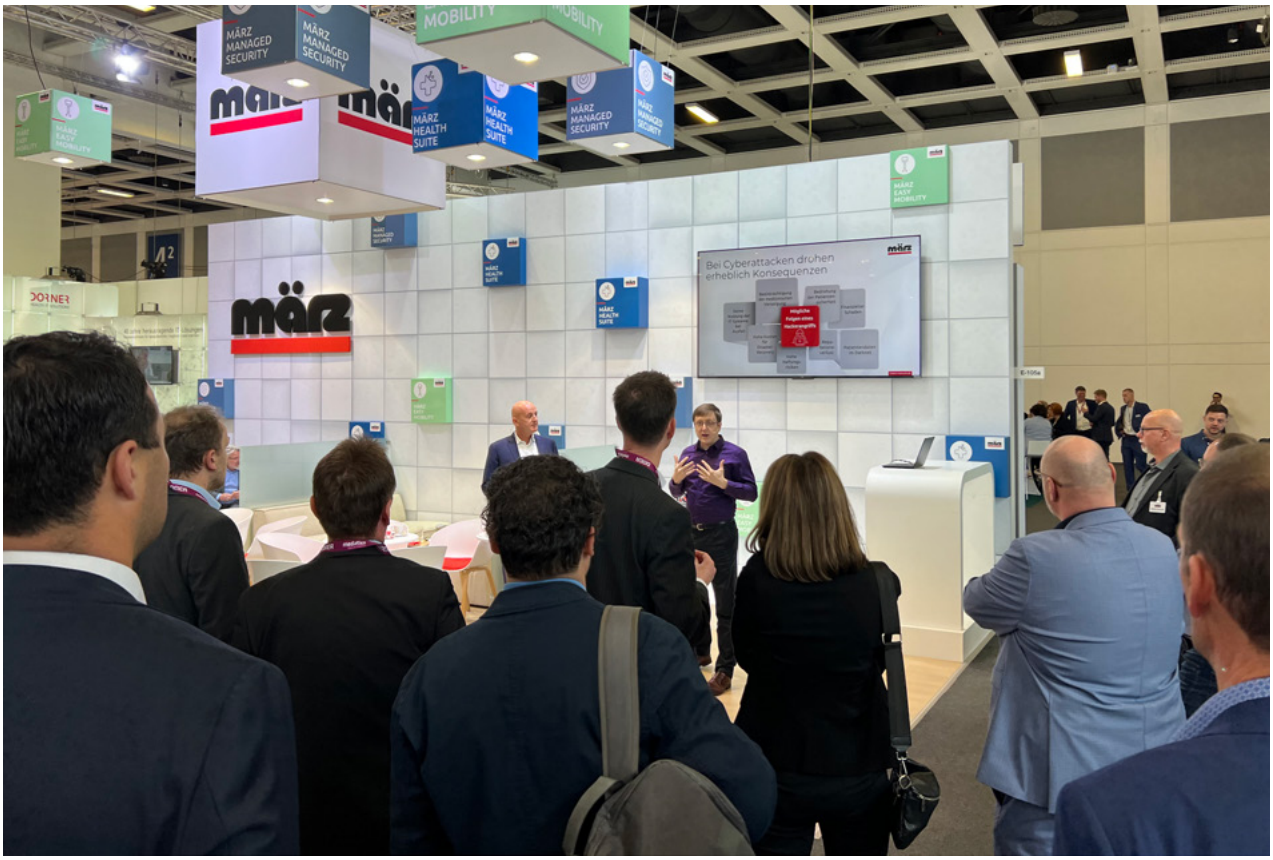
Es gibt noch viel zu tun

Insgesamt zeigen sich nach drei intensiven Tagen auf der DMEA viel guter Wille und vielversprechende Projekte. Es zeigt sich aber auch, dass der Stand des digitalen Identitätsmanagements und der Cybersecurity/Compliance stark auseinanderklaffen. Nur 33% stufen das digitale Identitätsmanagement ihres Unternehmens als "sehr ausgereift" ein (im Vergleich zu 65%, wenn es um Cybersicherheit und Compliance geht). Die relative Mehrheit (40%) bezeichnet das digitale Identitätsmanagement als "durchschnittlich" und mehr als ein Viertel (26%) findet es "nicht sehr ausgereift".

Einrichtungen des Gesundheitswesens sollten die digitale Identitäts- und Zugangsverwaltung mit Compliance und Cybersicherheit in Einklang bringen. Eine ganzheitliche Plattform für das Identitäts- und Zugriffsmanagement (IAM) stellt nicht nur sicher, dass nur autorisierte Nutzer Zugang zu sensiblen Daten haben und die Compliance-Anforderungen erfüllt werden, sondern spart auch wertvolle Zeit im Krankenhausalltag und verbessert so die Qualität der Pflege. Durch die Zusammenarbeit mit einem strategischen Partner und die Konsolidierung von Anbietern im Bereich IAM können Gesundheitseinrichtungen eine effektive Strategie für die digitale Identität entwickeln, die den aktuellen Stand der Systeme, Prozesse und Arbeitsabläufe berücksichtigt. Die sorgfältige Planung und Umsetzung einer digitalen Identitätsstrategie mit einem strategischen IT-Partner hebt die Cybersicherheit von Organisationen auf ein neues Level.

Wenn Sie mehr über Imprivata und OGiTiX erfahren möchten, besuchen Sie bitte unser DMEA Resource Center:

Wir freuen uns auf die nächste DMEA vom 09. bis 11. April 2024!



Breites Informationsangebot bei März auf der DMEA

Mobility, Nachhaltigkeit, Vernetzung, Informationssicherheit, Interoperabilität

Große Aufmerksamkeit erhielt der Stand der März AG auf der DMEA: Der IT-Anbieter hatte hochkarätige Referentinnen und Referenten eingeladen, über wichtige Markttrends und Lösungsangebote zu sprechen – Experten, Kunden und Partner.

Die Digitalisierung im deutschen Gesundheitswesen hat inzwischen enorm an Dynamik zugelegt, betonte Dr. Gerald Gaß. Das, so der DKG-Präsident am März-Stand, fordere die Managementkompetenz und die Personalressourcen der Krankenhäuser in hohem Maße: „Wir sind ein Stück weit Getriebene – aber treiben uns auch selbst, weil das Thema unheimlich wichtig ist“. Ein wichtiger Katalysator sei das KHZG mit seinen Fördermitteln und Sanktionsdrohungen. Die engen Fristen bei der Vielzahl von Projekten lassen sich insbesondere durch den Mangel an Personalressourcen nicht einhalten – seitens der Krankenhäuser ebenso wie bei den Dienstleistern, die bereits gut ausgelastet waren, sagte Dr. Gaß. „Diese Entwicklungen führen die Häuser jedenfalls auf ein höheres Niveau der Technologie“: Während vor dem KHZG die IT-Ausstattung bei den Krankenhäusern sehr heterogen gewesen sei, geschehe jetzt eine Anpassung. Eine zentrale Herausforderung, unterstrich der DKG-Präsident, sei die Interoperabilität – die Anbindung ans KIS sowie intersektoral.

Digitalisierung beschleunigt

„Wir müssen noch schneller werden“, merkte Dr. Gaß an. Sein Ausblick lautete: „Die Politik muss Schritte nach dem KHZG planen, Fristen verlängern und die Weiterfinanzierung gewährleisten. Für die ePA müssen die Daten aus den Krankenhäusern automatisiert einfließen – bis das funktioniert, ist noch viel Arbeit zu leisten“.

Der Alltag in Krankenhäusern sei äußerst herausfordernd – insbesondere hinsichtlich der Fristen, stellte auch Markus Holzbrecher-Morys fest. „Im Rahmen der Arbeiten an den Sanktionsvereinbarungen ist Flexibilität eine wichtige Anforderung", sagte der Geschäftsführer IT, Datenaustausch & eHealth bei der DKG. Zu sehen sei das etwa im Kontext des KIS, das bei laufenden KHZG-Arbeiten abgekündigt wurde. Auch sei nach dem Prozessabschluss „Ausschreibung, Zuschlag und Unterschrift" mitunter ein Beginn erst 2025 möglich – „so reißt man die Deadline".

Die KHZG-Fördertatbestände bilden eine solide Basis, um die Krankenhäuser voranzubringen, sagte Holzbrecher-Morys. So schaffe die zentrale Bereitstellung von Daten das Fundament für die Zukunft. Auf dieser Basis kann KI ein Fortschrittspotenzial für die Medizin bringen; hierbei liegen die Herausforderungen etwa beim Schaffen von Vertrauen. „Aber sicher birgt diese Entwicklung ein ganz enormes Fortschrittspotenzial."

Daten mobilisieren

Medizinische Daten für die digitale Visite und Pflege mobilisieren – auch dieses Angebot hatte März nach Berlin mitgebracht. Die mobile, elektronische Patientenakte mit der dazugehörigen IT-Infrastruktur professionell betreiben und Daten orts- und zeitunabhängig zugreifbar machen – dies gelinge dank März Hosp.IT Easy Mobility, so die Botschaft am Stand. Diese modulare Betreiberlösung hält die mobile IT bei plan- und überschaubaren Kosten verfügbar und gewährleistet, dass Krankenhäuser auf dem aktuellsten Stand der Technik handeln.

Cyber Security

Ransomware stellte Martin Tschiersich von zentrust partners als eine der kritischsten Bedrohungen für die Krankenhäuser dar. Er nannte Log4j als Beispiel. Das Gesundheitswesen ist für Kriminelle attraktiv, weil dort hohe Umsätze zu holen sind. Schützen können sich die Häuser laut Tschiersich zum Beispiel bei den „low hanging fruits": Die Bestandaufnahme und Bewertung verwundbarer Komponenten bei Hard- und Software, also Asset Management, stünden im Mittelpunkt. In der Zukunft, sagte der Experte voraus, würden KI und Large Language Models (LLM) auf Angreiferseite zum Einsatz kommen. Neue Schlagzahlen, neue Verwundbarkeiten kämen dadurch ins Spiel. Mindern ließen sich die Folgen ggf. durch KI-Einsatz auch auf der Seite der Verteidigung.

Digitalisierungsplatform Distance

Allgemeinkrankenhäuser an die digitale Infrastruktur anbinden – so lautet das Ziel des Projekts „Distance", erläuterte Dr. Denise Molinnus. Im Fokus steht hier, Daten aus dem klinischen Alltag zu generieren und auszuwerten, auch für Zwecke der Forschung, fuhr die Senior Projektmanagerin DISTANCE beim Universitätsklinikum RWTH Aachen fort. Das Konsortium beinhalte Partner aus Leipzig sowie Jena und zwölf Rollout-Partner, mit denen die Infrastruktur aufgebaut wird. Im Verbundprojekt ermöglicht die Picos-App das Nachvollziehen longitudinaler Datenverläufe stationärer Fälle. Patienten nutzen die App nach Entlassung selbstständig für die intensivmedizinische Nachsorge. Wie diese Verteidigung auf höchstem Niveau aussieht, erläuterte Carsten Fehler, GF März Niederlassung Berlin.

Zu den spannenden Projektpräsentationen am Stand von März zählte die Plattform „Distance" (Dr. Denise Molinnus und Volker Lowitsch).

Distance hat die Aufgabe, die Strukturen personeller, organisatorischer und technischer Art für die regionalen 200- bis 1000-Betten-Häuser sowie Arztnetze an die Medizininformatikinitiative anzupassen, ergänzte Volker Lowitsch. Die Konzepte der MII, so der Geschäftsführer von Healthcare IT Solutions, gehen nur auf die Strukturen der Unikliniken ein. Der Ansatz lautete daher, diese Welten zusammenzubringen – auch mit einem Betriebskonzept. Es gehe darum, Lösungen für diese Einrichtungen ohne große IT-Abteilungen einzurichten, die auch nach Auslaufen der Projektförderungen nachhaltig nutzbar sind, sagte Lowitsch. Als Komponenten stehen im Mittelpunkt: eine Connectbox zur Verbindung des Primärsystems von Praxis oder Krankenhaus mit Legacy-Standards sowie der Aufbau von Repositories mit Personenbezug ebenso wie die Anbindung an die Prozesse der MII durch pseudonymisierte Daten.

Nachhaltigkeit ermöglichen

Die „Smart Green Hospital Platform" ist eine neue Produktentwicklung in Zusammenarbeit mit Hewlett Packard Enterprise. Sie war ein herausragendes Element des DMEA-Auftritts von März. Die Hintergründe: Die Energiekosten explodieren, aber kaum jemand weiß wo genau im Krankenhaus. Die Bettenplanung steht nicht im Kontext mit allen zugehörigen Verbrauchsdaten. Wechselnde Besucherzahlen erschweren nicht nur eine ressourcenschonende Kantinenplanung, sondern auch die Planung von Kühlung und Wärmebedarf. Die neue strategische Plattform kombiniert Medizin, Energie, Cybersicherheit und IT, um datengestützt unter Einsatz von KI gesetzliche Rahmenanforderungen wie KRITIS und Nachhaltigkeit umzusetzen.

„Die Smart Green Hospital Platform zielt darauf ab, die Nachhaltigkeit von Krankenhäusern zu verbessern und gleichzeitig eine qualitativ hochwertige Gesundheitsversorgung zu gewährleisten", erläuterte Andreas Kumbroch, Vorstand Software Entwicklung Vertrieb bei März. So lassen sich Energiekosten faktenbasiert aufstellen – unter wirtschaftlichen Kriterien und Ausfallaspekten. Auch die Kritische Infrastruktur lasse sich mit Fakten steuern. Die Managementebene erhalte Realtime-Daten; und der Leitstand zeige die Abläufe im vor- und nachstationären Bereich für die Steuerung der Patienten.

Technisch, sagte Kumbroch, beruhe die Lösung auf Erfahrungen im Kontext KHZG – mit einem FHIR-Repository und der applikationsunabhängigen Vorhaltung von Daten im Dialog mit Sav... in Zusammenarbeit mit Partnern aus dem Versorgungs-/Energiebereich. Workflow- und strukturierte Daten ermöglichen kaufmännische, medizinische und weitere Sichten. „Dies bahnt auch den Weg hin zur personalisierten Medizin."

„Daten innerhalb und außerhalb der Krankenhäuser verknüpfen – in Richtung Smart City und Smart Home" sei ebenfalls ein Ziel, sagte Ralph Schirmeisen, Enterprise Architect, Hewlett Packard Enterprise. Ferner solle die Krankenhaustechnik dank der Plattform intelligenter vernetzt werden – mit dem An und Aus der Beleuchtung, mit elektronischem Parkraummanagement sowie Elektromobilität auch für Patienten. Für die Umsetzung eines solchen Konzepts seien Daten nötig.
„Auf dem Markt ist noch keine Lösung zu finden; wir denken, dass die Lösung, die wir in den letzten zwei Jahren erarbeitet haben, eine attraktive Innovation darstellt", betonte Schirmeisen. Die Lösung bestehe aus mehreren Paketen – mit medizinischen ebenso wie energetischen Daten, mit Antworten auf Fragen wie „Welche Station nutzt derzeit wieviel Strom?".

Auf der Messe wurde das Pre-Release der Plattform präsentiert, das jetzt als fertiges Servicepaket ins Angebot kommt– mit Komponenten wie etwa dem Bettenmanagement.

Das attraktive Paket an Angeboten, präsentiert mit kompetenten Vorträgen, wurde auf der DMEA äußerst positiv angenommen. Unser Redakteur Michael Reiter führte im Nachgang der Vorträge Kurzinterviews mit den Referenten.

„Smart Green Hospital Platform": Ralph Schirmeisen (links) und Andreas Kumbroch

Dynamik in der Digitalisierung: Dr. Gerald Gaß, Frau Savli

Digitalisierung mit der Cloud beschleunigen

Wie kommen wir mit der Digitalisierung des Gesundheitswesens voran und wie werden wir dabei schneller? Zwei zentrale Fragen der DMEA 2023 in Berlin. Neben einheitlichen Standards liegt viel Hoffnung auf neutralen Plattformen zur Vernetzung unterschiedlicher Marktteilnehmer, um den Ausbau der digitalen Infrastruktur zu beschleunigen.

Dass wir schneller digitalisieren müssen, war unter den DMEA-Besuchern unbestritten. Allerdings beschäftigte die Besucher des Telepaxx-Stands vor allem die Frage, wie das angesichts chronisch überlasteter IT-Abteilungen gelingen soll. Hoffnung auf Entlastung bringen die viel diskutierten Cloud-Technologien. Sie erleichtern den Zugriff auf medizinische Daten und ermöglichen eine softwareunabhängige Nutzung über Einrichtungsgrenzen hinweg. Davon profitiert die IT, da aufwendige Wartungsarbeiten entfallen und Software als Service (SaaS) direkt aus der Cloud implementiert werden kann. Das hohe Interesse auf der DMEA an Lösungen wie der TMD Cloud ist ein klares Signal, dass Cloud-Technologien im Gesundheitswesen angekommen sind.

Sichere Nutzung von Gesundheitsdaten

Ein weiteres Thema der DMEA war die Nutzung von Gesundheitsdaten - im Rahmen der elektronischen Patientenakte, aber auch des europäischen Gesundheitsdatenraums. Es ging vor allem darum, wie Daten gesetzeskonform genutzt werden können. Die DSGVO gibt den Rahmen hierfür vor, doch einzelne Landeskrankenhausgesetze sorgen für Unsicherheit, was erlaubt ist und was nicht. Zudem wurde diskutiert, wie solche Daten technisch einfach und gleichzeitig sicher bereitgestellt werden können. Auch hier ist die Cloud ein Lösungsansatz: Als virtueller Datenspeicher kann sie die Datenintegrität deutlich erhöhen und beugt unberechtigten Zugriffen dank klarer technischer Berechtigungskonzepte vor. So gelangen Daten rechtskonform in die ePA oder perspektivisch in einen nationalen oder europäischen Gesundheitsdatenraum. Gleichzeitig können über die Cloud auch die Patienten einen geschützten Zugriff auf ihre Medizindaten erhalten. Ein Konzept, das die IT-Verantwortlichen an unserem Stand überzeugte.

Persönlicher Austausch ist unersetzlich

Die DMEA hat sich darüber hinaus auch 2023 als wichtige Austauschplattform für Digital Health präsentiert, auf der drängende Fragestellungen der Branche diskutiert wurden. Als Anbieter der größten europäischen Cloud für diagnostische Medizindaten ist eine solch gut besuchte und inhaltlich relevante Präsenzveranstaltung für uns von großer Bedeutung. Der persönliche Austausch ist besonders bei komplexen technologischen Themen durch nichts zu ersetzen. Wir müssen den Nutzen der Digitalisierung greifbar machen - beispielsweise durch Live-Demos auf den Ständen - und Räume schaffen, um mögliche Bedenken zu besprechen. Mit der Vorstellung des neuen Cloud-Portals der TMD Cloud auf der DMEA 2023 ist uns das erfolgreich gelungen. Aus diesem Grund ist und bleibt die DMEA für uns eine der wichtigsten Messen.

Mitglieder der United Web Solutions sagen: „DMEA 2023 toppt alle Messen davor!“

Best of Breed Lösungen sind eine gefragte Alternative zu den KIS-Monolithen

Hamburg/Berlin, den 11.05.2023: Aufbruchstimmung oder Not? Egal aus welcher Motivation heraus, das Interesse an modernen und bezahlbaren IT-Lösungen für alle Versorgungsprozesse rund um das Krankenhaus ist groß. Die Firmen auf dem Gemeinschaftsstand der United Web Solutions konnten auf der DMEA 2023 zeigen, wie Digitalisierung Versorgung besser und wirtschaftlicher macht. Mit Lösungen aus der Cloud und individuellen IT-Landschaften nach dem Best of Breed Konzept.

„Ja, wir sind die mit dem KIS aus der Cloud und ja unsere Lösungen folgen konsequent dem Best of Breed Konzept“. So lautete die Antwort auf die am häufigsten gestellten Fragen am Stand der United Web Solutions bei der DMEA 2023. Die Messe hat den Mitgliedern des Verbandes die beste Plattform geboten, um zu zeigen, dass moderne, digitale Lösungen und Gesundheitsversorgung sehr gut miteinander funktionieren. Und zwar nicht nur bei dem KIS-Anbieter AMC Advanced Medical Communication Holding GmbH. Alle im Verband organisierten Unternehmen setzen auf webfähige IT-Lösungen, die On-Premises oder in der Cloud betrieben werden können. Gemeinsam bieten sie ein Portfolio, das den Funktionsumfang der großen KIS-Anbieter in Teilbereichen sogar übertrifft. Sie haben also auch bestätigende Antworten auf die Fragen:

- „Haben Sie da auch was für die Pflege, unsere Notaufnahme und die ICU?
- Wie plane ich mein Personal reibungslos und vertragskonform?
- Mit welcher KI treffe ich gute Entscheidungen und wie mache ich meine IT sicher?“

Bei United Web Solutions engagieren sich mittelständische Unternehmen aus Deutschland, die innovative und für die spezifischen Anforderungen der Gesundheitsversorgung spezialisierten IT-Lösungen anbieten. Das gibt Krankenhäusern die Möglichkeit, Softwarelösungen unterschiedlicher Hersteller für unterschiedliche Anwendungsgebiete in Medizin, Pflege und Verwaltung zu einem integrierten und innovativen Krankenhausinformationssystem+ zusammenzufügen. Denn alle Unternehmen sind Experten auf ihrem Fachgebiet und offen für den Austausch mit Partnern. So erhalten Krankenhäuser und MVZ die Möglichkeit, etablierte Software mit neuen, am Bedarf entwickelten Lösungen zu kombinieren und so die beste und passendste IT-Landschaft zu gestalten. Beratungskompetenz in Sachen IT-Sicherheit und Datenschutz, Plattformen für intersektorale Kommunikation mit Leistungserbringern und Patientinnen und Patienten inklusive.

Nachfolgend lesen Sie Statements zur DMEA 2023:

Jörg Reichardt, Geschäftsführer AMC Holding GmbH
„Mit durchgehend wertvollen Terminen und drei Vertragsabschlüssen mit Neukunden war die DMEA 2023 für AMC die erfolgreichste Messe in der Firmengeschichte. Das lag zum einen daran, dass wir mit einer Alternative zu SAP-ISH und unserem KIS CLINIXX® aus der Cloud, den Nerv der Besucher treffen. Zum anderen ist die Messe einfach der beste Event der Branche. Die Anzahl der Aussteller verteilt auf mittlerweile sechs Hallen, das interessante Kongressprogramm, zusätzliche Informationsangebote wie Rundgänge und das kollegiale Beisammensein - all das macht die Messe so vielseitig und so erfolgreich. Wir sind nächstes Jahr definitiv wieder dabei."

Sebastian Fraas, Geschäftsführer apenio GmbH & Co. KG
„Mit unserer Software für die Patientendokumentation apenio® haben wir auf der DMEA 2023 so viel Interesse erregt wie nie zuvor. In den zahlreichen, sehr konkreten Gesprächen lag der Fokus deutlich darauf Investitionen zu planen und die nächsten Schritte nach und mit den KHGZ-Förderprojekten zu orchestrie-ren. Der Auftritt auf dem Gemeinschaftstand der United Web Solutions war in dieser Hinsicht ein großes Plus, da wir unsere Partner direkt mit zusätzlichem fachlichem Hintergrund an der Seite hatten. So konnten wir unseren Gesprächspartner und Partnerinnen bei allen Themen passgenaue Lösungen präsentieren, um damit gemeinsam die richtigen Weichen für die digitale Zukunft der jeweiligen Einrichtungen zu stellen."

Stefan Osterkamp, Director Sales Health & Care bei d.velop
„Nach den langen Jahren des Remote-Arbeitens war es sehr schön, Kunden und Interessenten wieder persönlich zu treffen. Es war wunderbar, zu sehen, welche Begeisterung für Digitalisierung die Menschen zur DMEA 2023 mitgebracht haben. Diese Begeisterung hat sich auch in den Gesprächen widergespiegelt, die wir mit den Besuchern unseres Messestandes geführt haben. Es war zu spüren: Die Kliniken wollen ihre Prozesse digitalisieren, sie wollen agiler werden und sie wollen die digitale Transformation des Gesundheitswesens vorantreiben. Wir sind froh, dass wir im Rahmen der DMEA zeigen konnten, dass d.velop hierfür der ideale Partner ist. Auch die Gelegenheit zu Besuchen am Gemeinschaftsstand der United Web Solutions war sehr gelungen, welche wir als Mitglied nutzen konnten. Dort haben sich ebenfalls spannende Gespräche mit Interessenten und Kunden entwickelt, passend zur besonderen DMEA-Stimmung. Eine sehr gelungene Veranstaltung!"

Bernd Bolduan, IT Consulting and Sales bei LOWTeq GmbH
„Wir sind mit der DMEA 2023 recht zufrieden, weil wir eine Vielzahl guter und vielversprechender Gespräche führen konnten. Dabei ist auch der Gedanke, als Mitglied bei United Web Solutions gemeinsam aufzutreten, gut gelebt worden. So konnten wir Interessenten zum Beispiel mit dem Mitausteller apenio GmbH gemeinsam Lösungen für die Intensivmedizin und die Pflege vorstellen."

Michael Latz, Prokurist & Bereichsleitung Klinik/MVZ medatixx GmbH & Co. KG
„Wir von der medatixx ziehen eine absolut positive Messebilanz und freuen uns schon heute auf die DMEA 2024. Neben dem generell sehr großen Interesse an unseren Primärlösungen für Klinikambulanzen, MVZ und Arztpraxen, haben wir in diesem Jahr eine neue Offenheit für Themen wie SaaS und Cloudlösungen wahrgenommen. Häufige Themenschwerpunkte unserer Gespräche waren auch Interoperabilität, der geplante Ausbau der Telematikinfrastruktur (TI) und die zu erwartenden Auswirkungen der BMG-Digitalstrategie auf das operative Tagesgeschäft unserer Kunden und Interessenten."

Nadine Hopf, Vertriebsleiterin bei Transact - Ges. für Software & Analyse mbH
„Die Auslastung der Hallen und auch die große Zahl der Besucherinnen hat mich dieses Jahr besonders beeindruckt auf der DMEA. Das Publikum war zudem diverser als in den Vorjahren und es waren viele Frauen dabei. Ob das ein Zeichen ist, dass Digitalisierung mittlerweile bei allen an der Gesundheitsversorgung Beteiligten angekommen ist – ich weiß es nicht. Es hat in jedem Fall viel Spaß gemacht, gemeinsam mit den Kollegen und Kolleginnen der United Web Solutions Interessenten und Kunden zu betreuen und mein Netzwerk zu vergrößern."

Peter Schmid, Senior Vertriebsbeauftragter SIEDA GmbH
Die Atmosphäre auf der #DMEA23 war noch besser als im Vorjahr - nicht nur am Gemeinschaftsstand der United Web Solutions, sondern in allen Messehallen. Wir von der SIEDA haben mit unserem Claim „Eine neue Perspektive für Ihre Dienstplanung" sowohl zahlreiche Interessenten als auch unsere zahlreichen Bestandskunden angesprochen. Das absolute Messehighlight war das Modul „Selbstplanung/Wunschplanung der Mitarbeiter", welches wir zusammen mit den Waldkliniken Eisenberg entwickeln. Gemeinsam mit dem Kunden gehen wir neue Wege im Gesundheitswesen und das kam (und kommt) so richtig gut an. Wir freuen uns heute schon auf die DMEA 2024."

Online zum Master in Medizinischer Informatik: Universität UMIT TIROL bildet Experten für die Digitalisierung im Gesundheitswesen aus

Mit dem Master-Studium Medizinische Informatik bietet die Tiroler Privatuniversität UMIT TIROL ein zukunftsträchtiges viersemestriges Studium an, deren Absolvent*innen als Expert*innen die Entwicklung der Digitalisierung im Gesundheitswesen aktiv mitgestalten sollen. Das Studium ist – vorbehaltlich der behördlichen Abstimmung – als modernes online-Studium organisiert, wobei in der Regel einmal wöchentlich ein Online-Vorlesungsblock stattfindet.

Didaktisches Online-Konzept ermöglicht Vereinbarkeit mit dem Beruf

Das Master-Studium Medizinische Informatik setzt inhaltlich auf die Schwerpunkte Klinische Informationssysteme, Gesundheitsvernetzung und eHealth, Health Data und Decision Science sowie Biomedizinische Technik. Organisatorisch werden beim viersemestrigen Studium Medizinische Informatik, das mit dem akademischen Titel Master of Science (MSc) in Medizinischer Informatik abschließt, Online-Vorlesungsblöcke mit online-gestützten begleiteten Studienphasen kombiniert. Ein Praxisprojekt und die Masterarbeit runden das Studium ab. Beim begleiteten Selbststudium wird auf das preisgekrönte didaktische Konzept des Online-Universitätslehrganges Health Information Management der Privatuniversität UMIT TIROL zurückgegriffen. Damit ist sichergestellt, dass das Studium grundsätzlich bei entsprechendem Engagement mit einer Berufstätigkeit bzw. mit familiären Verpflichtungen vereinbar ist.

Qualitätsgesichert und international anerkannt

Das Studium ist von der für die Qualitätssicherung an Hochschulen zuständigen AQ Austria akkreditiert und mit dem Qualitätssiegel der AQ Austria versehen. Auch die European Medical Informatics Association (EFMI) hat die Qualität dieser universitären Ausbildung geprüft und offiziell akkreditiert.

Breites Netzwerk von Kooperationspartnern aus der Industrie

Während des Studiums profitieren die Studierenden von einem breiten Netzwerk von Kooperationspartnern aus Industrie, Gesundheits- und Forschungseinrichtungen und von Absolventen der UMIT TIROL, die national und international in Top-Positionen tätig sind.

Das Studium richtet sich an Bachelor-Absolventen*innen der Medizinischen Informatik, der Informatik, Technik, Medizin, Pflegewissenschaft oder Naturwissenschaften, die ihre berufliche Zukunft im Gesundheitswesen sehen und daher ihre weiterführende Ausbildung in der Medizinischen Informatik wissenschaftlich fundiert und mit der Möglichkeit zu einer anschließenden Promotion fortsetzen wollen.

Alle Infos zum Online-Studium Medizinische Informatik

Informationen zum Master-Studium Medizinische Informatik gibt es auf www.umit-tirol.at/mmi. Der Universität UMIT TIROL ist es wichtig, Interessierte persönlich über die Studien zu informieren. Deshalb finden regelmäßig am Campus der Universität in Hall in Tirol oder online Informationsveranstaltungen statt. Die Termine der Infoveranstaltungen und die Möglichkeit zur Anmeldung finden sich unter **www.umit-tirol.at/service**.

Kontakt:
UMIT TIROL – Privatuniversität für Gesundheitswissenschaften und -technologie
Institut für Medizinische Informatik
Univ.-Prof. Dr. Elske Ammenwerth
Elske.ammenwerth@umit-tirol.at
www.umit-tirol.at/mmi

KI-basierte klinische Entscheidungsunterstützung mit clinalytix

Bereit für die Zeitenwende

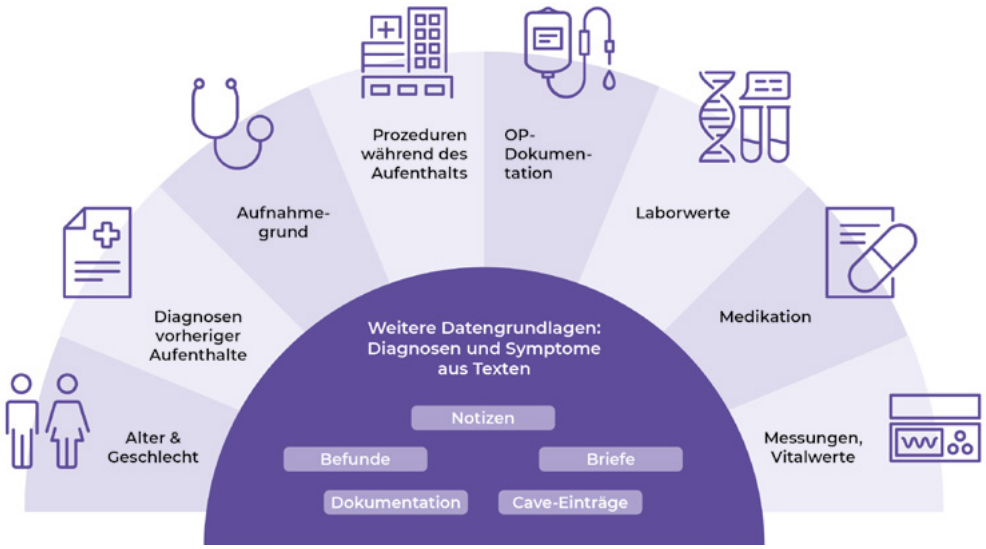
In der Außenpolitik und auf dem Arbeitsmarkt, vor allem aber auch im Gesundheitswesen lässt sich etwas beobachten, das die Politik als Zeitenwende beschreibt. Die Pandemie hat uns vieles gelehrt und Schwächen des Systems überdeutlich aufgezeigt. Doch die besondere Situation hat auch Innovationen gefördert und Digitalisierung in Krankenhäusern dringender als zuvor in den Fokus gerückt. Nun, wo sich das Pandemiegeschehen abzuflachen scheint, machen viele Kliniken einen Kassensturz und sehen: Die steigendenden Kosten, die zusätzlichen Belastungen der letzten Jahre, der Personalmangel und weitere Faktoren führen dazu, dass sie um ihre Existenz bangen müssen. Die Politik hat das mitbekommen und versucht, kurzfristig zu handeln. Aber schon jetzt monieren Branchenkenner, dass die Maßnahmen zu spät kommen und nicht weit genug reichen werden.

Entscheidungen stärken

Wir haben keine Glaskugel, mit der wir vorhersagen können, wie sich die deutsche Krankenhauslandschaft in den nächsten Jahren entwickeln wird. Wir haben jedoch eine Möglichkeit, im klinischen Bereich anzusetzen und dort für Entlastung der belasteten Kliniken zu sorgen. Die KI-Lösung clinalytix von Dedalus HealthCare bereitet klinische Daten und medizinische Informationen so auf, dass das behandelnde Personal sich in kürzester Zeit ein umfassendes Bild eines Patienten machen kann. Das ist ein komplexes Unterfangen, denn wir nutzen neuronale Netzwerke zur Risikovorhersage von bestimmten Krankheitsbildern. Die Daten, die wir dabei in Augenschein nehmen, sind flüchtig, es wird lediglich das Muster in einem neuronalen Netz gespeichert. Das System nimmt hier keine ärztlichen Entscheidungen vorweg, sondern unterstützt das ärztliche Personal dabei, valide und wissenschaftlich fundierte Entscheidungen zu treffen.

Innovationsdruck

Viele Krankenhäuser erkennen das Potenzial einer zunehmenden Digitalisierung, allerdings fehlen schlichtweg die Ressourcen, um diese innovativen IT-Lösungen in den klinischen Alltag zu integrieren. Den Druck zu Innovationen spüren die Krankenhäuser trotzdem. Zum einen hat die Bundesregierung mit dem Krankenhauszukunftsgesetz (KHZG) ein Maßnahmenpaket auf den Weg gebracht, um die Kliniken mit Incentives dazu zu bringen, digitale Lösungen schneller zu implementieren. Zum anderen ist die Erwartungshaltung der Patienten gestiegen. Die Art und Weise der Behandlung hat sich ebenfalls geändert, Patienten werden interdisziplinär und intersektoral behandelt, was in einer höheren Arbeitsbelastung für das pflegerische und ärztliche Personal resultiert.



clinalytix bereitet klinische Daten und medizinische Informationen so auf, dass das behandelnde Personal sich in kürzester Zeit ein umfassendes Bild eines Patienten machen kann.

clinalytix kann als Anhaltspunkt dafür dienen, welche individuellen Parameter für Patienten gelten sollten, und ein Fahrplan sein, der Risikofaktoren und Komplikationen individuell berücksichtigt und das Personal darauf hinweist.

clinalytix hilft, bei der zunehmenden Arbeitsbelastung nicht den Blick für relevante klinische Situationen zu verlieren, die einer schnellen medizinischen Entscheidung bedürfen. Wir von Dedalus HealthCare helfen den Krankenhäusern dabei, diese innovative Lösung schnell und unkompliziert zu implementieren.

Was bedeutet das in der Praxis?

Um die Funktionen der Lösung aufzuzeigen, stelle man sich folgendes Beispiel vor: Patientin Erika Mustermann, 89 Jahre alt, hat eine neue Hüftprothese bekommen und entwickelt nach der Operation auf Station ein Delir. Was bedeutet diese Zusatzdiagnose im klinischen Alltag? Es bedeutet, dass die Patientin erfahrungsgemäß eine längere Verweildauer auf Station hat, somit das Krankenhaus viel Geld kostet, sich mögliche Anschlusstherapien verschieben, was wiederum die Heilungschancen der Patientin verschlechtern kann. Was wäre also, wenn dieses Szenario durch KI-gestützte Entscheidungsunterstützung verhindert werden könnte?

Der Prävention von Krankheiten und der Prädiktion von Ereignissen kann im klassischen Krankenhaus-Workflow oft nicht ausreichend begegnet werden. Mit Hilfe Künstlicher Intelligenz, die sämtliche zum Patienten gehörige digitale Daten permanent scannt und die behandelnden Ärzte bei interventionsbedürftigen Konstellationen aktiv auf ein drohendes Ereignis hinweist, ist eine zusätzliche Unterstützung gegeben, um unerwünschte Ereignisse frühzeitig zu erkennen. So können eine entscheidende Hilfestellung bei Diagnostik und Therapie geleistet und die Patientensicherheit verbessert werden. Wenn die Wahrnehmung nach Operationen gestört ist, z. B. durch das Auftreten eines Delirs, ist das ein Warnsignal, das mit einer erhöhten Sterblichkeit einhergehen kann. Es hat also eine große klinische Bedeutung in der Patientenversorgung. Entwickelt Frau Mustermann also das Delir nach der OP, zieht das eine Reihe an unerfreulichen und potenziell lebensbedrohlichen Konsequenzen nach sich. Durch den Einsatz unserer KI-Anwendung clinalytix, die als zertifiziertes Medizinprodukt der Klasse IIa am Markt verfügbar ist, kann Frau Mustermann optimal durch den perioperativen Verlauf begleitet werden. Dabei stehen auch die Langzeitfolgen eines Delirs im Krankenhaus im Fokus. Auf ein postoperatives Delir folgen oftmals kognitive Defizite, die im schlechtesten Fall monatelang anhalten können. Lässt man clinalytix über die Daten von Frau Mustermann laufen und das System erkennt ein hohes Risiko für ein postoperatives Delir, kann dies womöglich nicht ganz verhindert, aber rechtzeitig erkannt und behandelt werden. Es verkürzt also unter Umständen die Dauer des Krankheitsbildes. Das Delir-Risiko wird außerdem tagesaktuell angezeigt, so dass es nach der Behandlung statistisch ausgewertet werden kann. Man kann somit feststellen, welche Risikofaktoren präoperativ bereits gegeben waren, was während des Krankenhausaufenthaltes von Frau Mustermann das Delir-Risiko hat steigen oder sinken lassen.

Klinische Unterstützung

Abschließend lässt sich festhalten, dass KI-gestützte Entscheidungshilfe niemals das ärztliche und pflegerische Personal ersetzen wird. Allerdings kann sie ein Fahrplan sein, der Risikofaktoren und Komplikationen individuell berücksichtigt und das Personal darauf aufmerksam macht. clinalytix kann als Anhaltspunkt dafür dienen, welche individuellen Parameter für Patienten wie Frau Mustermann gelten sollten, z. B. bezüglich der Herzfrequenz und des Blutdrucks, um ein unerwünschtes klinisches Ereignis wie ein postoperatives Delir zu verhindern.

www.dedalusgroup.de

Schutz vor Cyberattacken – Gewinnen Sie entscheidende Zeit!

Die fortschreitende Digitalisierung im Healthcare-Bereich macht auch Krankenhäuser mehr und mehr zum lohnenden Ziel für Hacker. Einen Diebstahl sensibler Daten oder eine empfindliche und nachhaltige Störung der Betriebsabläufe gilt es unbedingt zu verhindern. Die Lösungen von Nextron geben Ihnen Zeit, sich zu verteidigen und den Angriff im Keim zu ersticken.

Wer ist Nextron Systems?

Wir sind ein weltweit führender Anbieter von Sicherheitssoftware mit Fokus auf frühzeitige Erkennung und Abwehr von Hackerangriffen. Nextron's Hauptsitz ist Dietzenbach bei Frankfurt am Main. Obwohl Nextron erst im Jahr 2017 gegründet wurde, haben wir bereits heute eine Kundenbasis von über 450 Kunden in 35 Ländern – darunter viele Regierungen und große international tätige Konzerne.

Wodurch unterscheidet sich Nextron Systems von anderen Anbietern?

In wenigen Worten ausgedrückt: Wir finden die Dinge, die Antivirenprogramme und EDR-Systeme (EDR = Endpoint Detection and Response) gerne übersehen.

Wir hören immer wieder davon, dass ganze Unternehmen verschlüsselt werden oder in wirtschaftliche Schwierigkeiten geraten, weil Hacker sensible Daten stehlen. Diese Lücke schließen wir mit unserer Technologie. Wir detektieren schon die ersten Anzeichen eines erfolgreichen Angriffsversuchs. Da zwischen den ersten Anzeichen und dem Schadenseintritt in der Regel viele Wochen oder sogar mehrere Monate vergehen sind unsere Kunden ausreichend früh vorgewarnt. Sie können reagieren, bevor Schaden entsteht.

Was ist der besondere Trick? Auf welche Weise erreichen Sie diese Detektionsfähigkeit?

Im Wesentlichen stützen wir uns auf die Erfahrung unseres Research Teams. Unser Head of Research Florian Roth war schon in großen Hackingkampagnen um das Jahr 2012 herum aktiv und hat damals den Scanner THOR entwickelt. Das war damals noch für die BSK Consulting GmbH – eine der Gründungsgesellschaften der Nextron. Dieses Know-How ist auf die Nextron übergegangen. Seit dieser Zeit hat sich u.A. eine Regelbasis mit über 30.000 Detektionsregeln entwickelt mit deren Hilfe wir die Werkzeuge der Angreifer und deren Spuren und Methoden identifizieren.

Aber könnte es nicht sein, dass Sie einmal ein Werkzeug nicht erkennen und den Angriff übersehen?

Dass wir einmal ein Werkzeug nicht erkennen, ist natürlich möglich. Eher sogar hochwahrscheinlich. Aber es spielt für die Detektion des Angriffs eine wesentlich geringere Rolle als man denkt.

Sehen Sie, ein Angreifer muss ja sehr viele Dinge tun, um erfolgreich zu sein.

Er muss zunächst in ein IT-System eindringen, in der Regel muss er dort seine Rechte erweitern – etwa zum Systemadministrator – er muss dafür sorgen, dass es weitere Backdoors gibt, die er zukünftig nutzen kann, er muss sich im Unternehmen „digital umsehen" um ein lohnendes Ziel oder eine Möglichkeit des Zugriffs auf weitere Systeme zu finden. Ggfs. muss er eine Lösung finden, um größere Datenmengen aus dem Unternehmen abzutransportieren. Das sind schon viele Arbeitsschritte. Und für jeden Schritt wird ein Werkzeug oder eine Methode benötigt. Da ist es gar nicht so relevant, ob man einmal ein Werkzeug übersieht.

In der Praxis ist es sogar so, dass wir nicht alle – aber immer mehrere Werkzeuge eines Angriffs erkennen. Das reicht völlig aus, um weitere Untersuchungen zu starten und den Angriff noch rechtzeitig abzuwehren.

Können Sie hier einmal ein Beispiel nennen, das öffentlich bekannt ist?

Ein sehr illustratives Beispiel ist die Hafnium-Kampagne. Wie im März 2021 bekannt wurde, waren weltweit bereits tausende Exchange Server von verschiedensten Angreifergruppen übernommen worden. Obwohl auch wir den ursprünglichen Exploit nicht erkannt haben – so wie alle Anderen – waren die Kunden der Nextron Systems GmbH trotzdem bereits deutlich vor März 2021 gewarnt. Die Angreifergruppen brachten jeweils ihre Lieblingswerkzeuge für die weitere Exploitation mit und legten sie auf den Exchange Servern ab. Dies wurde von unseren Scannern entdeckt, da die Werkzeugsets auch uns bereits seit langem bekannte Werkzeuge enthielten.

Wenn ich es richtig verstehe, verkaufen Sie eigentlich Zeit. Zeit zu reagieren bevor großer Schaden durch einen Hackerangriff entsteht.

Ja, genau!

Welche Auswirkungen hätte ein erfolgreicher Angriff im Krankenhaus?

Als ehemaliger IT-Leiter habe ich mir öfters die Frage gestellt: „Sind alle Systeme ausreichend geschützt?" „Greifen alle eingestellten Regeln (z.B. EDR-System) und vor allem wie kann ich die Infrastruktur noch sicherer machen!"

Ein Cyberangriff stellt ein Krankenhaus vor große Herausforderungen. Der laufende Betrieb wird in vielen Bereichen gestört, was zu Ausfällen führt. Im schlimmsten Fall bedeutet das, dass beispielsweise lebenswichtige Informationen nicht abgerufen werden können.

Die Einschränkungen werden noch dadurch vergrößert, dass eine teilweise Abschaltung der Systeme erfolgt, um den Schaden so gering wie möglich zu halten. Selbst bei sofortigem Handeln kann die Analyse des Schadensausmaßes bis zu mehrere Wochen in Anspruch nehmen.

Ein solcher Vorfall trägt leider dazu bei, dass die Patientensicherheit und -privatsphäre gefährdet ist. Denn der Hacker erhält ggf. Zugriff auf die Patientenakten, welche er dann missbräuchlich verwenden könnte.

Welche Kosten kommen bei einer Kompromittierung auf das Krankenhaus zu?

Ein Sicherheitsvorfall kann zu hohen Kosten für das Krankenhaus führen. Die Schadensanalyse und Wiederherstellung von Systemen benötigen immense Ressourcen. Dazu kommen ggf. Schadensersatzforderungen von Betroffenen oder Bußgelder. Darüber hinaus stehen im Nachgang Arbeiten an der Systemumgebung an, die sich nicht selten über einen längeren Zeitraum erstrecken. Diese Arbeiten zu realisieren, während gleichzeitig der laufende Betrieb funktionieren muss, ist dann eine große Herausforderung.

Wie sehen sie das aus heutiger Sicht und wie kann sich ein Krankenhaus davor schützen?

Das A und O ist die Fähigkeit, einen Angriff schnell zu erkennen, also ein System, welches zu einem frühen Zeitpunkt warnt. Genau das bieten die Softwareprodukte von Nextron Systems. Sie ergänzen die vorhandene Sicherheitsarchitektur wie z.B. von Firewall, AV und EDR. Ein einfacher Firewall- oder Antivirenschutz kombiniert mit einem EDR-System reichen schon lange nicht mehr aus. Deshalb ist es nicht nur für Krankenhäuser immens wichtig, rechtzeitig Maßnahmen zur Cybersicherheit zu ergreifen. Dazu gehören auch die Überwachung und Erkennung von Bedrohungen. Um die Reaktionsfähigkeit auf Sicherheitsvorfälle zu verbessern ist ein Frühwarnsystem wie mit unserem THOR-Scanner unabdinglich.

Welche Leistungen und Produkte bietet Nextron konkret für den Healthcare-Markt an?

Unsere Produktpalette hat sich in den letzten Jahren wesentlich erweitert. Neben der Scanner-Lösung THOR bieten wir mit dem ASGARD Management Center sowie dem ASGARD Analysis Cockpit umfangreiche Verteilungs-, Orchestrierungs-, Kontroll- und Analyselösungen an. Auch Incident Response Funktionen sind fester Bestandteil des Portfolios. Neben dieser On-Premise Lösung bieten wir auch einen Managed Service an.

Mit dem Nextron Managed Detection and Response Service nutzen unsere Kunden unsere Detektionsfähigkeit und unsere Frühwarnfunktionen, ohne in diesem Bereich eigenes Knowhow oder eigene Ressourcen aufbauen zu müssen.

Follow THOR on Twitter: **@thor_scanner**

Boris Deibel
Head of Healthcare Business (DACH)
healthcare@nextron-systems.com
Phone: +49 179 67 00 88 6
Web: www.nextron-systems.com

Nextron Systems GmbH
Bruchstr. 8
63128 Dietzenbach
Germany

IT Sicherheit im Krankenhaus

Journal für Strategie und Praxis

Das Leben eines CISO – im Visier, ausgebrannt und streng kontrolliert

Nach dem Chaos und Stillstand im ersten Jahr der Pandemie befanden sich CISOs in einer Übergangsphase. Ihre Zuversicht in Homeoffice Umgebungen wuchs ebenso wie das Wissen über die Bedrohungslandschaft nach der Pandemie. Sie glaubten an ihre Fähigkeit, ihre Unternehmen in der „neuen Normalität" schützen zu können. Für CISOs gab es nichts Neues mehr an der mittlerweile normalen Arbeitsweise. Nachdem die anfänglichen Wirren bewältigt waren und sie zwei weitere Homeoffice-Jahre gemeistert hatten, kehrte die Realität zurück – und mit ihr ein vertrauter Zustand großer Sorge.

CISOs machen sich keine Illusionen über die Risiken, die von den Mitarbeitern ausgehen. Allerdings ist der Optimismus mancher, was den Schutz von Daten anbelangt, fehl am Platz. Insider-Bedrohungen sind ein zunehmendes Problem. Und angesichts der Tatsache, dass die Mitarbeiterfluktuation in vielen Branchen keine Anzeichen von Verlangsamung zeigt, dürfte das noch eine ganze Weile der Fall sein. Hinzu kommt, dass sich die Rezession auf die Sicherheitsbudgets niederschlägt. Möglicherweise reichen die bereits vorhandenen Kontrollen aus, um das Lieferkettenrisiko zu minimieren, Bedrohungsakteure zu erkennen und auszuschalten und potenzielle Verluste durch Ransomware zu verhindern. Wie lange das der Fall sein wird, kann jedoch nicht vorhergesagt werden.

Die Rückkehr in die harte Realität katapultiert viele CISOs an den Rand ihrer Belastbarkeit. Kein Wunder, dass sich die meisten durch wachsende Erwartungen und die Bürde der persönlichen Haftung unter Druck gesetzt fühlen und sogar von Burnout betroffen sind. Es besteht jedoch Grund zur Hoffnung. Die Tatsache, dass CISOs ihre Sorgen zur Sprache bringen, ist ein großer Schritt in die richtige Richtung. Da die Mehrheit auch eine Annäherung an die Geschäftsführung wahrnimmt, besteht durchaus eine solide Grundlage für das Herbeiführen von Veränderungen. Die Frage lautet: Werden CISOs angesichts der schrumpfenden Budgets und des langfristigen Fachkräftemangels über die dafür erforderlichen Ressourcen verfügen?

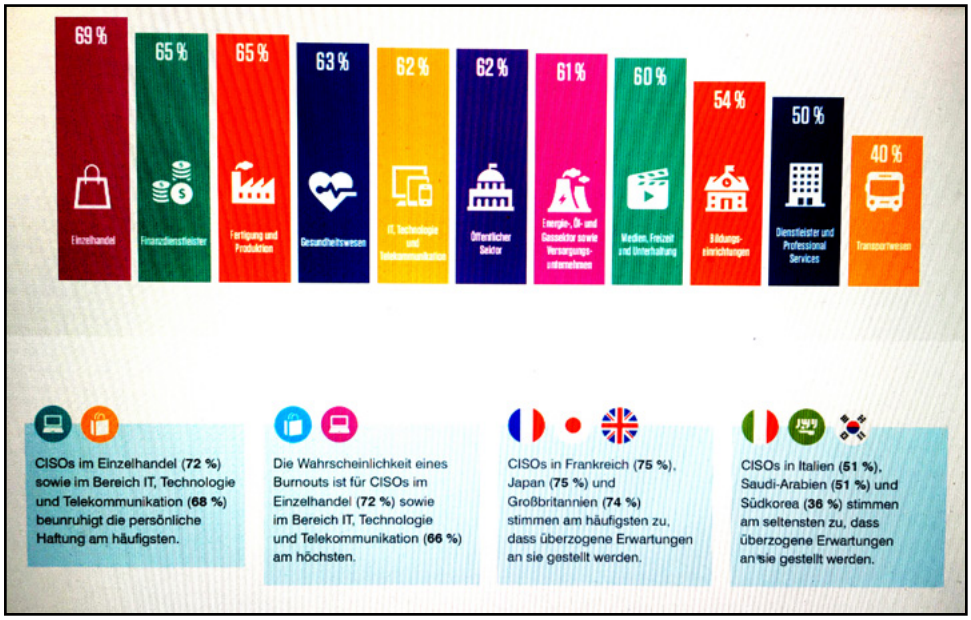
Anhaltend hoher Druck

Die Mitwirkung von Cybersicherheitsexperten bei der Bewältigung der Pandemie hat zweifellos einige Vorteile mit sich gebracht. CISOs können heute bei Vorstandsentscheidungen mehr mitreden. Nie zuvor ist es ihnen so überzeugend gelungen, die Bedeutung von effektiver Sicherheit für den Erfolg der Geschäftsstrategie zu demonstrieren. Es gibt jedoch auch schlechte Nachrichten.

Nachdem sie während der Krise quasi über Nacht auf breiter Ebene Homeoffice- und hybride Arbeitsmodelle ermöglicht haben, empfinden viele CISOs den anhaltend hohen Druck als unerträglich. Fast zwei Drittel (61 %) der CISOs betrachten die an sie gestellten Erwartungen als überzogen – eine Steigerung gegenüber 2022 (49 %) und 2021 (57 %). Hintergrund für die Zunahme des Problems könnte die Rückkehr zur Normalität sein. Nachdem die Hektik um die Absicherung ihrer Homeoffice- und Hybridumgebungen nachgelassen hat, kürzen viele Unternehmen ihr Budget für Cybersicherheit. Somit gelten für CISOs zwar weiterhin dieselben Ziele – ihnen stehen jedoch weniger Ressourcen zur Verfügung, um sie zu erreichen. Im Branchenvergleich werden die Erwartungen im Einzelhandel (69 %) und im Bereich IT, Technologie und Telekommunikation (69 %) als besonders hoch wahrgenommen. Am wenigsten unter Druck sehen sich CISOs in Transportunternehmen (48 %) und im Gesundheitswesen (42 %). Die Unterschiede lassen vermuten, dass die Last der Sicherheit in sicherheitskritischen Branchen breiter verteilt ist.

Die Bürde der persönlichen Haftung

Ein weiterer wichtiger Faktor, der den weltweit von den CISOs wahrgenommenen Druck zusätzlich erhöht, ist das omnipräsente Risiko der persönlichen Haftung. 62 % der Befragten bereitet dieser Aspekt Sorgen. Nur 15 % gaben an, dass persönliche Haftung in ihrer derzeitigen Rolle kein Problem darstellt. Die größere Verantwortung der CISOs ruft verstärkt die Aufsichtsbehörden auf den Plan. Das Versäumnis des ehemaligen CISO von Uber, eine Datenschutzverletzung zu melden, hat zu einer strafrechtlichen Verurteilung geführt. CISOs sind sich der Tragweite eines solchen Urteils durchaus bewusst und möchten sich gegen derartige Risiken absichern.



60% der CISOs gaben an, in den letzten 12 Monaten von Burnout betroffen gewesen zu sein.

Die meisten CISOs (61 %) geben an, dass sie nicht für ein Unternehmen arbeiten würden, das seinen Direktoren und Führungskräften keine Versicherung oder ähnliche Absicherung anbietet, um sie vor Schadensersatzansprüchen infolge eines erfolgreichen Cyberangriffs zu schützen. Nur 14 % sind anderer Meinung. Verständlicherweise wünschen sich CISOs in Branchen mit großen Mengen an vertraulichen Daten oder unter starker behördlicher Kontrolle am häufigsten eine Versicherungsabdeckung, z. B. in den Bereichen Einzelhandel (69 %), Finanzdienstleistungen (65 %) und Fertigung (65 %).

Der Anteil der CISOs, die nicht für ein Unternehmen arbeiten würden, das seinen Direktoren und Führungskräften keinen Versicherungsschutz (oder eine ähnliche Absicherung) anbietet, um sie vor Schadensersatzansprüchen infolge eines erfolgreichen Cyberangriffs zu schützen.

Leider bleiben die Folgen von erhöhtem Druck, Behördenprüfung und persönlicher Haftung nicht aus. Stressbelastete Umgebungen, knappe Budgets und steigende Erwartungen schlagen sich weltweit auf die Lebensqualität der CISOs nieder. Ganze 60 % geben an, in den letzten 12 Monaten von Burnout betroffen gewesen zu sein. Nur 15 % stimmen der Aussage nicht zu. Ein bedenkliches Resümee am Ende eines weiteren Jahres, das Cybersicherheitsverantwortliche vor zahlreiche Herausforderungen stellte. Die Zahlen unterstreichen einmal mehr, wie wichtig es ist, beruflich wie privat festen Boden unter den Füßen zu behalten. Die Tragweite des Problems kann nicht oft genug betont werden. Forrester prognostizierte kürzlich, dass ein Global 500-Unternehmen 2023 aufgrund der gesundheitlich bedenklichen Arbeitsbedingungen seiner Cybersicherheitsmitarbeiter gefährdet sein wird.9 Die Aufgabe sicherzustellen, dass dies nicht unter ihrer Verantwortung geschieht, liegt bei den für Cybersicherheit zuständigen Führungskräften. Dies ist jedoch nur dann möglich, wenn CISOs die Gelegenheit gegeben wird, Bedenken zu äußern, und Zeit eingeräumt wird, sich zu erholen und ihre Widerstandskraft zu stärken.

Am selben Strang ziehen

Knappe Budgets, durch Menschen bedingte Risiken und die wachsende Bedrohungslandschaft sind für CISOs nichts Neues. Die meisten dieser Herausforderungen gab es schon früher. Die positive Entwicklung der Beziehungen zur Vorstandsebene bedeutet für CISOs, dass sie neue Verbündete gewonnen haben. Gemeinsam haben Vorstände und CISOs eine gute Chance, ihre risikobasierten Strategien zu verbessern und wirksame Veränderungen herbeizuführen. Für CISOs und ihre Verbündeten im Vorstand bietet es sich mitunter an, Hilfestellung und finanzielle Unterstützung für Geschäftssegmente zu leisten, die die erforderliche Kapazität und Priorisierung zur Implementierung dieser Veränderungen nicht so leicht aufbringen bzw. leisten können. In der dynamischen Cybersicherheitsumgebung wird es immer wieder neue Herausforderungen geben. Diese lassen sich allerdings viel einfacher bewältigen, wenn beide Seiten am selben Strang ziehen, um ein gemeinsames Ziel zu erreichen.

Die Aufgaben der CISOs waren schon immer mit Stress verbunden, aber zusätzlicher Druck – etwa durch Vorstandserwartungen an eine schnellere Risikominimierung, die herausfordernde Überzeugungsarbeit bei der mittleren Führungsebene, Budgetkürzungen und Fachkräftemangel – hat für viele von ihnen zu einer nicht mehr tragbaren Situation geführt. Deshalb wechseln mehr CISOs die Stelle oder kehren der Cybersicherheit vollends den Rücken. Das Herstellen von mehr Ausgewogenheit mag zwar angesichts der mit der Rolle verbundenen Dauerbereitschaft unmöglich erscheinen, dennoch ist sie eine absolute Notwendigkeit, um genügend Widerstandskraft zum Schutz vor Burnout aufzubauen.

Celeste Lowe, Group Director, IT Security, Nine: „Die Aufgaben der CISOs waren schon immer mit Stress verbunden, aber zusätzlicher Druck hat für viele von ihnen zu einer nicht mehr tragbaren Situation geführt."

Verarbeitung von sensiblen Daten in der Cloud und die Governance

Die Rahmenbedingungen für die Verarbeitung von sensiblen Daten ändern sich schnell und sind vielfältig. Gesundheitsdienstleisterstellen sich die Frage, ob der Einsatz von Cloud-Diensten für sie in Frage kommen kann. Prof. Dr. Dr. Christian Dierks, Fachanwalt für Sozialrecht und Medizinrecht sowie Facharzt für Allgemeinmedizin und Professor für Gesundheitssystemforschung an der Charité Berlin, gibt in seinem Gastbeitrag zu dieser Frage Auskunft.

Sie sind sich unsicher, ob die Verarbeitung von Gesundheitsdaten in der Cloud im Einklang mit den für Ihre Organisation geltenden Regeln möglich ist? Gute Nachrichten: Aktuelle Entwicklungen auf deutscher und europäischer Ebene bestätigen erneut, dass die Nutzung der Cloud möglich ist – sowohl im öffentlichen Sektor als auch im Gesundheitswesen.

Das Angebot digitaler Produkte und Dienstleistungen im Gesundheitssektor – wie elektronische Patientenakten und Krankenhausinformationssysteme, telemedizinische Leistungen oder digitale Gesundheitsanwendungen – nimmt stetig zu und führt zu einer immer größer werdenden Menge an Gesundheitsdaten. Die technischen Entwicklungen steigern die Möglichkeiten der Datennutzung – aber auch die Gefahren für Datenmissbrauch. Die Speicherung und Verarbeitung der Daten innerhalb der On-Premises-Lösungen in eigenen Rechenzentren geraten zunehmend an ihre Grenzen. Ein steigender Kostendruck, der Bedarf an skalierbaren IT-Ressourcen sowie der einfache Zugang zu neusten Technologien bewegen Akteure zurecht dazu, ihre Daten in die Cloud umzuziehen. Die Nutzung von Dienstleistern für Cloud-Computing kann die Sicherheit der Daten erheblich erhöhen. Gleichzeitig können Kapazitäten freigesetzt und Potentiale für Innovationen in der Gesundheitsversorgung und -forschung geschaffen werden.

Schrems-II: „Angst“ vor dem „Drittlandstransfer“

Spätestens seit dem vielbeachteten Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) im Jahr 2020, wird die Möglichkeit des Einsatzes von Dienstleistern für Cloud-Computing, die ihren Konzernsitz in den USA haben, sowohl in Fachkreisen als auch in der breiten Öffentlichkeit noch intensiver debattiert. Die große Sorge der Datenschützenden ist hier stets das Risiko eines Zugriffs auf – auch in Europa gespeicherte – Daten durch die US-Behörden. Die Herausgabe von Daten an US-Institutionen wäre für das Unternehmen, auf dessen Daten zugegriffen werden würde, ein sogenannter „Drittlandstransfer“. Hervorzuheben ist jedoch, dass dieser zulässig sein kann, zum Beispiel wenn bestimmte Schutzmaßnahmen getroffen werden.

Die DSGVO und der EuGH halten den Einsatz von Cloud-Computing unter bestimmten Voraussetzungen für zulässig

Anders als teilweise behauptet ist seit der Schrems-II-Entscheidung des EuGH keineswegs der Einsatz von Cloud-Dienstleistern mit US-Konzernverbindungen pauschal verboten. Verkürzt sagt der EuGH, dass die Unternehmen beim Einsatz solcher Dienstleister „geeignete Garantien“ im Sinne des Kapitel V der Datenschutz-Grundverordnung (DSGVO) schaffen müssen, um die Daten angemessen zu schützen, damit ein Drittlandstransfer nicht ohne angemessene Schutzmaßnahmen stattfindet. Solche Maßnahmen können durch vertragliche Absprachen, interne organisatorische Konzepte und technische Vorkehrungen sichergestellt werden.

Herausforderungen im Gesundheitssektor

Organisationen im deutschen Gesundheitswesen müssen neben dem hohen Schutzniveau, das die DSGVO für sensible Gesundheitsdaten fordert, auch noch Bundes- und Landesregelungen beachten. So gelten beispielsweise für Krankenkassen die Vorschriften aus dem Sozialgesetzbuch (SGB) V und X und für Hersteller Digitaler Gesundheitsanwendungen (DiGA), den sogenannten „Apps auf Rezept", die Regelungen der DiGAV. Krankenhäuser wiederum sind den Vorschriften in den Landeskrankenhausgesetzen unterworfen, deren Regelungen nicht bundesweit einheitlich sind. Diese Zersplitterung der relevanten rechtlichen Rahmenbedingungen erschwert es Unternehmen des Gesundheitssektors, einen Überblick über die jeweils geltenden Regelungen zu erhalten. Aber auch hier gilt: Der Einsatz von Cloud-Dienstleistern ist auch nach diesen Vorschriften erlaubt, unter Beachtung bestimmter Maßnahmen. Die Speicherung von Gesundheits- und Sozialdaten in der Cloud ist auch in Deutschland vor dem Hintergrund der genannten Regelungen rechtlich möglich.

Aktuelle Entwicklungen bestätigen erneut: Cloud-Nutzung im Gesundheitswesen ist möglich

Aktuelle Entwicklungen auf deutscher und europäischer Ebene zeigen einmal mehr, dass die Nutzung von Cloud-Services rechtlich zulässig ist – auch im öffentlichen Sektor und im Gesundheitswesen. Im Jahr 2022 wurden in den Landeskrankenhausgesetzen in Berlin und Bayern die Regelungen zum Einsatz von Auftragsverarbeitern überarbeitet, sodass Krankenhäuser in diesen Bundesländern nun leichter Cloud-Dienstleister einsetzen können. In einem wegweisenden Beschluss hat das Oberlandesgericht (OLG) Karlsruhe im September des Jahres 2022 entschieden, dass öffentliche Krankenhäuser einen Anbieter für digitales Entlassmanagement beauftragen dürfen, der die europäische Tochtergesellschaft einer US-Mutter als Hosting-Anbieterin einbindet. Die Vergabekammer Bund bestätigte diese Auffassung für Sozialdaten im März 2023.

Deutschland nähert sich somit an die Ansichten und die Rechtsprechung in anderen europäischen Staaten an. So wurde in Frankreich vom Conseil d'État bereits in den Jahren 2020 und 2021 entschieden, dass der Einsatz eines Cloud-Dienstleisters mit Konzernverbindungen in die USA zulässig ist, wenn die Daten verschlüsselt sind. Der Europäische Datenschutzausschuss (EDSA) hat sich in seinem Bericht zur „Coordinated Enforcement Action" zum Einsatz von Cloud-Dienstleistern im öffentlichen Sektor geäußert. Hervorzuheben ist auch hier, dass der Einsatz von Cloud-Dienstleistern mit Konzernverbindungen in die USA unter Einhaltung eines Maßnahmenkatalogs zulässig sein kann. Auch mit Blick auf den Drittlandstransfer tut sich etwas: Endlich nimmt das sogenannte EU-U.S. Data Privacy Framework Formen an, auf dessen Grundlage noch dieses Jahr von der EU-Kommission ein Angemessenheitsbeschluss erlassen werden soll, der die USA als ein Drittland mit einem angemessenen Schutzniveau anerkennt.

Fazit: Cloud geht nicht – gibt's nicht

Auch wenn die Rechtslage gerade in Deutschland unübersichtlich ist – lassen Sie sich nicht abschrecken, wenn Sie rechtliche Bedenken in Bezug auf den Einsatz von Cloud-Dienstleistern für Gesundheits- und Sozialdaten hören. Lassen Sie die für Ihr Unternehmen geltenden rechtlichen Rahmenbedingungen prüfen und informieren Sie sich, wie der Einsatz von Cloud-Dienstleistern auch für Ihre Daten möglich gemacht werden kann.

Quelle: Blog Amazon Web Services (AWS)

Prof. Dr. med. Dr. iur. Christian Dierks ist Fachanwalt für Sozialrecht und Medizinrecht, Facharzt für Allgemeinmedizin und Professor für Gesundheitssystemforschung an der Charité Berlin. Er ist Gründer und Managing Partner von Dierks+Company, einem Beratungsunternehmen, das sich auf die Förderung von Innovationen im Gesundheitswesen und in den Life Sciences spezialisiert hat.

ChatGPT, Bard & Co.

Wie künstliche Intelligenz die Gesundheitswirtschaft verändert und welche Rolle der Datenschutz dabei spielt

Die Digitalisierung in der Gesundheitswirtschaft schreitet auch mit speziellem Blick auf die Künstliche Intelligenz (KI) unaufhaltsam und rasant voran. Der Einsatz von KI in der Radiologie oder die Verwendung von ChatGPT bilden dabei nur den Anfang. Welche Auswirkungen diese Entwicklungen auf den Datenschutz haben, beschreiben David Grosse-Dütting, Manager Curacon GmbH Wirtschaftsprüfungsgesellschaft, & Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH, in diesem Beitrag.

Spätestens die Veröffentlichung von ChatGPT im November 2022 hat einen Hype in Bezug auf Nutzung Künstlicher Intelligenz (KI) ausgelöst und das Thema der breiten Öffentlichkeit bekannt gemacht. Mancher Experte ist der Meinung, dass die KI viele Wirtschaftszweige grundlegend verändern oder sogar ganz obsolet machen könnte. Und tatsächlich hat der Dienst innerhalb weniger Monate eine enorme Verbreitung gefunden. So ergab eine Umfrage in den USA, dass bereits 43 % aller Berufstätigen KI-Tools für ihre Arbeit nutzen.[1] Und Bill Gates bezeichnete in seinem Blog ChatGPT als revolutionärste Entwicklung der vergangenen 40 Jahre[2].

Bedenken nehmen zu

Gleichzeitig mehren sich auch die kritischen Stimmen zur KI. Im März forderte eine Gruppe von 1.000 Experten aus der Tech-Branche und Forschung in einem offenen Brief[3] ein Moratorium für die Entwicklung Künstlicher Intelligenz. „KI-Systeme mit einer Intelligenz, die Menschen Konkurrenz macht, können große Risiken für Gesellschaft und Menschheit bergen", heißt es dort. Daher sollten zunächst gemeinsame Sicherheitsstandards für die Entwicklung und den Einsatz von KI festgelegt werden. Vor allem Branchen, die sicherheitskritisch sind oder große Bedeutung für den Einzelnen haben, können die Risiken besonders leistungsfähiger KI-Systeme erheblich sein.

Bereits im Jahr 2021 gelang es dem Team um den Datenforscher Nicholas Carlini durch eine data extraction and reconstruction attack, Teile der Trainingsdaten des Sprachmodells GPT-2 zu rekonstruieren – darunter auch persönliche Daten wie Namen, Telefonnummern und E-Mail-Adressen.[4] Die Forscher kommen zu dem Schluss, dass data extraction attacks nicht nur im akademischen Kontext durchführbar sind, sondern sehr wohl eine große praktische Relevanz haben und ihre Bedeutung in Zukunft zunehmen wird.

Dr. Uwe Günther, Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH.
Partner Curacon GmbH Wirtschaftsprüfungsgesellschaft und Geschäftsführer Sanovis GmbH. Als Leiter der Geschäftsfelder IT-Management und Datenschutz liegen die Fachgebiete von Dr. Uwe Günther sowohl in der IT als auch im betriebswirtschaftlichen Bereich. Dabei gilt er als ausgewiesener Experte für die Beratungsschwerpunkte IT-Strategie, IT-Management, Datenschutz und IT-Sicherheit.

Es seien daher Maßnahmen zu ergreifen, um bereits beim Training der KI-Modelle mögliche negative Auswirkungen auf die Privatsphäre zu vermeiden.

Neue Anwendungsmöglichkeiten in der Gesundheitswirtschaft

Die möglichen Anwendungsfälle und Nutzungsmöglichkeiten sind auch in der Gesundheitswirtschaft scheinbar unbegrenzt. Sie reichen von der Patientenkommunikation im Vorfeld einer Behandlung, über die Befundung von EKGs, radiologischen Befunden und Laborparametern, der automatischen Erstellung von Arztbriefen und Dienstplänen bis hin zur Ableitung von Therapieempfehlungen oder Robotern, die Unterstützung in Pflege und Betreuung leisten sollen. Naturgemäß sind die Risiken aufgrund der hohen Sensitivität der Daten im Gesundheitswesen besonders groß.

Da die KI-Modelle abhängig von den Trainingsdaten sind, können die Ergebnisse der Modelle diskriminierend wirken, wenn in den Trainingsdaten Menschen mit bestimmten Merkmalen unterrepräsentiert sind. So zeigte die Netflix-Dokumentation „Coded Bias“[5] aus dem Jahr 2020, dass die Aussagekraft von Algorithmen und Gesichtserkennungssoftwares bei Menschen mit dunkler Haut deutlich geringer ist, als bei Menschen mit einer hellen Hautfarbe. Auch konnten Unterschiede zwischen den Geschlechtern identifiziert werden, zu Ungunsten von Frauen. Und diese Ungleichbehandlung beginnt bereits bei der Erstellung der Trainingsdaten, da die Instrumente zur Datenerfassung ebenfalls auf Personen mit bestimmten Merkmalen ausgelegt sind, wie z.B. die Lichttechnik bei Fotoaufnahmen, die häufig für Menschen mit heller Haut kalibriert wurde.

Dies wirft natürlich vor allem im medizinischen Kontext bedeutende Fragen auf. Ist es möglich, Patienten transparent zu machen, wenn der Arzt bei der Befundung von radiologischen Bildern von einer KI unterstützt wird? Wird die Entscheidungsfähigkeit des Arztes durch die KI-Unterstützung beeinflusst. Das Fraunhofer benennt bereits für den gesamten Versorgungsprozess im Krankenhaus mögliche Anwendungsfälle, weist aber gleichzeitig darauf hin, dass „ganzheitliche Sicherheitskonzepte“ für den Einsatz von KI-Anwendungen in der Medizin erforderlich sind[6].

Die Rolle des Datenschutzes

Im Jahr 2019 beschloss die Datenschutzkonferenz die Hambacher Erklärung zur Künstlichen Intelligenz[7]. Darin heißt es, dass „nicht alles, was technisch möglich und ökonomisch erwünscht ist, [...] in der Realität umgesetzt werden darf.“ Der Einsatz von selbstlernenden Systemen könne in massiver Weise in die Grundrechte der Menschen eingreifen und müsse daher gesetzlich reglementiert werden.

Für die Entwicklung von KI-Systemen kommen daher die Anforderungen zum Datenschutz durch Technikgestaltung in besonderem Maße zum Tragen. Hierzu formulieren die Datenschützer wesentliche Grundsätze, die ein KI-System einhalten müsse.

1. **KI darf Menschen nicht zum Objekt machen:** Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen nicht allein einer Maschine überlassen werden. Betroffene hätten auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person, auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. **KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben:** KI-Systeme dürfen nur für verfassungsrechtlich legitimierten Zwecken eingesetzt werden, erweiterte oder neue Verarbeitungszwecke müssten mit dem ursprünglichen Erhebungszweck vereinbar sein.

3. **KI muss transparent, nachvollziehbar und erklärbar sein:** Die Verarbeitung muss für die Betroffenen transparent sein, insbesondere hinsichtlich des Prozesses der Verarbeitung und über die verwendeten Trainingsdaten. Nach der DSGVO ist dafür auch über die involvierte Logik ausreichend aufzuklären.

4. **KI muss Diskriminierungen vermeiden:** Vor dem Einsatz von KI-Systemen müssen die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. **Für KI gilt der Grundsatz der Datenminimierung:** Die Verarbeitung personenbezogener Daten muss stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. **KI braucht Verantwortlichkeit:** Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten.

7. **KI benötigt technischen und organisatorischen Standard:** Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft.

Seit 2021 versuchen die EU-Institutionen im sogenannten „AI Act" einen rechtlichen Rahmen zu erstellen, um KI-Systeme zu regulieren. Dort sollen unter anderem die Zuständigkeiten der Aufsichtsbehörden, die Notwendigkeit zum Auditing und der Zertifizierung von KI-Systemen, Produktverantwortung und die zwingende Kennzeichnung von maschinenunterstützten Produkten geregelt werden. Der Act verzögert sich allerdings weiter aufgrund eines festgefahrenen Streits, ob große Sprachmodelle generell als Hochrisiko-Technologie definiert werden sollten.

Fazit

Viele Einrichtungen der Gesundheitswirtschaft werden in der nahen Zukunft mit neuen Produkten konfrontiert sein, die KI-Systeme enthalten. Fachkräftemangel und hoher Wettbewerbsdruck verstärken die Erforderlichkeit zur Einführung solcher Lösungen. Es gilt daher, solche Lösungen nicht ohne gründliche Prüfung in die Prozesse zu integrieren. Die Beteiligung des Datenschutzbeauftragten dürfte hier unumgänglich sein, besonders da es bislang an einem verbindlichen und umfänglichen regulatorischen Rahmen mangelt.

David Große Dütting, Manager Curacon GmbH Wirtschaftsprüfungsgesellschaft.
David Große-Dütting ist als Manager in der Unternehmensberatung im Geschäftsfeld Datenschutz tätig und in vielen Unternehmen verschiedener Branchen als Datenschutzbeauftragter bestellt. Seine Schwerpunkte liegen in der Umsetzung der konfessionellen Datenschutzgesetze, der Bestandsaufnahme und Bewertung von Datenschutzmanagementsystemen sowie der datenschutzkonformen Gestaltung von Websites und Social Media Auftritten.

[1] https://www.fishbowlapp.com/insights/70-percent-of-workers-using-chatgpt-at-work-are-not-telling-their-boss/ [zuletzt aufgerufen am 24.03.2023]
[2] https://www.gatesnotes.com/The-Age-of-AI-Has-Begun [zuletzt aufgerufen am 24.03.2023]
[3] https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [zuletzt aufgerufen am 06.04.2023]
[4] https://www.usenix.org/system/files/sec21-carlini-extracting.pdf [zuletzt aufgerufen am 06.04.2023]
[5] https://www.netflix.com/de/title/81328723 [zuletzt aufgerufen am 06.04.2023]
[6] https://www.iks.fraunhofer.de/de/themen/kuenstliche-intelligenz/kuenstliche-intelligenz-medizin.html [zuletzt aufgerufen am 06.04.2023]
[7] https://datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf [zuletzt aufgerufen am 06.04.2023].

Zeitenwende in der Healthcare IT

Webbasiertes KIS

CLINIXX®

Krankenhausinformationssystem aus der Cloud

CLINIXX® Krankenhausinformationssystem

CLINIXX® aus der Cloud

CLINIXX® als SAP ISH Ersatz

CLINIXX Angebot anfragen
https://anfrage.clinixx.de

AMC Holding GmbH
Tel.: 040 2442 270 | E-Mail: info@amc-gmbh.com | Web: www.amc-gmbh.com

Infor Cloverleaf®

infor

FUTURE READY

Den Datenpuls stabilisieren. Von Datenbrücken profitieren.

Eine IT-Lösung im Gesundheitswesen ist nur so gut wie ihre Interaktionsfähigkeit mit dem Behandlungsverlauf des Patienten und den daraus resultierenden Prozessen im Krankenhaus. Davon sind wir überzeugt und haben die Infor™ Cloverleaf® Integration Suite nach diesem Credo entwickelt.

Sprechen Sie mit unseren Consultants über Ihre individuelle Lösung aus stabilem Datenpuls und profitablen Datenbrücken.

Health-Comm.de

Health·Comm