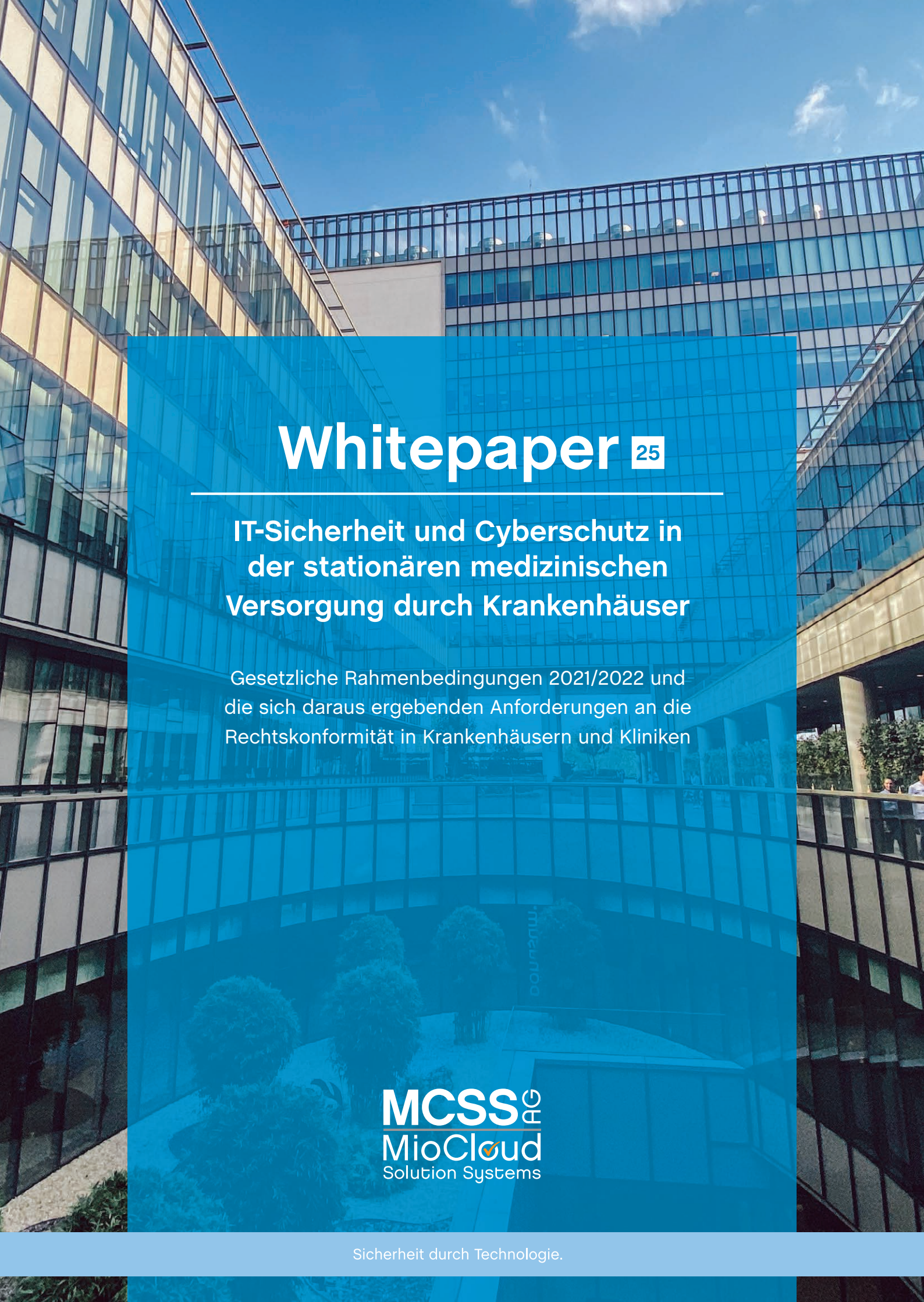


Whitepaper 25

IT-Sicherheit und Cyberschutz in der stationären medizinischen Versorgung durch Krankenhäuser

Gesetzliche Rahmenbedingungen 2021/2022 und die sich daraus ergebenden Anforderungen an die Rechtskonformität in Krankenhäusern und Kliniken

MCSS AG
MioCloud
Solution Systems

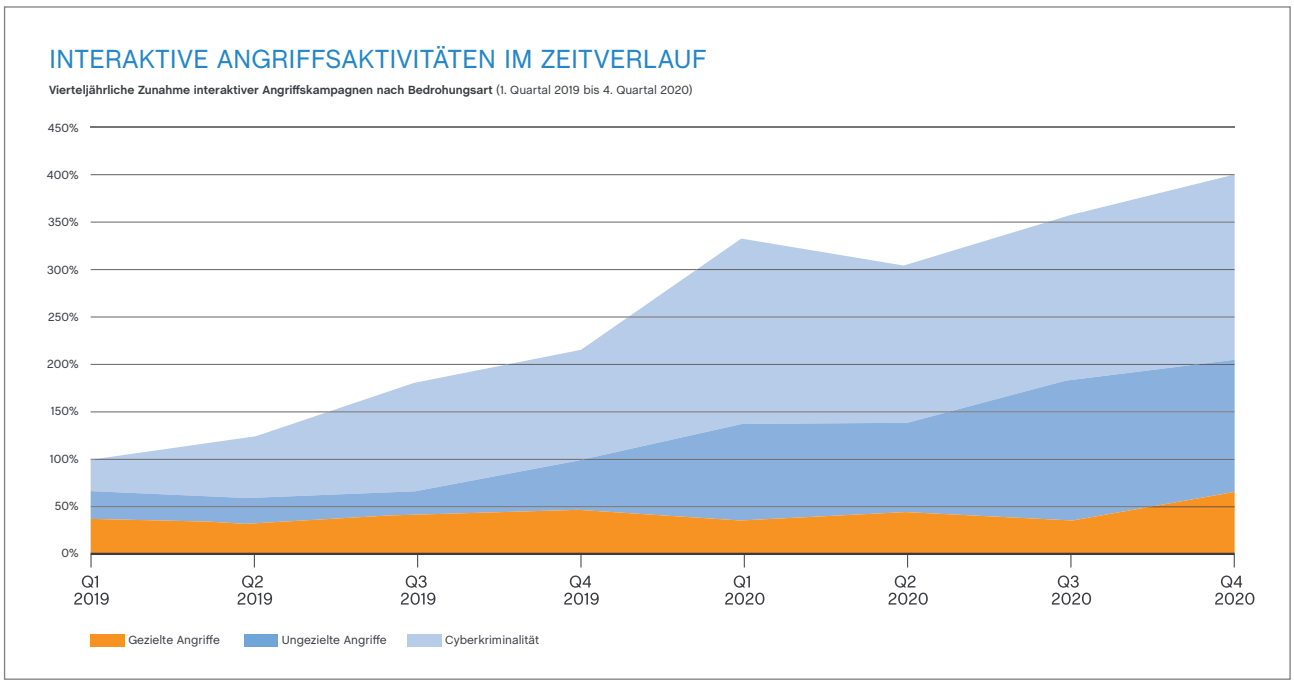
Sicherheit durch Technologie.

INHALT

1 Extrakt

Die Berichte über Cyberangriffe nehmen national und international zu. Damit steigen auch die Risiken für Krankenhäuser und andere medizinische Versorgungseinrichtungen deutlich. Im Gesundheitsbereich sind dafür verschiedene Faktoren verantwortlich:

- Durch die Pandemie werden Krankenhäuser und Arztpraxen stärker belastet und Abläufe sind weniger sicher organisiert.
- Die Digitalisierung im Healthcarebereich verändert die Prozesse und die verstärkte Nutzung elektronischer Funktionen erhöhen das Risiko.
- Die Cyberkriminellen haben zielgruppenübergreifend ihre Angriffe vervielfacht (Vervierfachung in nur 24 Monaten).



Die Vervierfachung der Angriffe in nur 2 Jahren macht die steigende Cybergefahr deutlich. Die ungezielten Angriffe (also Attacken mit zufälligen Zielen) können jede Organisation treffen. Der Cyberstörfall an der Universitätsklinik in Düsseldorf ist dafür ein erschreckendes Beispiel (Quelle: Global Threat Report 2021, Crowdstrike).

Als Konsequenz steigen die rechtlichen Anforderungen zur Informationssicherheit, IT-Sicherheit, Cyberschutz sowie Datenschutz in der ambulanten und stationären Versorgung. Die neuen Rahmenbedingungen werden durch verschiedene Gesetze, Verordnungen und Richtlinien definiert. Im Wesentlichen sind dies:

- Art. 32 DSGVO
- Art. 34 DSGVO
- § 75b und § 75c SGB V (Digitale-Versorgung-Gesetz) inkl. Richtlinien
- Qualitätsmanagement nach § 135ff SGB V und QM-Richtlinie
- §§ 8a Absatz 1/8b BSIG (KRITIS-Krankenhäuser)
- § 203 StGB i.V.m. MBO-Ä zur ärztlichen Schweigepflicht

Die o.g. Normen sind rechtsverbindlich und verpflichtend für die Verantwortlichen. In der ambulanten Versorgung sind dies die verantwortlichen Ärzte und in der stationären Versorgung die rechtlichen Vertreter der Krankenhäuser und die medizinischen Leiter der jeweiligen Abteilungen.

Die entsprechenden Risiken, sowie die rechtlichen und wirtschaftlichen Konsequenzen bei Nichteinhalten oder Nichterfüllung der verbindlichen Normen sind komplex und abhängig von vielen Kriterien. Vertiefende Hinweise können den folgenden Veröffentlichungen entnommen werden:

- Dittrich / Ippach „IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich“, GesR 2021, 285 ff.
- Prölss / Martin: Versicherungsvertragsgesetz: VVG, 31., überarbeitete Auflage, 2021
- Prof. Dr. Andreas Becker / Gärtner „Der neue § 75c SGB V – Anforderungen an die Informationssicherheit in Krankenhäusern“, in: Das Krankenhaus 04/2021, 292 ff.

Wegen der Komplexität der relevanten Rechtsnormen und den daraus abzuleitenden technischen und organisatorischen Maßnahmen, sieht der Gesetzgeber die Risikoübertragung sowie die Umsetzung der relevanten rechtlichen Verpflichtungen auch durch Dienstleister und Versicherungen vor.

Konkret sieht die Präambel der Richtlinie nach § 75b SGB V für Arztpraxen die Risikoübertragung auch an externe Dritte vor:

> *Bei der Umsetzung (der Richtlinie nach § 75b SGB V) können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen werden.*

In diesem Kontext sind auch die Anforderungen für Risikoübertragungen an Dritte, wie Dienstleistende und z.B. Cyber-Versicherer, in die aktuelle rechtliche Bewertung für Krankenhäuser einzubeziehen. Explizit wird im KHZG mehrfach auf externe Dienstleistende/IT-Dienstleistende zur Umsetzung der Vorgaben abgestellt. Im Unterschied zu § 75c SGB V wird ausdrücklich darauf hingewiesen, dass im ambulanten Bereich bei der Umsetzung der Anforderungen Risiken auch auf Versicherungen übertragen werden können.

Das Segment der Cyber-Policen wird im Jahr 2021 zu einem der Aufsichts-Schwerpunkte der Versicherungsaufsicht (BaFin). Neben einer inhaltlichen Analyse des am Markt angebotenen Versicherungsschutzes soll dabei auch die Tragfähigkeit der Produkte im Mittelpunkt stehen (Pressemitteilung Assekurata 17.05.2021).

2 Stationäre Versorgungsstruktur in Deutschland

An der stationären medizinischen Versorgung sind etwa 1.900 Krankenhäuser und etwa 1.100 Reha-Kliniken beteiligt. Sie unterscheiden sich insbesondere durch ihre Trägerschaften:

Krankenhäuser

- 40% öffentliche Krankenhäuser
- 27% freigemeinnützige Trägerschaften (Kirchen, Wohlfahrtsverbände etc.)
- 34% Privatkliniken

Reha-Kliniken

- 20% öffentliche Reha-Einrichtungen
- 28% freigemeinnützige Trägerschaften
- 52% private Reha-Kliniken

Die Krankenhäuser unterscheiden sich speziell nach ihrer Größe.
Etwa 600 kleinere Krankenhäuser mit bis zu 200 Betten übernehmen die Versorgung in ländlichen Gebieten. Die größeren Krankenhäuser (ca. 1.300) befinden sich in den Ballungsgebieten und haben durchschnittlich um die 350 Betten.

Etwa 1,0 Mio. Beschäftigte arbeiten in Krankenhäuser und betreuen insgesamt ca. 500.000 Betten.

3 Bestandsaufnahme der IT-Sicherheit und des Datenschutzes in Krankenhäusern

3.1 Heterogene IT-Umgebungen (teilweise veraltet)

Die IT-Landschaft in Krankenhäusern ist im Jahr 2021 gekennzeichnet durch heterogene und teilweise veraltete Systeme. Dies gilt einerseits für Arbeitsplätze und die medizinische Dokumentation von Patientendaten. Andererseits trifft die Analyse aber auch in besonderem Maße auf die eingesetzte Medizintechnik mit ihren digitalen Funktionen zu.

Während die Komponenten der IT-Netzwerke geschätzt durchschnittlich zwischen drei und sechs Jahren alt sind, sind viele medizintechnische Komponenten 5 – 10 Jahre alt. Das gilt insbesondere für Krankenhäuser mit nicht-privaten Trägerschaften, da in den vergangenen Jahren ein relativ großer Investitionsstau entstanden ist. Dieser soll durch das Krankenhauszukunftsgesetz (KHZG) überwunden werden.

Viele digitale Diagnose- und Therapiesysteme werden durch handelsübliche PCs gesteuert.
Die nach den früheren MPG Richtlinien zertifizierten Systeme können nicht auf aktuelle Betriebssystem- und Softwareversionen upgegradet werden, da ansonsten die Zertifizierung damit aufgehoben würde. Deshalb werden in vielen Krankenhäusern immer noch PCs mit Windows 7 oder sogar Windows XP Software eingesetzt.

Hinzu kommt, dass viele kleinere Peer-to-Peer Netze für einen Geräteverbund mit digitalen Diagnostik- und Testsystemen betrieben werden (müssen). Teilweise werden Daten physikalisch mit USB-Sticks oder auch CDs übertragen. Im Regelfall sind diese veralteten Systeme nicht standardisiert und basieren nur auf proprietären Herstellerstandards, die keinerlei Zertifizierung möglich machen.

3.2 Personalmangel im Bereich Health-IT

Die zweite große Herausforderung für die Digitalisierung im Gesundheitswesen ist der Mangel an IT-Fachleuten. Insgesamt werden Mitte 2021 ca. 86.000 offene IT-Stellen gemeldet. Davon entfallen auf den Gesundheitsbereich zwischen 10.000 – 12.000 Stellenangebote. Angesichts der Nachfrage nach IT-Spezialisten durch das Krankenhauszukunftsgesetz (KHZG) ist die Tendenz steigend.
Für 2022 werden über 20.000 offene Stellen erwartet. Können diese nicht besetzt werden, lassen sich auch die Investitionen von geförderten 4,3 Milliarden Euro schwer realisieren. Alternativen bieten Beauftragungen von Health-IT Dienstleistern. Allerdings sind gerade die überregionalen Anbieter bereits durch Großprojekte aus- bzw. überlastet.

Der Mangel an Health-IT Fachleuten ist auch ein internationales Problem. Selbst Länder aus denen ansonsten Arbeitskräfte nach Deutschland kommen könnten, brauchen die IT-Fachleute im Gesundheitswesen selbst.

3.3 Mangelnde Standardisierung der Health IT

Health-IT Standards sind in Deutschland noch stark unterrepräsentiert. Der Datenaustausch zwischen digitaler Medizintechnik und dem Netzwerk für die klinische Dokumentation basiert oft noch auf proprietären Entwicklungen.

Nach statistischen Ermittlungen sind an jedem 3. IT-Arbeitsplatz im Krankenhaus Medizintechniksysteme mit digitalem Datenaustausch installiert.

In einem Krankenhaus mit 500 Computerarbeitsplätzen werden also ca. 150 medizintechnische Systeme mit Datenspeicherung und -austausch genutzt. Nur etwa 30% realisieren den Datenaustausch nach öffentlichen Standards.

Durchgesetzt haben sich in diesem Kontext drei Standards:

- HL7 (Health-Level 7) hat sich für den Austausch von numerischen Mess- und Diagnosedaten durchgesetzt.
- DICOM (Digital Imaging and Communications in Medicine) wird hauptsächlich zur Kommunikation von Bild- und Grafikdaten genutzt, welche in sogenannten PACS (Picture and Archive Communication systems) gespeichert werden.
- GDT (Gerätedatenträger) ist eine in Deutschland entwickelte Norm für den Austausch numerischer Daten, insbesondere für Testsysteme mit seriellen Schnittstellen.

In deutschen Krankenhäusern sind insgesamt etwa 300.000 digitale Schnittstellen zwischen der Medizintechnik und dem Kliniknetzwerk installiert. Etwa 200.000 entsprechen keinem genormten Standard. Davon müssen etwa 20 – 25% als unsicher nach IT-Sicherheitsstandards gelten.

4 Rechtliche Rahmenbedingungen IT-Sicherheit und Datenschutz in der stationären Versorgung

4.1 Art. 32 DSGVO

Die Verpflichtungen aus Art. 32 der Datenschutz-Grundverordnung kann als zentrales Element auch der Regulierung der Informationssicherheit angesehen werden. Die DSGVO gilt europaweit und stellt damit eine übergeordnete Rechtsnorm dar:

> *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:*
>
> *a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
> *b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
> *c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
> *d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

4.2 § 75c SGB V

Der § 75c SGB V stellt ab 1. Januar 2022 die neue Rechtsgrundlage für die sichere Nutzung von Informationstechnologie in Krankenhäusern dar:

> *(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.*

(2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

(3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

4.3 § 8 BSI Gesetz (BSIG)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt die Rechtsnorm auch für die IT-Sicherheit in Krankenhäusern fest:

(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Das Bundesamt berät die Stellen des Bundes auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.

(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.

(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Bundesbehörden diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann festgelegt werden, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Die Sätze 5 und 6 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.

4.4 DSGVO/BDSG in der stationären Versorgung

Die Datenschutz-Grundverordnung (DSGVO) ist eine europäische Rechtsnorm. Sie wird ergänzt durch das BDSG (Bundesdatenschutz Gesetz) und die jeweiligen datenschutzrechtlichen Landesvorschriften.

Besondere Daten

Bei den in Art. 9 Abs. 1 DSGVO genannten Kategorien personenbezogener Daten, ist neben der Datenschutz-Grundverordnung immer auch das jeweilige nationale Recht zu betrachten (BDSG). Viele Erlaubnistatbestände in Art. 9 Abs. 2 DSGVO verweisen auf nationales Recht, Art. 9 Abs. 4 DSGVO erlaubt den Mitgliedsstaaten für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten eigene Rechtsgrundlagen zu schaffen. Im deutschen Recht müssen daher neben der DSGVO die jeweils geltenden bundes-bzw. landesrechtlichen Bestimmungen beachtet werden.

Protokollierung

Die Protokollierung nach DSGVO dient einerseits den Zwecken zur Erfüllung datenschutzrechtlicher Anforderungen, wie der Erteilung einer datenschutz-rechtlichen Auskunft an die betroffene Person (Art. 15 DSGVO i. V. m. mit der Regelung des jeweils geltenden Landeskrankenhausrechts), andererseits der Gewährleistung der Sicherheit und der Verfügbarkeit des Systems (Art. 32 DSGVO) und dem Nachweis der Rechtmäßigkeit der Verarbeitung der verantwortlichen Stelle.
Außerdem dient die Protokollierung auch der Nachvollziehbarkeit der Verarbeitung bei einer Verletzung des Schutzes von Gesundheitsdaten (Art. 33, 34 DSGVO).

4.5 Krankenhauszukunftsgesetz (KHZG)

Das KHZG ist mit einer umfassenden Förderung der Digitalisierung mit über 4,3 Milliarden Euro verbunden und tritt 2021 in Kraft. Das Ziel des Krankenhauszukunftsgesetzes ist unter anderem, die Modernisierung der Krankenhäuser mit Blick auf die stationäre Notfallversorgung voranzutreiben. Darüber hinaus liegt ein besonderer Fokus auf der Digitalisierung der Krankenhäuser und Ausgestaltung in Form von bundesweiten Standards.
Damit wird ein höherer Grad der Vernetzung innerhalb des Gesundheitswesens angestrebt und die Patientenversorgung verbessert. Die förderungsfähigen Vorhaben ergeben sich aus § 19 Absatz 1 Satz 1 der Krankenhausstrukturfonds-Verordnung (KHSFV). Für einige Fördertatbestände ergeben sich weitere zu erfüllende Kriterien nach § 19 Absatz 2 KHSFV.

4.6 IT-Sicherheitsgesetz (IT-SIG 2.0)

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein am 25.07.2015 in Kraft getretenes Gesetz und resultiert nach Angaben des Bundesinnenministeriums aus der im Februar 2011 beschlossenen Cyber-Sicherheitsstrategie.

Am 27.05.2021 wurde das zweite Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme (IT-Sicherheitsgesetz 2.0) im Bundesgesetzblatt verkündet (BGBl. I S. 1122). Der überwiegende Teil des IT-Sicherheitsgesetzes tritt damit am 28.05.2021 in Kraft.

Optimierte Angriffserkennung

KRITIS-Betreiber müssen mit Inkrafttreten des IT-SiG 2.0 eine Angriffserkennung umsetzen und damit sicherstellen, dass sie neben einer Anti-Viren-Lösung und einer Firewall zusätzlich ein System implementieren, welches sie automatisiert und in Echtzeit über Sicherheitsausfälle informiert.

4.7 Branchenstandard B3S für Krankenhäuser (BSI / DKG)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in Zusammenarbeit mit der Deutschen Krankenhausgesellschaft (DKG) den Branchenstandard nach B3S veröffentlicht (Oktober 2019). Danach werden die Anforderungen für große Krankenhäuser, die zu den KRITIS-Einrichtungen gehören, konkret definiert.

Krankenhäuser mit mehr als 30.000 Abrechnungsfällen pro Jahr fallen unter die sogenannten KRITIS-Regelung. Nach Angaben des statistischen Bundesamtes stehen in Deutschland ca. 1.900 Krankenhäuser mit knapp 500.000 Betten zur Verfügung. Die Zahl großer Kliniken mit 600 und mehr Betten belief sich im Jahr 2017 auf 175.

Die Rechtsnormen sind entsprechend der Größenordnung (KRITIS) und den Trägerschaften (öffentliche Träger, Kirchen, Stiftungen oder Vereine) zu beurteilen. Das gilt sowohl für die Regelungen für Informationssicherheit als auch für den Datenschutz (die Kirchen folgen eigenen Datenschutz-Regelungen)

4.8 Digitale Reifegrad-Prüfung für Krankenhäuser und Kliniken

In den meisten Krankenhäusern werden die klinischen und organisatorischen Prozesse nur partiell und unzureichend durch IT-Systeme unterstützt. Der angestrebte potenzielle Nutzen der Digitalisierung kann deshalb an vielen Stellen nicht ausgeschöpft werden. Das hat eine Auswertung von Nutzerdaten des Analysetools „Check IT“ ergeben:

Mit dem vom Marburger Bund (MB) und dem Bundesverband Gesundheits-IT entwickelten Tool können Ärzte seit Ende Mai 2019 systematisch den Nutzen von IT-Lösungen in 88 klinischen Einzelprozessen bewerten.

Der durchschnittliche digitale Reifegrad der teilnehmenden Kliniken liegt demnach bei lediglich 48 Prozent. Gründe für die unzureichende IT-Unterstützung liegen laut Marburger Bund vor allem in der fehlenden Verfügbarkeit, im Nebeneinander von analogen und digitalen Prozessen und den damit verbundenen Medienbrüchen, sowie in einer unzureichenden Funktionalität für eine vollständige Prozessunterstützung.

So gab etwa die Hälfte der Teilnehmer an, dass die notwendige Software nicht überall verfügbar ist, wo sie benötigt wird. Wichtige Anwendungen sind nur an einzelnen Arbeitsplätzen oder in einigen Abteilungen verfügbar. Nur 16 Prozent der Teilnehmer bestätigten weitgehend oder vollständig, dass mobile Endgeräte und damit nutzbare klinische Programme verfügbar sind. Bei der WLAN-Verfügbarkeit waren dies nur 26 Prozent der Teilnehmer (Ärzteblatt 09.12.2019).

Das Krankenhauszukunftsgesetz (KHZG) verpflichtet die Krankenhäuser, eine Reifegradmessung der Digitalisierung des Krankenhauses durchzuführen. Das dort verwendete Reifegradmodell und die damit verbundene Evaluationsforschung verfolgt zum einen das Ziel zu eruieren, inwieweit sich der digitale Reifegrad der geförderten Krankenhäuser im Zeitraum Juni 2021 bis Juni 2023 durch die (Teil-)Umsetzung der Fördervorhaben verbessert hat, aber auch, inwieweit nicht geförderte Kliniken das Krankenhauszukunftsgesetz als Anlass genommen haben, Maßnahmen umzusetzen, um ihren digitalen Reifegrad zu verbessern. So soll sich im Sinne einer Longitudinalstudie ein flächendeckender Überblick des digitalen Reifegrades der Krankenhäuser in Deutschland ergeben.
Die Ergebnisse werden zu einer aggregierten Analyse zusammengefasst und können so dafür genutzt werden, aufzuzeigen, welche konkreten digitalen Maßnahmen einen entscheidenden Beitrag zur umfänglichen Verbesserung des digitalen Reifegrades (Binnen- sowie Außendigitalisierung) beitragen, um hieraus Handlungsempfehlungen abzuleiten.

4.9 Die Informationssicherheits-Ausschöpfungskennzahl (ISAK)

Die **MCSS AG, Köln** hat ein Benchmarking speziell für den Gesundheitsbereich entwickelt.
Mit den **ISAK** Parametern kann der Konformitäts-Status in der Informationssicherheit eines Krankenhauses, aber auch einer ärztlichen Einzel- oder Gemeinschaftspraxis oder eines MVZ ermittelt und im Zeitverlauf bewertet werden. Mit diesem Benchmarking kann sektorenübergreifend eine Analyse und Vergleichbarkeit hergestellt werden.

Digitale Reifegradmessung: Datensicherung

Aufgabe	1	2	3	4	5	6
Regelmäßige Datensicherung täglich		X				
Regelmäßige Datensicherung wöchentlich			X	X		
Regelmäßige Datensicherung Quartal						X
Regelmäßige Datensicherung jährlich				X		
Datensicherung Archivierung intern				X		
Datensicherung Archivierung extern						X
Datensicherung Transport-Sicherheit			X			
Datensicherung Archivierung				X		
Datensicherung Verfahrensanweisungen					X	

1 = absolut geregelt
2 = weitgehend geregelt
3 = etwas geregelt
4 = eher nicht geregelt
5 = bisher nicht geregelt
6 = wird nicht geregelt

Ergebnis: ISAK Datensicherung 0,87

Referenz: ISMS C 16

Empfehlung: Das Gesamtergebnis für die Datensicherung ist zufriedenstellend. Leider bestehen offensichtlich Lücken in der mittel- und langfristigen Archivierung der Datensicherung

Die digitale Reifegradmessung der Datensicherung durch die Informationssicherheits-Ausschöpfungskennzahl (ISAK) der **MCSS AG**

5 Definitionen

5.1 IT-Sicherheit

Die IT-Sicherheit bezieht sich in der medizinischen Versorgung auf den Schutz der IT-Infrastruktur von Arztpraxen, Kliniken und Krankenhäusern etc. mit dem Ziel, wirtschaftlichen Schaden und Datenschutzverstöße zu verhindern. Es finden Werkzeuge wie Antivirenprogramme, Spamfilter und Passwortmanager ihre Anwendung.

5.2 Informationssicherheit

Die Informationssicherheit beinhaltet die IT-Sicherheit, erweitert diesen Begriff jedoch um die Sicherheit von nicht technisch gespeicherten und elektronisch verarbeiteten Daten.
Um das Erreichen von Informations- und IT-Sicherheit messbar zu machen, werden sogenannte Schutzziele definiert.

Allgemeine Schutzziele sind dabei:

- Die Vertraulichkeit von Daten, dass keine Daten von unberechtigten Personen gelesen oder verändert werden dürfen, beispielsweise durch Richtlinien, Nutzergruppen und der Anwendung des sogenannten Need-to-know-Prinzips.
- Die Integrität von Daten, dass keine Daten unbemerkt verändert werden dürfen und jede Veränderung beispielsweise durch Logs nachvollziehbar belegt werden kann. Auch die Konsistenz von Daten, also der Abhängigkeit der Daten untereinander zählt zum Schutzziel Integrität.
- Die Verfügbarkeit von Daten, die in definierten Zeiträumen gewährleistet sein muss (beispielsweise Aufbewahrungsfristen medizinischer Daten und Informationen). Dieses Schutzziel wird unter anderem durch das Erstellen von regelmäßigen Datensicherungen (Backups), redundanter Datenhaltung und Langzeit-Archivierung erreicht.
- In § 8a BSIG wird noch zusätzlich die Authentizität aufgeführt, deren Erwähnung in § 75c SGB V ohne Begründung fehlt (vgl. in Referenzen Aufsatz Becker Seite 293).

5.3 Cyber-Sicherheit

Die Cyber-Sicherheit wird häufig entweder mit der Informationssicherheit gleichgesetzt oder dieser übergeordnet. Sie beinhaltet dann nicht nur die Sicherheit von Daten und der IT-Infrastruktur einer einzelnen Organisation, sondern bezeichnet den Sicherheitsbegriff umfassender bis hin zur nationalen oder globalen Sicherheit. Damit ist Cyber-Sicherheit als Prozess zur Implementierung von Kontrollen zu verstehen, mit dem die Eintrittswahrscheinlichkeit von Datenschutzverletzungen aus einem Cyber-Angriff reduziert werden kann.

Zusammenfassung 5.1 bis 5.3 für den Bereich der medizinischen Versorgung:

IT-Sicherheit bezieht sich auf ein soziotechnisches System, in dem Informationen mit Hilfe von Informationstechnik (IT) erfasst, gespeichert und verarbeitet werden. IT-Sicherheit erhält durch die Einführung der elektronischen Patientenakte (ePA) eine deutlich größere Bedeutung.
Dagegen ist Informationssicherheit umfassender definiert und umfasst auch auf Papier dokumentierte Daten und Informationen.

5.4 Übergeordnete Definitionen

Art. 32 DSGVO Sicherheit der Verarbeitung

Stand der Technik

Der Terminus „Stand der Technik“ unterliegt einer ständigen Entwicklung.
Im Gesetz existieren verschiedene Definitionen wie z.B. in

§ 3 Abs. 10 GefStoffV

Der ‚Stand der Technik’ ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.

Eintrittswahrscheinlichkeit und Schwere des Risikos

Bei der Risikobetrachtung in der Informationssicherheit ist die Sichtweise der Patienten einerseits und die der Verantwortlichen andererseits zu betrachten:

- Risiken für Patienten
  - Risiken der Patientensicherheit
  - Risiken der Versorgungsqualität
  - Risiken der Verletzung der Privatsphäre
- Risiken für die Verantwortlichen (Ärzte und Krankenhausmanager)
  - Vertragsärztliche Risiken
  - Datenschutzrechtliche Risiken
  - Berufsrechtliche Risiken
  - Versicherungsrelevante Risiken

Spezifische Risikobereiche für Ärzte

Die exponentiell gestiegenen digitalen Anwendungen in der Medizin haben die Risikosituation hinsichtlich Cyberangriffen und IT-Störfällen extrem erhöht. Folgende Bereiche konnten in einer Studie der **MCSS AG, Köln**, identifiziert werden:

- Einsatz der Telematikinfrastruktur (verpflichtend) für alle Kassenärzte in Deutschland
- Medizintechnik mit digitaler Speicherung und digitalen Schnittstellen
- Anwendungen des elektronischen Rezepts (eRezept)
- Einsatz von Videosprechstunden mit Spezialsoftware für Telekonsultation

- Verordnung von Gesundheits-Apps in der Arztpraxis
- eArztbrief als Ablösung der analogen Kommunikation zwischen Ärzten
- Anwendung von digitalen Studien und Qualitätssicherungsprojekten (Pharma-Studien etc.)
- Medizinische Großgeräte
- Elektronische Notfalldaten für Patienten
- E-Medikationsplan mit kompletten Therapieinformationen
- elektronisches Terminmanagement über Web-Kalender

6 IT-Sicherheitsbereiche

Die IT-Landschaft eines Krankenhauses ist eine komplexe und heterogene Struktur. Mit der zunehmenden Digitalisierung besteht die Notwendigkeit die einzelnen IT-Komponenten unter Sicherheits- und Datenschutzgesichtspunkten differenziert zu betrachten und zu dokumentieren.

6.1 Digitale Medizinische Dokumentation

Die medizinische Dokumentation steht vor einem weiteren Paradigmenwechsel.
Die traditionelle Erfassung medizinischer Informationen auf Papier wurde bereits weitgehend durch digitale Textdokumentationen ersetzt. Im Rahmen der ePA-Einführung steht jetzt der Wechsel von der unstrukturierten zur strukturierten Standarddokumentation bevor. Dazu müssen die bestehenden IT-Systeme aufgerüstet und in den Funktionen erweitert werden.

Bislang war lediglich die Erfassung strukturierter Diagnosen nach dem ICD-10 Katalog erforderlich. Die zukünftige Patientenakte sieht allerdings eine strukturierte Erfassung in allen Bereichen wie z.B. bei Befunden, Therapieplänen, Anamnese-Daten etc. mit strukturierten Kodierungen vor.
Dazu wurde SNOMED-CT als internationaler Standard ausgewählt. Die entsprechenden Kodierungskataloge werden zukünftig im Rahmen der Anwendung der Telematikinfrastruktur organisationsübergreifend gestellt. Dazu sind die korrespondierenden Funktionen in den KIS-Anwendungen zur Verfügung zu stellen.

Mit der Einführung der strukturierten medizinischen Dokumentation werden technische und organisatorische Maßnahmen im Qualitätsmanagement, im Datenschutz und in der Informationssicherheit verpflichtend.

6.2 Digitale Medizintechnik

Im laufenden Jahrzehnt ist qualitativ hochwertige medizinische Versorgung ohne digitale Medizintechnik nicht mehr denkbar. Dazu werden in diesem Kontext Standardtestsysteme (beispielsweise ein Autorefraktor in der Ophthalmologie) wie auch medizinische Großgeräte (beispielsweise MRT in der Radiologie) gezählt.

Fast alle innovativen Systeme erlauben auch die Speicherung von Patientendaten in einer separaten Datenbank, die häufig redundant zur elektronischen Patientenakte geführt wird.
Der Datenaustausch zwischen der Medizintechnik und der klinischen Dokumentation wird mit standardisierten oder auch noch proprietären Schnittstellen realisiert.

Diese Schnittstellen können als die größten Herausforderungen für IT-Sicherheit und Cyberschutz angesehen werden, weil häufig nicht der globalen IT-Verwaltung des Krankenhauses unterliegen. Je nach Facharztbereich und technischer Ausstattung eines Krankenhauses sind nur ca. 30%–40% über Standards wie HL7, DICOM und GDT realisiert (eigene Untersuchungen der MCSS AG).

Die digitalen Schnittstellen der heterogenen IT-Landschaft sind die größten Risikobereiche für IT-Sicherheit und auch die häufigsten Ursachen für Stör- und Schadensfälle.

6.3 Forschungs- und Qualitätssicherungsprojekte

Medizinischer Fortschritt ist zunehmend abhängig von validen Daten und deren Auswertung. Dies ist ausdrücklich auch im Digitale-Versorgung-Gesetz (DVG) rechtlich verankert.

Die klinischen Daten werden in strukturierten Formaten in internen und externen Datenpools gesammelt und mit innovativen „Big Data“ Analysetools ausgewertet.

Die Kommunikation dieser Daten stellt eine zusätzliche Risikoebene für IT-Sicherheit und Datenschutz dar. In Artikel 35 DSGVO ist in diesem Kontext eine Datenschutz-Folgenabschätzung (DSFA) vorgesehen. Für den Cyberschutz sind komplexe technische und organisatorische Maßnahmen in Krankenhäusern zu etablieren. Die relevanten Prozessbeschreibungen sind nach QM-Gesichtspunkten zu dokumentieren und für Audits in Nachweisdokumenten zu erfassen.

6.4 Innovative Anwendungen (ePA, eRezept, eArztbrief, Videosprechstunden, Gesundheits-Apps, IoT Anwendungen etc.)

Die Digitalisierung im Gesundheitswesen wird aktuell geprägt durch Funktionen und Anwendungsbereiche, die im Digitale-Versorgung-Gesetz (DVG) beschlossen wurden.
Ab Juli 2021 besteht die Verpflichtung in der kassenärztlichen Versorgung eine elektronische Patientenakte (ePA) anzubieten. Damit muss auch das Krankenhaus standardisierte Prozesse etablieren und zukünftig die Telematikinfrastruktur (TI) nutzen. Da die meisten Krankenhäuser ebenfalls Ambulanzkliniken vorhalten, sind in diesen Bereichen der Versorgungseinheit die gleichen technischen Anforderungen wie in traditionellen Arztpraxen zu erfüllen.

Parallel zur Entwicklung der ePA wird das bisherige Papierrezept durch ein elektronisches Medikamentenrezept ersetzt. Damit überträgt die Krankenhausabteilung die Verordnungsdaten direkt auch dem KIS über die TI-Struktur an die beteiligten Apotheken.
Im Rahmen des digitalen Entlass- und Überleitungsmanagement ermöglicht das sichere Übermittlungsverfahren Kommunikation im Medizinwesen (KIM) den sicheren Versand digitaler Nachrichten und Dokumente. Zudem unterstützt KIM die automatisierte Auswertung für Empfänger.

KIM basiert auf der regulären E-Mail-Kommunikation, bietet jedoch zusätzliche Funktionen für das Signieren, Verschlüsseln und das Versenden großer Dokumenten-Anhänge. Ein speziell für diesen Zweck entwickeltes Clientmodul, das zwischen dem Mailclient und dem Mailserver positioniert wird, setzt diese Sicherheitsfunktionen um. Dieses Clientmodul kann in ein Krankenhausinformationssystem integriert werden.

Hinsichtlich der IT-Sicherheit ist die Gematik von der Verbindungsstelle im Krankenhaus bis zur Weiterverarbeitung verantwortlich. Das Krankenhaus ist für die Sicherheit der Übertragung bis zum Hardware- bzw. Software-Konnektor intern zuständig.

7 IT-Sicherheits- und Datenschutz-Störfälle

Durch die fortschreitende Digitalisierung in der stationären Versorgung ist auch die Anzahl der Störfälle in der Informationssicherheit und im Datenschutz deutlich gestiegen. Dies gilt auch für die Zeiten der Pandemie, in denen personelle Zusatzbelastungen den „Faktor Mensch“ als Auslöser vieler Schadensfälle auf deutlich über 70% steigen ließ.

Die im Folgenden aufgeführten Beispiele zeigen die große Varianz der IT-Sicherheits- und Datenschutz-Pannen:

- Im Dezember 2019 wird die gesamte IT-Infrastruktur des Klinikums in Fürth durch einen Cyberangriff lahmgelegt. Ursache ist die Einschleusung der Schadsoftware EMOTET. Für mehrere Tage kann keine Patientenaufnahme erfolgen.
- Anfang September 2020 wurde das Universitätsklinikum Düsseldorf Opfer einer Cyberattacke. Die Hacker hatten eine Schadsoftware namens „DoppelPaymer“ in das System eingebracht. Dieser sogenannte Verschlüsselungstrojaner ist bereits in zahlreichen anderen Fällen weltweit gegen Unternehmen und Institutionen von einer Hacker-Gruppe eingesetzt worden, die nach Einschätzung privater Sicherheitsunternehmen in der Russischen Föderation beheimatet sein soll. Das teilte das Gesundheitsministerium von Nordrhein-Westfalen in einem Bericht an den NRW Rechtsausschuss mit. Nach einem Bericht des BSI (Bundesamt für Sicherheit in der Informationstechnik) hatten die Hacker eine Lücke in dem System ausgenutzt, um die Server der Uniklinik zu verschlüsseln. Das BSI hatte nach eigenen Angaben bereits im Januar vor dem Problem bei Citrix gewarnt. Es wird vermutet, dass Sicherheits-Updates nicht rechtzeitig vorgenommen wurden (Organisationsfehler und menschliches Versagen).

Die Staatsanwaltschaft Düsseldorf ermittelt wegen fahrlässiger Tötung, nachdem eine Patientin starb, die wegen der Hacker-Attacke in ein weiter entferntes Krankenhaus verlegt werden musste. Es entstand außerdem ein erheblicher „Betriebsunterbrechungs-Schaden“, da über Wochen keine Patienten aufgenommen werden konnten.

- Bereits im Februar 2016 wurde das Lukaskrankenhaus in Neuss Opfer einer schweren Cyberattacke. Der Schaden belief sich auf ca. 1,9 Mio. Euro für Kosten, Umsatzausfälle durch Ersatzinvestitionen.
- Im November 2018 wurde das Kreiskrankenhaus Fürstenfeldbruck Opfer einer Cyberangriffs. Mit der Schadsoftware wurden die 450 IT-Arbeitsplätze des modernen Krankenhauses blockiert. Der Ausfall der Systeme führte zu erheblichen Unterbrechungen der medizinischen Versorgung, insbesondere der Neuaufnahme von Patienten. Der Schaden kann auf 1,0–1,5 Mio. Euro beziffert werden.

Die geschilderten Fälle, die in den Medien berichteten wurden, sind nur die Spitze des Eisbergs. Fachleute gehen davon aus, dass über 95% der Störfälle nicht an die Öffentlichkeit kommen.

Weitere Standard-Beispiele für Störungen der Informationssicherheit und Datenschutz-verstöße:

- Ein Patient bringt einen USB-Stick mit Vorbefunden als wichtigen Teil seiner Anamnese mit in die Klinik. Entgegen den Regelungen (QM-Verfahrens-anweisung) erfolgt keine Prüfung auf Schadsoftware, da der Test-Rechner defekt ist und kein Back-Up System (Verstoß gegen Richtlinie) zur Verfügung steht. Der infizierte USB-Stick wird in den Arbeitsplatzrechner der Abteilung eingelesen. Erst nach Wochen wird die Schadsoftware aktiv und legt die hochspezialisierte Medizintechnik lahm (hoher „Hidden-Cyber“ Schaden).
- Auf einem „Stand-alone“ Arbeitsplatz im Krankenhaus wird die Privatliquidation des Chefarztes abgerechnet. Aus Gefälligkeit stellt ein IT-Mitarbeiter eine Kabelverbindung zum Arbeitsplatzrechner des Krankenhauses her, um Abrechnungsdiagnosen zeitsparend zu übernehmen. Da der Abrechnungsrechner auch für die Erstellung der Vorträge verwendet wird, werden Texte aus dem Internet heruntergeladen. So kommt auch Schadsoftware auf den privaten Rechner und damit in das Netzwerk des Krankenhauses. Der Vorfall fällt erst nach Wochen auf und in der Zwischenzeit wurden mehr als 40% aller Arbeitsplätze (mehr als 200 in der Klinik) infiziert.
- Ein neues Laser-Diagnosesystem wird angeschafft und ein altes Gerät zur Verrechnung in Zahlung gegeben. Die Patientendaten mit vollständigen Namen und Befunden werden nur virtuell und damit unsachgemäß gelöscht. Das alte Gerät wird überholt und von einem Zwischenhändler an eine andere Klinik verkauft. Nach einiger Zeit wird festgestellt, dass noch die Patientendaten des ursprünglichen Krankenhauses einsehbar sind. Ergebnis: eklatanter Verstoß gegen die DSGVO und das BDSG (menschliches Versagen mit Verstoß gegen QM-Regelungen).
- Ein sogenannter Geräterechner, der eine medizinische Kamera steuert und die Bilddaten speichert läuft noch auf dem Betriebssystem Windows 7. Ein Update ist nicht möglich, da ansonsten die Zertifizierung für das teure Kamerasystem erlischt. Da das System aber im Netzwerk eingebunden ist, installiert der Techniker einen nicht autorisierten Patch. Der alte Windows 7 Rechner wird zu einem „Einfallstor“ für das gesamte Netzwerk und verursacht damit erhebliche Schäden durch zeitweisen Ausfall der IT-Arbeitsplätze der gesamten Abteilung.
- Ein Patient nutzt ein digitales Schmerztagebuch, das auch Grundlage für ein wissenschaftliches Forschungsprogramm ist. Es wurde ein improvisiertes Übertragungsprogramm (ohne technische Sicherheitsprüfung) entwickelt, mit dem die Daten vom Tablet-Computer in eine separate Patienten-Dokumentation im Krankenhausnetzwerk gespeichert werden kann. Der Tablett Computer des Patienten wird aber auch privat in der Familie genutzt. Nach einer Infizierung mit einem Schadprogramm wird mit der Übertragung des Schmerztagebuchs auch das Kliniknetz infiziert. Problem: die improvisierte digitale Schnittstelle und die proprietäre Software sind der IT-Abteilung unbekannt und kann so auch nicht evaluiert oder eliminiert werden.
- Ärzte nehmen regelmäßig an Kongressen und anderen Fortbildungs-maßnahmen teil. Ein Kongressteilnehmer hat im Poster Bereich (Ausstellung wissenschaftlicher Forschungsergebnisse) einen USB-Stick mit der Aufschrift der medizinischen Fachgesellschaft „gefunden“ und zur Übertragung seiner Dateien an seinen Kollegen verwendet.

- Der USB-Stick war von Cyber-Kriminellen infiziert, um sogenannte „Trojaner“ in Kliniksysteme zu platzieren. Im Krankenhaus wurde der infizierte USB-Stick im Kliniknetz genutzt. Nach einigen Wochen wurde das eingeschleuste Schadprogramm aktiv und führte zu einem Erpressungsversuch. Der eigentliche Ursprung konnte nur durch Zufall ermittelt werden.
- Moderne Klinikbetriebe nutzen umfangreiche Bildarchivierungssysteme, sogenannte PACS-Server (Picture Archive and Communication Systems-Server), in denen die Bilder gespeichert werden und von Medizinern bei Bedarf abgerufen werden können. PACS-Server nach DICOM-Standard sind häufig angreifbar und große Mengen sensibler Patientendaten sind einsehbar: Über 24 Millionen Datensätze mit mehr als 700 Millionen verlinkten Bildern.
- Aus diesen sind 400 Millionen tatsächlich herunterladbar. Diese ungeschützten Systeme stehen in 52 Ländern der Welt. Neben der “Offenheit“ der Systeme, haben diese auch noch tausende „echte“ Schwachstellen, also veraltete Webserver-Versionen und angreifbare Datenbank-Instanzen. Zum Teil erlauben es die PACS-Server auch, via http und einen Webbrowser die Patientendaten und Bilder zu betrachten. (aus Greenbone Report).

  Da alle großen Krankenhäuser in Deutschland DICOM Server nutzen gehen Fachleute von erheblichen Risiken aus, wenn die Systeme noch mit veralteten Versionen genutzt werden.

  Die (bei der Greenbone Analyse) gefundenen, offenen PACS-Server sind Teil eines medizinischen/klinischen Prozesses. Die gefundenen, offenen PACS-Server sind Teil eines medizinischen/klinischen Prozesses. D.h. sie kommunizieren innerhalb eines Netzwerkes mit IP-fähigen Geräten über das DICOM-Protokoll. Ein Netzwerk-Scan im Addressbereich des jeweiligen Systems könnte weitere „lohnende Ziele“ für einen Angreifer aufdecken. Dabei kann ein Angreifer davon ausgehen, dass auch auf diesen Systemen die Absicherung nicht den gängigen Standards entspricht – analog zum bereits gefundenen PACS-Server.

8 Mögliche Rechtsfolgen bei Nichterfüllung der Normen

8.1 Datenschutzrechtliche Folgen

Die negativen Rechtsfolgen aus Datenschutzverstößen aufgrund von Missachtung der Regelungen nach § 75b SGB V sind wahrscheinlicher als die Rechtsfolgen nach Vertragsarztrecht.
Die Abschreckung steht häufig im Vordergrund der Begründung.

In der Präambel der Richtlinie nach § 75b SGB V wird ausdrücklich darauf hingewiesen, dass die Regelungen auch der Konkretisierung der Pflichten nach Art. 32 DSGVO dienen (siehe 2.1. Definitionen und Geltungsbereiche).

Erstaunlich ist, dass die Anforderungen im § 75c Absatz 1 SGB V nicht – wie im KRITIS-Bereich gemäß BSI-Kritisverordnung (BSI-Kritis-V) – auf die stationäre Patientenversorgung eingegrenzt sind. Daher dürfte hier auch die teilstationäre Behandlung und die ambulante Versorgung zum Regelungsbereich gehören. Dann stellt sich die Frage zur Abgrenzung der Regelung im Verhältnis zu § 75b SGB V, der ja eigentlich die Regelung für die niedergelassenen Ärzte enthält, zu denen auch die ermächtigten Krankenhausärzte und Ambulanzen gehören. Hier kommen – zumindest vom Wortlaut – beide Normen für denselben Sachverhalt zur Anwendung, eine gesetzgeberische Ungenauigkeit, die die Praxis klären muss. Die Festlegung des individuellen Geltungsbereichs sollte daher das tatsächliche Leistungsgeschehen und die für das ISMS relevanten Strukturen und Prozesse heranziehen.

Bußgeldverfahren nach Art. 83 DSGVO

Bei Verstößen gegen Art. 32 DSGVO im Kontext der Richtlinie nach § 75b SGB V können erhebliche Bußgelder verhängt werden. Nach Art. 83 der DSGVO können Bußgelder bis zu 2% des Jahresumsatzes der medizinischen oder pflegenden Einrichtung verhängt werden. Das sind für eine Einzelpraxis maximal 10.000 Euro und für eine große Gemeinschaftspraxis mit 5 Mio. Euro Jahresumsatz bis zu 100.000 Euro. Die maximale Höhe beträgt 10 Millionen Euro, was aber in der ambulanten und stationären medizinischen Versorgung nicht relevant ist.

Gegen Krankenhäuser wurden bereits Bußgelder über 100.000 Euro wegen organisatorischer Versäumnisse verhängt.

Schadensersatzzahlungen nach Art. 82 DSGVO

Eine unzureichende IT-Sicherheit nach § 75b SGB V in Praxen und nach § 75c SGB V in Krankenhäusern kann zu erheblichen Schadensersatzzahlungen an Patienten führen. Nach Art. 82 der DSGVO können durch Datenschutzverstöße geschädigte Patienten Schadensersatzansprüche geltend machen. Dies gilt sowohl für materielle wie auch für immaterielle Schadensereignisse.

Fachleute sehen in den potenziellen Schadensersatzforderungen erhebliche Gefahren.
Dabei wird darauf hingewiesen, dass die zivilrechtlichen Ansprüche im Kontext der EU-Datenschutz-Grundverordnung abschreckende Wirkungen erzielen sollen. Da bislang keine gefestigte Rechtsprechung vorliegt, ist die Bandbreite der Zahlungen schwer einzuschätzen bzw. zu limitieren.

Ein weiteres Risiko ergibt sich aus der möglichen Beweislastumkehr, die Juristen im Kontext der Rechenschaftspflicht nach Art. 5 DSGVO als wahrscheinlich ansehen.

Fazit:

Die Eintrittswahrscheinlichkeit von Datenschutzverstössen ist nicht zu unterschätzen und auch die Schadenshöhe aus Sicht des Arztes ist schwer kalkulierbar. Mit den konkreten Anforderungen nach § 75c SGB V ist eine Missachtung der Anforderungen an die IT-Sicherheit grob fahrlässig und damit mit sehr konkreten Risiken verbunden.

Meldepflichten nach Art. 33 DSGVO

Ein weiteres finanzielles Risiko ergibt sich aus § 33 DSGVO. Danach müssen die Verantwortlichen eine konkrete Datenschutzverletzung innerhalb von 72 Stunden nach Kenntnisnahme der zuständigen Datenschutz-Aufsichtsbehörde melden.

Bei der Meldepflicht einer Datenschutzverletzung kommt es nicht darauf an, ob der Arzt für einen Vorfall selbst verantwortlich ist. Ist ein Auftragsverarbeiter (z.B. der Dienstleister für die externe Datensicherung) involviert, so muss dieser unverzüglich die Meldung des Vorfalls an den Arzt veranlassen. Somit kommt es auf die Schuldfrage bei der Meldepflicht nicht an.

Für die Meldeprozesse sind genaue Vorschriften veröffentlicht. Die Anforderungen ergeben sich aus Art. 34 DSGVO. Hinzu kommt die Regelung zur Benachrichtigung der betroffenen Patienten. Unterschieden wird hier zwischen einer Einzelbenachrichtigung und einer öffentlichen Benachrichtigung (z.B. in der Tagespresse). Aus letzterer kann sich ein erheblicher Reputationsschaden ergeben, der nur sehr schwer kalkuliert werden kann.

Zusammenfassung:

Meldepflichtverletzungen bei einer Datenschutzverletzung sind nicht selten. Bei Verlusten großer Mengen von Patientendaten, oder wenn Datensicherungsmedien mit medizinischen Daten öffentlich zugänglich werden, können Schäden im 6-stelligen Euro-Bereich entstehen.

8.2 Folgen nach § 8b BSIG

Nach § 8b Abs. 3 BSIG sind Krankenhäuser, die den KRITIS-Sicherheitsstandard erfüllen müssen, verpflichtet eine jederzeit erreichbare Kontaktstelle einzurichten. Damit verbunden ist eine Verpflichtung zur Meldung von möglichen Risiken und Störfällen.

Konkret ergibt sich hieraus die Anforderung zur Einführung eines BCMS (Business-Continuity-Management-System).

8.3 Versicherungsrelevante Folgen

Im Bereich der IT-Sicherheit sind 3 Versicherungsbereiche relevant:

- Cyber-Versicherung
- Haftpflicht- und Berufshaftpflichtversicherung
- Betriebsunterbrechungs-Versicherung (BU)

Die steigende Gefährdung der Informationssicherheit im Gesundheitswesen leitet einen Paradigmenwechsel auch für Versicherungen in der medizinischen Versorgung ein. Im Mittelpunkt steht die Digitalisierung mit den neuen Errungenschaften der medizinischen Versorgung, aber auch mit zusätzlichen Risiken für IT-Sicherheit und Datenschutz.

Verstößt der Versicherungsnehmer gegen Verpflichtungen aus dem Versicherungsvertrag, so kann der Versicherer Schadenszahlungen reduzieren oder ganz verweigern.

Im Einzelfall kommt es auf den konkreten Vertrag an.

Unterschieden wird dabei nach vertraglichen und gesetzlichen Obliegenheiten:
Obliegenheiten sind Normen, die dem Versicherungsnehmer auferlegen, sich in einer bestimmten Weise zu verhalten. Das einem Versicherungsnehmer obliegende Verhalten kann ein Tun oder auch ein Unterlassen sein. Der Versicherer kann zwar vom Versicherungsnehmer nicht verlangen, sich entsprechend einer Obliegenheit zu verhalten. Beachtet der Versicherungsnehmer eine Obliegenheit jedoch nicht, kann der Versicherer nach § 28 Absatz 2 VVG seine Leistung ganz oder teilweise kürzen.

Verstöße gegen Obliegenheiten können den Versicherer im Schadenfall zu Leistungskürzungen berechtigen. In der Sachversicherung spielt die Einhaltung von Sicherheitsvorschriften eine große Rolle. Die Regulierungspraxis zeigt, dass Versicherer den Einwand der Verletzung von Sicherheitsvorschriften erheben können, um die Einigungsbereitschaft von Versicherten in Verhandlungen zu erhöhen. Um Auseinandersetzungen zu vermeiden, sollten Verantwortliche deshalb die Einhaltung des Art. 32 DSGVO, § 75c SGB V und der Richtlinie nach § 75b SGB V jederzeit dokumentieren können.

Mögliche Folgen für Versicherte

Kündigung des Versicherungsvertrags

Verletzt der Versicherungsnehmer vorsätzlich oder grob fahrlässig eine Obliegenheit, die er vor Eintritt des Versicherungsfalls gegenüber dem Versicherer zu erfüllen hat, so kann der Versicherer innerhalb eines Monats, nachdem er von der Verletzung Kenntnis erlangt hat, den Vertrag kündigen (§ 58 VVG).

Der Versicherer hat kein Kündigungsrecht, wenn der Versicherungsnehmer nachweist, dass er die Obliegenheit weder vorsätzlich noch grob fahrlässig verletzt hat (§ 57 VVG).

Leistungsfreiheit bei Obliegenheitsverletzungen

Verletzt der Versicherungsnehmer eine Obliegenheit vorsätzlich, so ist der Versicherer von der Verpflichtung zur Leistung frei. Bei grob fahrlässiger Verletzung der Obliegenheit ist der Versicherer berechtigt, seine Leistung in dem Verhältnis zu kürzen, das der Schwere des Verschuldens des Versicherungsnehmers entspricht.

Verletzt der Versicherungsnehmer eine nach Eintritt des Versicherungsfalls bestehende Auskunfts- oder Aufklärungsobliegenheit, so ist der Versicherer nur dann vollständig oder teilweise leistungsfrei, wenn er den Versicherungsnehmer durch gesonderte Mitteilung in Textform (z.B. E-Mail, Telefax oder Brief) auf diese Rechtsfolge hingewiesen hat.

8.4 Förderrechtliche Folgen

Förderrechtliche Folgen aus Verpflichtungen zur IT-Sicherheit können sich aus dem Krankenhauszukunftsgesetz (KHZG) ergeben. Im Rahmen dieses Gesetzes werden Investitionen in die Digitalisierung der Krankenhäuser mit mehr als 4 Milliarden Euro gefördert. Nach § 14a Abs. 3 Satz 5 KHZG sind 15% der beantragten Fördermittel für Maßnahmen zur IT-Sicherheit zu verwenden. Damit stehen über 600 Millionen Euro Fördermittel (ca. € 300.000 pro Krankenhaus), für die IT-Sicherheit, zur Verfügung.

Bei Nichteinhaltung der geforderten Mittelrelationen sind Rückzahlungen und Sanktionen aufgrund von nicht korrekter Verwendung vorgesehen.

8.5 Risikoübertragung an Dienstleister und Versicherer

Der Gesetzgeber geht davon aus, dass in der stationären und ambulanten Versorgung nicht ausreichende personelle Kapazitäten und Qualifikationen zur Verfügung stehen. Es ist deshalb vorgesehen, dass die Umsetzung des Risikomanagements auch an Dritte, wie qualifizierte Dienstleister und spezialisierte Versicherungen mit entsprechenden Assistance Leistungen übertragen werden können.

9 Lösungen in der Umsetzung der Rechtskonformität

Die neuen umfassenden Rechtsnormen und Empfehlungen für Krankenhäuser machen eine konsolidierte Planung erforderlich. Rechtliche Rahmenbedingungen bestehen für die IT-Sicherheit (z.B. § 75c SGB V), den Datenschutz nach DSGVO und BDSG und das Qualitätsmanagement, insbesondere nach §§ 135 ff SGB V und den korrespondierenden GBA Richtlinien Beschluss.
Alle drei Bereiche sind prozessorientiert und überschneiden sich in wesentlichen Teilaspekten.
Es ist deshalb sinnvoll, dass in Krankenhäusern ein übergeordnetes Prozessmanagement definiert wird, um Kapazitäten und Kompetenzen zu bündeln und gezielt einzusetzen.

Anforderungsprofile aus den drei Organisations- und Arbeitsbereichen können in einer Mindestanforderung zur Realisierung einer Rechtskonformität definiert werden.

9.1 Organisatorische Maßnahmen

In allen drei Prozessbereichen (Informationssicherheit, Datenschutz, QM) werden technische und organisatorische Maßnahmen (TOM) umgesetzt. Dementsprechend bietet sich eine Strukturierung und Synchronisierung der Maßnahmen an.

9.1.1 Verantwortungsbereiche und Rollen

Der erste Schritt eines konsolidierten Prozessmanagements in Krankenhäusern ist die Definition der Verantwortungsbereiche und Rollen. In vielen Krankenhäusern bestehen unterschiedliche Abteilungszuordnungen. So ist für den DSGVO Bereich häufig die Rechtsabteilung zuständig und für IT-Sicherheit und den Cyberschutz die interne IT-Abteilung.

Nach der DSGVO ist ein qualifizierter Datenschutzbeauftragter (DSB) zu benennen und öffentlich bekannt zu geben. Im Rahmen eines Informations-Sicherheit-Management-System (ISMS) wird ein Informations-Sicherheitsbeauftragter (ISB) empfohlen. Ebenso ist im Bereich des Qualitäts-Managements (QM) ein interner Qualitäts-Management-Berater (QMB) der übliche Standard.

Unter dem Gesichtspunkt der Patientensicherheit und des Hygienemanagements gibt es zusätzlich den Patientensicherheitsbeauftragten sowie den Hygiene-beauftragten. Je nach Organisationsstruktur des Krankenhauses können unter Effizienz-Gesichtspunkten in einem übergeordneten Organigramm die genauen Schnittstellen zwischen den einzelnen Beauftragten bzw. Abteilungen definiert werden.

9.1.2 Notfallplan und Notfallmanagement

Die Bezeichnung Notfallmanagement ist in den Rechtsnormen unterschiedlich belegt.
Im Rahmen des Qualitätsmanagements wird das Notfallmanagement insbesondere im Kontext der Patientensicherheit definiert. In den Rahmenbedingungen für IT-Sicherheit bezieht sich das Notfallmanagement auf die Wiederherstellung der arbeitsfähigen IT-Infrastruktur nach einem Störfall.

In einem übergeordneten Notfallmanagement können die einzelnen Maßnahmen konzertiert betrachtet werden. Dies ist insbesondere im Zusammenhang mit dem übergeordneten Versicherungsmanagement (Cyberschutz, Haftpflicht und Betriebsunterbrechung) sinnvoll.

9.1.3 Awareness Coaching aller Mitarbeitenden

Für alle Prozessbereiche im Krankenhaus gilt, dass bis zu 80% der Stör- und Schadensfälle auf den „Faktor Mensch“ zurückzuführen sind. Dies wird durch Untersuchungen des Bundesamts für Sicherheit der Informationstechnik (BSI) und des Gesamtverbands der Deutschen Versicherungen (GDV) deutlich. Danach sind über 50% der Mitarbeitenden nicht ausreichend ausgebildet oder unvollständig informiert, wenn es um Pflichten für Informationssicherheit, Datenschutz und Qualitätsmanagement geht.

Zur Gewährleistung der Rechtskonformität ergibt sich aus den Rechtsnormen die Notwendigkeit einer konsolidierten Schulungs- und Coachingplanung. Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Ein übergreifendes Curriculum kann je nach Reifegrad der Organisation auf 24 bzw. 36 Monate ausgerichtet werden.

9.1.4 Digitale Managementsysteme (ISMS, DSMS, QMS)

Herkömmliche Organisationsmittel wie analoge Dokumentensammlungen sind für ein zeitgemäßes Prozessmanagement ungeeignet. Es empfiehlt sich ein digitales, idealerweise cloudbasiertes System, das die Verfügbarkeit aller Prozessbeschreibungen, Verfahrensanweisungen und internen Regelungen für alle Mitarbeitenden gewährleistet und zur Verfügung stellt.

Aus Sicherheitsgründen (siehe Empfehlungen der Bundesärztekammer und der KBV) ist das cloudbasierte System von den internen IT-Infrastrukturen, wie z.B. dem KIS, zu trennen. Das BSI (siehe IT-Sicherheitsrichtlinie nach § 75b SGB V) definiert in der 75b Richtlinie entsprechende Sicherheitsmaßnahmen für den Einsatz von Tablet-Computern und Smartphones.

Digitale Managementsysteme in der stationären Versorgung können Informationssicherheit, Datenschutz und QM in einer Anwendung konsolidieren. Nach dem „Stand der Technik“ bieten sich cloudbasierte SaaS Systeme mit E-Learning und Big Data Analysen an.

Digitale Managementsysteme in der stationären Versorgung können Informationssicherheit, Datenschutz und QM in einer Anwendung konsolidieren. Nach dem „Stand der Technik“ bieten sich cloudbasierte SaaS Systeme mit E-Learning und Big Data Analysen an.

9.1.5 Inventarisierung und laufende Dokumentation

In allen Krankenhäusern bestehen heterogene IT-Landschaften. Dies gilt insbesondere im Zusammenhang mit der digitalen Medizintechnik in dem Gesamtnetzwerk und den Subsystemen der Fachabteilungen. Deshalb ist die vollständige Dokumentation aller IT-Komponenten in vielen Fällen eine organisatorische, aber auch zeitliche Herausforderung. Teilweise sind den IT-Abteilungen Peer-to-Peer Netzwerke in der Steuerung von Diagnosegeräten gar nicht offiziell bekannt. Veränderungen und vor allem Sicherheitsupdates für alle Systeme sind abteilungsübergeordnet zu dokumentieren.

Die Schadenshöhen sind deshalb häufig unnötig groß, weil nicht alle IT-Anwendungen mit dem letzten Status dokumentiert sind. Dies gilt insbesondere dann, wenn die Hersteller digitaler Medizintechnik ihre Systeme unabhängig von der lokalen IT-Abteilung aktualisieren und betreuen.

9.1.6 Benchmarking und Monitoring

Der Status einer Prozessorganisation ist nur dann aussagekräftig, wenn ein Benchmarking als Steuerungssystem für das Management der Organisation und die risikotragenden Versicherungen transparent eingerichtet ist. Ein erster Schritt in die richtige Richtung ist die Messung des digitalen Reifegrades. Diese ist bislang allerdings auf Investitionsbedarf und weniger auf Risikobeherrschung ausgerichtet.

Ein solches übergeordnetes Benchmarking wird mit dem ISAK-System (Informationssicherheits-Ausschöpfungskennzahl der MCSS AG) angeboten. Die allgemeinen Datenpunkte entsprechen dem Fragenkatalog zu Cyber-Risiken des GDV. Der Katalog wird ergänzt über die spezifischen risikorelevanten Datenpunkte im Healthcare-Bereich (z.B. zu digitaler Medizintechnik und speziellen Datenschnittstellen).

9.2 Technische Maßnahmen

Zu den technischen Maßnahmen im Sinne der Informationssicherheit und des Cyberschutzes werden alle Anforderungen gezählt, die in einem ISMS nach BSI-Standard definiert sind.

Eine Mindestanforderung auch für Krankenhäuser kann auch nach der Standardvorgabe der VdS 10000 und 10010 abgeleitet werden. Im KRITIS-Bereich empfiehlt sich eine Anwendung nach ISO 27001.

9.2.1 Schutzmaßnahmen mit Datensicherungen, Virenschutz, Firewall etc.

Mit der IT-Sicherheitsrichtlinie nach § 75b SGB V hat das BSI in Kooperation mit der Kassenärztlichen Bundesvereinigung (KBV) genaue Anforderungen für den Gesundheitsbereich definiert. Während in der Richtlinie konkrete Anforderungen an Großpraxen ab 20 Mitarbeitenden definiert werden, sind bislang keine Spezifikationen nach § 75c SGB V veröffentlicht worden.

9.2.2 Pen-Testing

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Klassifikationsschema entwickelt, anhand dessen sich ein Penetrations-Test (Pen-Test) beschreiben lässt.
Im Wesentlichen werden sechs verschiedene Kriterien betrachtet:

Informationsbasis, Aggressivität, Umfang, Vorgehensweise, Technik, Ausgangspunkt

Anhand dieser Kriterien wird dann zusammen mit dem Krankenhaus ein individueller Test zusammengestellt. In der Praxis werden meist mehrstufige Tests durchgeführt, bei denen mehrere Kriterien nacheinander zur Anwendung kommen.

In Krankenhäusern wird bei Pen-Tests häufig die digitale Medizintechnik ausgespart. Bei Vorkommnissen entstehen Haftungsrisiken und die wichtigen Systeme können nicht mehr eingesetzt werden (Handelsblatt: Hacker greifen in Coronakrise verstärkt Krankenhäuser an, 09.04.2020).

9.3 Standardisierung nach Health-IT (siehe DGV)

Mit Umsetzung des Digitale-Versorgung-Gesetzes werden auch internationale Health-IT Standards eingeführt. Dies stellt eine weitere Herausforderung für Krankenhäuser dar, da mit der Umsetzung von Standards auch neue Prozesse in der klinischen Dokumentation verbunden sind.

SNOMED CT

Als Terminologie Standard wurde SNOMED CT („Systematized Nomenclature of Medicine Clinical Terms“) in den Richtlinien festgeschrieben. Seit 1. Januar 2021 wird die medizinische Terminologie SNOMED CT vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) für alle Nutzer in Deutschland zur Verfügung gestellt.

SNOMED CT ermöglicht es, medizinische Begriffe in verschiedenen Computersystemen international eindeutig abzubilden – die Voraussetzung für den elektronischen Austausch von Gesundheitsdaten. SNOMED CT wird als Terminologie der elektronischen Patientenakte (ePA) zukünftig eingesetzt.

Mit der Einführung einer öffentlichen Standardisierung der medizinischen Begriffe steigt auch die Gefahr des gezielten Missbrauchs. Entsprechend sind die Dokumentationsprozesse im Krankenhaus anzupassen (z.B. Verfahrensanweisungen im Qualitätsmanagement).

HL7

Als Health Level 7 (HL7) bezeichnet man sowohl eine Sammlung internationaler Standards, die einen Datenaustausch zwischen IT-Systemen von Einrichtungen des Gesundheitswesens erlauben, als auch die Organisation selbst, die diese Standards entwickelt.

Die HL7-Standards ermöglichen eine Interoperabilität unterschiedlicher Systeme innerhalb des Gesundheitswesens. Dazu zählen Krankenhaus-Informationssysteme (KIS), Laborinformations- und Managementsysteme (LIMS), Praxis-Verwaltungs-systeme (PVS), Systeme zur Leistungsabrechnung und zur Elektronischen Patientenakte (ePA).

Der HL7 CDA Standard (Clinical Document Architecture) ist die Grundlage des Informationsaustausches zwischen Ärzten in der Telematikinfrastruktur. Die Definition des elektronischen Arztbriefs nach HL7 CDA erlaubt den strukturierten Datenaustausch zwischen Arztpraxen und Krankenhäusern. Es gelten entsprechende Sicherheitsstandards nach der HL7 Norm.

DICOM

Der DICOM-Standard (Digital Imaging and Communications in Medicine) ist das gängige Framework für alle PACS Produkte (Picture Archive and Communication Systems). Da bildgebende Verfahren und Systeme Standard in der zeitgemäßen medizinischen Diagnostik sind, werden DICOM Komponenten in fast allen Krankenhäusern eingesetzt. Dabei ist zu unterscheiden nach DICOM Formaten und DICOM basierten Workflows.

Der DICOM-Standard wurde vor über 25 Jahren in den USA mit den großen PACS Anbietern entwickelt und stellt eine hohe Kompetenzanforderung an die IT-Experten. Da es zu wenige DICOM Fachleute auf dem internationalen Markt gibt, kommt es immer wieder zu Störfällen durch unsachgemäße Nutzung von DICOM Systemen (siehe hierzu auch die Beispiele für IT-Sicherheitsstörfälle).

Im Rahmen des Krankenhauszukunftsgesetzes (KHZG) wird der Einsatz investitionsintensiver DICOM Installationen zunehmen. Dadurch entsteht aber auch eine weitere Abhängigkeit von qualifizierten DICOM Dienstleistern.

9.4 Fördermöglichkeiten aus dem KHZG

Für die Förderung der IT-Modernisierung in Krankenhäusern stehen über 4 Milliarden Euro zur Verfügung

Beim Bundesamt für Soziale Sicherung (BAS) wurde ein Krankenhauszukunftsfonds (KHZF) eingerichtet. Ab dem 1. Januar 2021 werden dem KHZF durch den Bund 3 Milliarden Euro über die Liquiditätsreserve des Gesundheitsfonds zur Verfügung gestellt. Die Länder und/oder die Krankenhausträger übernehmen 30 Prozent der jeweiligen Investitionskosten. Insgesamt steht für den KHZF somit ein Fördervolumen von bis zu 4,3 Milliarden Euro zur Verfügung.

Förderung von Notfallkapazitäten und digitaler Infrastruktur

Gefördert werden Investitionen in moderne Notfallkapazitäten und eine bessere digitale Infrastruktur, z.B. Patientenportale, elektronische Dokumentation von Pflege- und Behandlungsleistungen, digitales Medikationsmanagement, Maßnahmen zur IT-Sicherheit sowie sektorenübergreifende telemedizinische Netzwerk-strukturen. Auch erforderliche personelle Maßnahmen können durch den KHZF finanziert werden.

Der Stand der Digitalisierung der Krankenhäuser wird zum 30. Juni 2021 und 30. Juni 2023 evaluiert.

Grundlagen der Krankenhausfinanzierung

In Deutschland werden Krankenhäuser in einem „dualen Finanzierungssystem“ finanziert. Die Länder übernehmen die Investitionskosten der Krankenhäuser (zum Beispiel Errichtung von Gebäuden, Geräteausstattung), die in den Krankenhausplan aufgenommen wurden. Die Krankenkassen und selbstzahlende Patientinnen und Patienten finanzieren mit den für Krankenhausbehandlungen zu entrichtenden Entgelten die Betriebskosten (Personal, Gebäudeerhaltung, Verbrauchsgüter).

10 Ableitung von Handlungsempfehlungen aus den aktuellen Entwicklungen der Cyberschutz- und Informationssicherheits-Risiken

- Initiierung einer konzertierten Analyse im Krankenhaus mit Beteiligung aller Beauftragten für IT-Sicherheit (ISB), Datenschutz (DSB), Patientensicherheit (PSB), Qualitätsmanagement (QMB). Ziel ist die Identifikation von übergeordneten Risiken und Synchronisierung der Prozesse in Notfällen mit Identifikation von Synergien.
- Etablierung eines system-unabhängigen Notfallmanagements, das cloudbasiert auch auf Smart-Phones und Tablets laufen kann, wenn das Klinik-Netzwerk nach einem IT-GAU nicht für den Abruf der Notfall-anweisungen zur Verfügung steht.
- Abstimmung und Vereinbarung eines angemessenen Versicherungsschutzes gegen Cyberangriffe, Betriebsunterbrechungen und Haftpflicht-Risiken mit einem spezialisierten Versicherer.
- Etablierung eines cloudbasierten Awareness- und Coaching-Systems für alle Mitarbeitende bei Nutzung handelsüblicher Endgeräte (Smart-Phones, Tablet Computer) mit E-Learning Komponenten wie Wissenstests, Erklärvideos und digitalen Schulungskomponenten.
- Einführung eines digitalen Monitoringsystems zur laufenden Kontrolle des jeweils aktuellen Reifegrads der Schutz- und Sicherheitsmaßnahmen im Krankenhaus.
  Beispiel: **MCSS** Benchmarking mit **ISAK** (Informationssicherheitskennzahl).
- Einführung eines digitalen Prozess-Managementsystems für konzertiertes und rechtskonformes Umsetzen von Informationssicherheit, Datenschutz und Qualitätsmanagement.

11 Zusammenfassung

Die zunehmende Digitalisierung im Gesundheitswesen bietet viele Potentiale für die medizinische Versorgung. Der Gesetzgeber hat dazu mit zusätzlichen Rechtsnormen neue Rahmenparameter definiert. Exemplarisch dafür ist z.B. § 75c SGB V und das Krankenhauszukunftsgesetz (KHZG). Damit verbunden ist ein umfassendes „Change-Management“ in den Krankenhäusern.
Die Mehrzahl der Krankenhäuser ist darauf weder personell noch organisatorisch vorbereitet. Dies wird besonders in der Umsetzung technischer und organisatorischer Maßnahmen zur Informationssicherheit und zum Cyberschutz deutlich.

1. Ab dem 1. Januar 2022 sind alle Krankenhäuser verpflichtet geeignete Maßnahmen zur Informationssicherheit und zum Cyberschutz nach dem „Stand der Technik“ umzusetzen.

2. Ergänzend gilt die Datenschutz-Grundverordnung (DSGVO) und insbesondere der Art. 32 zur „Sicherheit der Verarbeitung“ von Patientendaten in Krankenhäusern.

3. Die rechtlichen Rahmenbedingungen haben bei Nichteinhaltung der umfassenden Normen erhebliche negative Folgen. Sanktionen und Schadensersatzverpflichtungen können den Krankenhäusern entstehen.

4. Analysen (siehe Veröffentlichungen zur digitalen Reifegradmessung) machen deutlich, dass die Mehrzahl der Krankenhäuser und Kliniken nur unzureichend auf die zeitgemäßen Anforderungen vorbereitet sind. Die Gründe der Defizite: heterogene und veraltete IT-Infrastrukturen, fehlende Personalkapazitäten für Health-IT und fehlende IT-Standardisierung (z.B. Schnittstellen zwischen Medizintechnik und Patientendokumentation (ePA).

5. Das Krankenhauszukunftsgesetz (KHZG) definiert neue Parameter für die Digitalisierungsprozesse und schafft die Voraussetzungen für finanzielle Förderungen mit einem Gesamtvolumen von 4,3 Milliarden Euro. Voraussetzung für finanzielle Zuwendungen ist auch die nachgewiesene Investition von 15% des Gesamtvolumens für IT-Sicherheit.

6. Die Gefahren durch Cyberattacken und andere IT-Störfälle sind in den Zeiten der Pandemie deutlich angestiegen und Versicherer berichten von signifikant höheren Schadenssummen. Fachleute befürchten eine weitere Steigerung in der Zukunft, weil die kriminelle Energie der Schadensverursacher mit innovativen technologischen Instrumenten (z.B. künstliche Intelligenz) kombiniert werden.

7. In diesem Umfeld wird Versicherungsmanagement in der medizinischen Versorgung zu einem zentralen Baustein der Risikominimierung. „Hidden Cyber“ Strategien stellen Cyber-Versicherungen mit Haftpflicht- und BU-Policen in einen integralen Zusammenhang.

⑧ Wesentliche Bestandteile des Versicherungsmanagements für Heilberufe werden zukünftig sogenannte „Assistance Dienstleistungen“ für die Versicherten sein. Mit digitalen Coaching Systemen und benchmark-basiertem digitalen Monitoring können Schadensrisiken für Versicherte und Versicherer in der medizinischen Versorgung nachweislich reduziert werden.

⑨ Der „Faktor Mensch“ ist ursächlich für bis zu 80% der Schäden durch IT-Sicherheitsvorfälle verantwortlich. Dazu zeigen Untersuchungen (z.B. GDV), dass durchschnittlich bis zu 50% der Mitarbeitenden nicht oder nur unvollständig über IT-Risiken und notwendige technische und organisatorische Maßnahmen aufgeklärt sind.

⑩ Der Marburger Bund (MB) und der Bundesverband für Gesundheits-IT haben ein System zur Messung des digitalen Reifegrads für Krankenhäuser entwickelt. Die erste Untersuchung (200 teilnehmende Krankenhausärzte) haben einen Reifegrad von nur 48% ergeben. Die Befragten gaben an, dass professionelle Software-Anwendungen nur zu 26% verfügbar sind (Verfügbarkeit auf mobilen Endgeräten sogar nur 16%).

⑪ Der Paradigmenwechsel der Klinik-Organisation von analogen zu digitalen Prozessen macht neue und kombinierbare Organisationsinstrumente erforderlich. Das Prozessmanagement für Informationssicherheit (§ 75c SGB V), Datenschutz (DSGV/BDSG) und Qualitätsmanagement kann in einem digitalen System kombiniert werden und damit erhebliche Synergien realisieren (siehe z.B. das digitale MCSS Ökosystem im Gesundheitswesen).

Konzertiertes Prozessmanagement in Krankenhäusern

Cyberschutz + 4 Upgrade-Möglichkeiten in der rechtskonformen medizinischen Versorgung

Cybersicherheit	Datenschutz	Qualitätsmanagement	Patientensicherheit	Hygienemanagement
Umsetzung Richtlinie § 75c SGB V	**Rechtskonformität nach DSGVO und BDSG**	**Strukturqualität, Prozessqualität, Ergebnisqualität**	**Risikomanagement & Incident Reporting System**	**Digitale Hygieneplanung und -monitoring**
Leistungen	Leistungen	Leistungen	Leistungen	Leistungen
Informationssicherheit nach Art. 32 DSGVO und insbesondere nach dem Digitale-Versorgung-Gesetz (DVG). Das digitale **MCSS Ökosystem** kompatibel mit den Anforderungen des § 75c SGB V.	**MC-KLINIK** navigiert die Nutzer durch die umfangreichen Regeln der EU-DSGVO und des BDSG. Das Monitoring beinhaltet Jahresberichte und z.B. Datenschutzfolgeabschätzungen (DSFA)	QM-Systeme nach verschiedenen Standards wie ISO 9001, QEP, KTQ, JCI etc. werden durch das **MCSS Ökosystem** unterstützt. Die Verwaltung von bestehenden und neuen Dokumenten wie Prozessbeschreibungen, Verfahrensanweisungen und Checklisten ist universell.	Patientensicherheit ist primär abhängig vom „Faktor Mensch“. Wissenstests für die Mitarbeiter, digitale Erklärvideos, Webinare und wissensbasierte Datenbanken sind überall aus der Cloud abrufbar (über PC, Laptop, Tablet und Smart Phones.	Hygiene steht gerade in Zeiten der Pandemie auf der Prioritätenliste für Patientensicherheit. Über einen regelmäßigen Status-Check mit Benchmarking wird der Hygieneplan und der Medizinproduktebereich ständig überwacht.

Das Prozessmanagement im Krankenhaus bietet hohe Synergie- und Einsparpotentiale, indem das Cyberschutz-Management mit Datenschutz und QM inkl. Patientensicherheit kombiniert wird.

⑫ Cloudbasierte Organisationslösungen, getrennt vom Krankenhausnetzwerk, optimieren die Verfügbarkeit und können das Cyber-Risiko um bis zu 35% reduzieren und damit die Informationssicherheit signifikant erhöhen (Cloud-Computing-Systeme nach § 19 KHSFV Absatz 1 Satz 1 Nr. 7 KHSFV).

⑬ Standardisierung der Krankenhaus-IT werden das Sicherheitsmanagement deutlich optimieren. Verbindungen zwischen Medizintechnik und ePA durch HL7-, DICOM und GDT-Schnittstellen können aktuell noch bestehende Sicherheitslücken eliminieren.

⑭ Innovative Technologien wie Big Data Analysen, Machine Learning Konzepte bis hin zu KI-Anwendungen (künstliche Intelligenz) werden die Digitalisierung effektiv und im Sinne der Patienten gestalten können.

Die Sammlung medizinischer Daten für Forschungszwecke und zur Entwicklung sogenannter „Clinical Decision Support Systems (CDSS)“ wird die medizinische Versorgung revolutionieren können. IT-Sicherheit und Datenschutz ist dabei eine elementare Voraussetzung (siehe auch das „Digitale-Versorgung-Gesetz“ DVG).

Notizen

12 Die Autoren

Arno Zurstraßen

Arno Zurstraßen, M.A. ist als Fachanwalt für Medizinrecht und Sozialrecht, Mediator und Supervisor in Köln niedergelassen.
Mit seiner Erfahrung von über 25 Jahren berät er Ärzte, Zahnärzte, Praxisnetze und ärztliche Berufsverbände mit Schwerpunkt Rechtskonformität und Arzthaftungsrecht.
Die Umsetzung der umfangreichen Rechtsvorschriften für Ärzte mit innovativen Konzepten und professionelle Technologien ist ein besonderes Credo für ihn.

Arno Zurstraßen berät Ärzte auch bei Praxisabgaben oder -verschmelzungen. Dabei stützt er sich auf ein strukturiertes Projektmanagement, das er speziell nach Qualitätsmanagement-Kriterien im Team mit IT-Fachleuten entwickelt hat.

Er ist Autor vieler Publikationen in der Fachpresse und bekannter Referent auf ärztlichen Kongressen. Als Mitglied des Aufsichtsrats der **MCSS AG, Köln** gewährleistet er die rechtliche Kompatibilität innovativer digitaler Managementsysteme für die medizinische Versorgung.

Christian Schottmüller

Christian Schottmüller studierte Betriebswirtschaftslehre und Jura an der Universität in Köln.

Seit dem Jahr 2008 ist er in verschiedenen Leitungsfunktionen für die Versicherungswirtschaft tätig und arbeitete dort seit 2014 unter anderem daran mit, Standards für die IT-Sicherheit im präventiven Bereich durch Informationssicherheits-Managementsysteme zu entwickeln. In seiner Laufbahn vermittelte er sein profundes Branchenwissen in zahlreichen Schulungen und Vorträgen.

Im Jahr 2021 übernahm Christian Schottmüller die Verantwortung für die Umsetzung von Cyberschutz und Informationssicherheit im Gesundheitswesen und in der Sozialwirtschaft als Direktor der **MCSS AG, Köln**.

Rainer Waedlich

Rainer Waedlich ist Experte für Health-IT (E-Health), Cyberschutz und Qualitätsmanagement im Gesundheitsbereich. In seiner über 40-jährigen Berufslaufbahn im Gesundheitswesen hat er – national und international – softwarebasierte Produkte im Bereich der elektronischen Patientenakte (EPA), Qualitätssicherung und Qualitätsmanagement entwickelt und über 1.000 Arztpraxen und Kliniken weltweit in IT-Fragen beraten.

Im Bereich Big Data Analytics und Machine Learning hat Rainer Waedlich in internationalen Projektgruppen an Health-IT Anwendungen, u.a. mit IBM Watson Teams in den USA und Japan gearbeitet.

Als Aufsichtsratsvorsitzender deutscher und amerikanischer Health IT-Unternehmen war er 15 Jahre lang u.a. für die Rechtskonformität von wissensbasierten Projekten verantwortlich (Entwicklung von Algorithmen für Vorstufen von KI-Anwendungen, „Artificial Intelligence in Medicine“).

Sein Spezialgebiet, neben E-Health, sind Optimierungs-Strategien im organisatorischen und versorgungstechnischen Bereich, z.B. mit KAIZEN Konzepten (KAIZEN = das japanische Prinzip der ständigen Optimierung).
Aktuell ist er Aufsichtsratsvorsitzender der **MCSS AG, Köln** und im Unternehmen verantwortlich für Rechtskonformität von IT-Anwendungen.

13 Referenzen

- Digitale-Versorgung-Gesetz (DVG) § 75b SGB V
- Krankenhauszukunftsgesetz (KHZG)
- BSI Empfehlungen nach Anlage 6
  (Informatorische Quellen des BSI zu den Anforderungen der Richtlinie nach § 75c SGB V)
- EU-Datenschutzverordnung Art. 32 DSGVO
- BS3-Standard nach BSI
- § 8 BSI Gesetz
- Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus
  (DKG Veröffentlichung)
- VdS Standard RL 10000 Informationssicherheit (ISMS) und VdS 10010 (DS)
- Tillmann Dittrich / Jan Ippach: Aufsatz zu „IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich“
- Prof. Dr. Andreas Becker / Edgar Gärtner: „Der neue § 75c SGB V – Anforderungen an die Informationssicherheit in Krankenhäusern“, in: Das Krankenhaus 04/2021, 292 ff.

Anmerkung

Das im Text erwähnte digitale **MCSS-System** wurde vom Bundesministerium für Wirtschaft (BMWi) im Rahmen eines ZIM Forschungs- und Innovationsprojekts gefördert.

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

MCSS AG
MioCloud
Solution Systems

A Weinsbergstraße 190
50825 Köln
T 0221/47 44 77 44
F 0221/47 44 77 55
E info@mcss-ag.de
W mcss-ag.de