1 Krisenresilienz als Aufgabe und Herausforderung für Krankenhäuser und MVZ-Strukturen

Gerhard Dannecker, Tilmann Dittrich, Nadja Müller, Marcel Schaich

1.1 Einleitung

Bevor die bereits im Titel angedeuteten Krisenszenarien dargestellt und diesbezügliche Hilfestellungen gegeben werden, soll in die Thematik eingeführt und der Aufbau des Handbuchs erläutert werden, um den praktischen Umgang mit diesem Buch zu erleichtern. Das Werk nähert sich den Regelungen für Krankenhäuser und MVZ-Strukturen[1] zur Vorsorge vor und zum Umgang mit Krisenereignissen aus juristischer Perspektive de lege lata, geht aber auch auf bereits absehbare Rechtsentwicklungen de lege ferenda ein, um den sich bereits abzeichnenden neuen Anforderungen in diesem Bereich Rechnung zu tragen.

Das Business-Continuity-Management (BCM) stellt einen Schwerpunkt des Umgangs mit Krisen dar. Hierbei handelt es sich um einen Managementprozess, der darauf angelegt ist, die Funktionsfähigkeit einer Einrichtung bei störenden Ereignissen aufrechtzuerhalten. Es sticht durch seinen präventiven Charakter heraus. Gerade für die Gesundheitsversorgung stellt das BCM den Schlüssel dar, um den gesetzlichen Aufgaben auch in Störfällen nachkommen zu können und die Gesundheit der Bevölkerung zu sichern.

Die Besonderheit des BCM liegt darin, dass der Gesetzgeber, sei es auf EU-Ebene, auf Ebene des Bundes oder auch auf Ebene der Länder, bereits Regelungen getroffen hat, die verschiedene Aspekte des BCM betreffen. Während einige der Regelungen, wie etwa die Vorschriften zur Cybersicherheit von Kritischen Infrastrukturen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) (► Kap. 3.2.1), bereits in der Rechtsprechung behandelt und im Schrifttum intensiv diskutiert werden, werden andere Vorschriften, wie etwa die seit längerem bestehenden Regelungen zur Krankenhausalarm- und -einsatzplanung (KAEP) (► Kap. 3.5), unter rechtlichen Gesichtspunkten wenig erörtert. Die praktische Bedeutung auch solcher Vorschriften wird in Zukunft noch deutlich zunehmen. Bereits das BSIG hat in den vergangenen Jahren mehrere Überarbeitungen erlebt, welche die Verpflichtungen der Kritischen Infrastrukturen gesteigert haben. Durch die Anfang 2023 in Kraft getretene NIS-2-Richtlinie (► Kap. 3.2.1) wird es deutlich

1 Wenn im Buch nur der Begriff des Krankenhauses verwendet wird, sind hier regelmäßig auch die MVZ-Strukturen inbegriffen, sofern nicht gesondert auf die Unanwendbarkeit hingewiesen wird oder sich dies klar aus dem Kontext ergibt.

mehr betroffene Einrichtungen geben, für die der nationale Gesetzgeber Vorschriften erlassen muss (▶ Kap. 3.2.3, Abschnitt »Umsetzung der NIS-2-RL in Deutschland«). Der Pflichtenkanon wird durch die zeitgleich mit der NIS-2-Richtlinie verabschiedete Resilienz-RL noch einmal erweitert (▶ Kap. 3.4.1).

Bereits hieraus wird deutlich, dass das BCM längst ein Thema geworden ist, das sowohl die Führungsebene als auch die Rechts- wie auch die Compliance-Abteilung eines Krankenhauses bzw. eines MVZ-Trägers »auf dem Schirm« haben muss. Krisenresilienz ist weder alleinige Aufgabe der IT-Abteilung noch alleinige Aufgabe des Krisenmanagements. Krisenresilienz ist ein Führungsthema, das nicht vollständig delegiert werden kann und für das es spezifischer Fachkenntnisse bedarf.

Das Handbuch geht daher nach der Einführung im *zweiten Kapitel* (▶ Kap. 2) – »Rechtsgrundlagen des BCM und die Compliance« – dezidiert auf das Verhältnis zwischen Compliance-Management und BCM ein (▶ Kap. 2.5), um zu konkretisieren, welche Anforderungen an die Leitungsebene und welche an Compliance-Officer einer Einrichtung gestellt werden, wenn es um die Einhaltung der rechtlichen Vorgaben mit BCM-Bezug geht. Außerdem wird dargelegt, welche Compliance-Maßnahmen erforderlich sind, um auf Verstöße gegen gesetzliche Vorgaben oder interne Regelungen zu reagieren. Diese Maßnahmen betreffen sowohl interne Compliance-Verfahren als auch die Einbindung Dritter.

Anschließend folgt im *dritten Kapitel* (▶ Kap. 3) – »Spezielle Bereiche des BCM im Krankenhaus und in MVZ-Strukturen« – eine eingehende Erörterung der für die verschiedenen Krisenszenarien geltenden rechtlichen Regelungen sowie eine Darstellung der sich aus zukünftigen Gesetzen ergebenden Anforderungen (bspw. aus dem Kritis-Dachgesetz, ▶ Kap. 3.4), damit die aufwändige Krisenvorsorge bereits frühzeitig in Angriff genommen werden kann und nicht eine Anpassung in kleinen Schritten erfolgen muss. Den Schwerpunkt dieses Kapitels bilden die Vorschriften zur Cybersicherheit von Krankenhäusern und MVZ-Strukturen. Außerdem wird die Einbindung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dargestellt.

Im *vierten Kapitel* (▶ Kap. 4) wird ausgeführt, dass die von einem Cyberangriff betroffenen Einrichtungen verpflichtet sind, sich frühzeitig an die Ermittlungsbehörden zu wenden. Den Ermittlungsbehörden in Baden-Württemberg gelang so bspw. im Jahr 2023 in Zusammenarbeit mit US-amerikanischen Behörden ein wichtiger Schlag gegen die Hacking-Gruppierung »Hive«, die auch Gesundheitseinrichtungen attackiert hatte.[2] Auf diese Weise kann die Resilienz eines gesamten Systems gestärkt werden. Zudem wird dargelegt, welche Rolle die Strafverfolgungsbehörden bei Cyberangriffen spielen.

Ein ebenfalls wichtiger Akteur für Unternehmen im Bereich Cybersicherheit sind Versicherungen. Der Beitrag im *fünften Kapitel* (▶ Kap. 5) – »Versicherungslösungen für Krankenhäuser« – gibt daher einen Überblick, welche Erwartungen an den Dreiklang der in Betracht kommenden Versicherungslösungen – D&O-Versicherung, Cyberversicherung, Vertrauensschadensversicherung – gestellt werden kön-

2 https://www.swr.de/swraktuell/baden-wuerttemberg/cyber-angriffe-unternehmen-behoerden-pressekonferenz-us-justiz-100.html, sämtliche Online-Quellen wurden zuletzt am 15.07.2023 abgerufen.

nen, aber auch darüber, was die Versicherungsunternehmen von den Krankenhäusern erwarten.

Das *sechste Kapitel* (▶ Kap. 6) – »BCM in der Praxis« – stellt die zu ergreifenden Maßnahmen anhand gängiger BCM-Standards vor. In diesem Kapitel wird dargelegt, wie die rechtlichen Vorgaben von der Leitungsebene des Unternehmens und der Compliance umgesetzt werden können und welche Anforderungen sich hieraus für die Ebene der Abteilungsleitung ergeben.

Einen letzten Kurzüberblick über die einzelnen Schwerpunkte des Buchs liefert das abschließende *siebente Kapitel* (▶ Kap. 7), das die wesentlichen Aspekte zusammenfassend aufgreift und so dazu beitragen will, dass sich die Verantwortlichen in Krankenhäusern und MVZ-Strukturen immer wieder die elementaren Herausforderungen im Zusammenhang mit der Krisenresilienz vor Augen führen können.

1.2 Die Entwicklungen der Gefahrenbereiche

Krankenhäuser und MVZ-Strukturen nehmen als Bestandteil der Gesundheitsversorgung eine elementare Aufgabe für das Funktionieren des Gemeinwesens wahr. Sowohl die stationäre als auch die ambulante Versorgung sind für die Bevölkerung nicht hinwegzudenken. Daher müssen sie den ihnen zugewiesenen Aufgaben umfassend und in höchster Versorgungsqualität nachkommen. Allerdings ist diese *Kontinuität der Versorgung* seit jeher Gefahren ausgesetzt.

Zu den »Dauerbrennern« der Bedrohungsszenarien für die Versorgungsqualität durch Brandereignisse, Hygienemängel etc. sind in den letzten Jahren *neue Gefahrenbereiche* hinzugekommen, die in der Praxis immer wieder zu Störungen der Funktionsfähigkeit von Gesundheitseinrichtungen geführt haben. Insbesondere das Szenario der Cyberangriffe bedroht sowohl die öffentliche Verwaltung als auch sämtliche Wirtschaftssektoren in Deutschland. Doch im Gesundheitswesen sind solche Angriffe besonders heikel, da stets nicht nur wirtschaftliche Gefahren, sondern auch solche für Gesundheit und Leben der Patientinnen und Patienten sowie der Mitarbeitenden drohen. Dies macht es notwendig, dass *Krankenhäuser und MVZ-Strukturen eine Krisenresilienz aufbauen*, um für solche Gefährdungen gewappnet zu sein und ihren eigenen Ansprüchen, aber auch denen des Gesetzgebers und der Krankenkassen genügen zu können.

1.2.1 Schadensszenario Brandereignis

Eine solche Gefahr geht seit jeher von *Brandereignissen* aus. Denn bei Krankenhäusern (und teilweise auch bei MVZ) handelt es sich um große Gebäude und oft um Gebäudekomplexe, in denen eine Vielzahl von Gefahrenherde für Brände bestehen. Kein Krankenhaus kommt heute ohne umfangreiche technische Brandschutzanlagen aus. Insbesondere die zunehmende Digitalisierung im Gesundheitswesen hat

hier noch einmal zu einem deutlichen Gefahrenzuwachs geführt. Bereits kleine Brände in IT-Räumen können große Schäden für die Betriebskontinuität der Einrichtung bewirken. Brandschutz ist daher auch IT-Sicherheit. Außerdem sind in Krankenhäusern Gefahrstoffe gelagert (bspw. Sauerstoff), die für die medizinische Versorgung benötigt werden, zugleich aber auch besondere Risiken für Brände bergen. Erschwert wird die Überwachung dieses Gefahrenbereichs dadurch, dass eine Gesundheitseinrichtung, anders als etwa übliche Bürogebäude, im Brandfall nicht einfach und schnell geräumt werden kann. Es werden bettlägerige Patientinnen und Patienten versorgt, bei deren Evakuierung besondere Maßnahmen und Sicherungsvorkehrungen notwendig sind. Vergrößert wird dieser Aufwand dann, wenn die Patientinnen und Patienten für ihr Überleben oder die Aufrechterhaltung ihres Gesundheitszustands und Genesungsfortgangs auf intensivmedizinische Behandlungen angewiesen sind. Daher sind Brandschutzübungen für die Leitungspersonen sowie für die sonstigen Beschäftigten in Krankenhäusern üblich, allein aber nicht ausreichend (► Kap. 3.6).

1.2.2 Schadensrisiko Hygiene

Ebenfalls ein klassisches Feld betriebsbeeinträchtigender Risiken für Krankenhäuser und MVZ-Strukturen stellt der Bereich der *Hygiene* dar. Hygiene-Vorfälle, die zu Stationsschließungen geführt haben, haben in der Vergangenheit immer wieder für mediale Aufmerksamkeit und damit einhergehende Reputationsschäden für die betroffenen Einrichtungen gesorgt. Auf die Spitze getrieben wurde dieser Gefahrenbereich durch den Ausbruch der Corona-Pandemie im Frühjahr 2020 (► Kap. 1.2.6).

Fallbeispiele aus dem Risikobereich der Hygiene

Im Jahr 2017 wurde in einem Bonner Krankenhaus als Vorsichtsmaßnahme aufgrund von Krätze-Fällen eine komplette Station geschlossen. Anschließend wurde die Station in einem mehrstufigen Verfahren gereinigt und desinfiziert, während die erkrankten Patienten auf einer Isolierstation behandelt wurden.[3]

Während der Corona-Pandemie musste das Klinikum Bayreuth im Januar 2021 seine Häuser für einige Zeit schließen, da der Verdacht einer hochansteckenden Coronamutation bestand. Mehr als 3000 Mitarbeitende des Klinikums mussten sich in Quarantäne begeben und durften keine öffentlichen Verkehrsmittel mehr benutzen, um zur Arbeit zu kommen. Patienten wurden nur in absoluten Notfällen aufgenommen und nach zwei negativen Testergebnissen entlassen.[4]

3 https://www.welt.de/regionales/nrw/article169617591/Bonner-Krankenhaus-schliesst-ganze-Station-wegen-Kraetze.html.

4 https://www.aerzteblatt.de/nachrichten/120545/Klinikum-Bayreuth-Rund-3-000-Mitarbeiter-unter-Quarantaene.

1.2.3 Schadensszenario Cybervorfall

Unter den neuen Gefahrenbereichen sind zuvörderst die durch *Cyberangriffe und Cybervorfälle* drohenden Gefahren zu nennen. Denn Krankenhäuser und MVZ-Strukturen sind hochtechnologische Einrichtungen, die ohne informationstechnologische Systeme und Prozesse in einem vernetzten Raum nicht mehr funktionsfähig sind. Dies beginnt unmittelbar bei der medizinischen Versorgung, wenn bspw. telemetrische und telemedizinische Verfahren genutzt werden, und reicht über das Verwaltungs- und Abrechnungssystem bis in die Krankenhauslogistik und das Personalmanagement solcher Einrichtungen. Krankenhäuser und MVZ können hier aber nicht nur als einzelne Einheiten in den Blick genommen werden, sondern gehören vielfach Trägergesellschaften, bei denen es sich aus Kosten- und Verwaltungsgründen anbietet, gemeinsame Systeme einzuführen und zu nutzen. Daher wird nachfolgend nicht der Begriff des MVZ, sondern der MVZ-Strukturen verwendet, sei es, weil mehrere MVZ miteinander vernetzt sind oder gemischte Strukturen aus Krankenhäusern und MVZ vorhanden sind.

Fallbeispiel Rehaklinik Bad Säckingen 2022

Laut Medienberichten wurde eine Rehaklinik im südbadischen Bad Säckingen mit einer durchschnittlichen Belegung von bis zu 150 Rehabilitanden im Oktober 2022 Opfer eines Hackerangriffs.[5] Hiervon war im Ort auch ein MVZ mit verschiedenen Fachrichtungen und zwei Standorten betroffen (Ergänzung der Autoren: vermutlich aufgrund historisch gewachsener IT-Strukturen nach der Schließung des Krankenhauses). Nachdem die IT-Abteilung den Angriff auf die Systeme der Klinik bemerkt hatte, wurden sämtliche Server heruntergefahren und der Lösegeldforderung nicht Folge geleistet. Stattdessen begann die Klinik gemeinsam mit einem Dienstleister mit dem Aufbau eines neuen Netzwerks.

Einige Monate nach diesem Ereignis wurde der Schaden durch die Klinik auf eine sechsstellige Summe geschätzt.[6] Die Verwaltungsabläufe in der Klinik und im MVZ mussten vorübergehend analog durchgeführt werden. Im Nachgang verbesserte die Klinik ihre IT-Systeme und brachte diese auf ein höheres Schutzniveau. In diesem Zusammenhang wurden zumindest Überlegungen über regelmäßige Tests der IT-Systeme angestellt. Außerdem wurde die Entkoppelung der IT von Klinik und MVZ vorangetrieben.

Die Gefahren für die Cybersicherheit bedeuten unter *mehreren Gesichtspunkten eine Herausforderung.* Die Herausforderung wird bereits bei den Ursachen von Cybervorfällen ersichtlich. Vielfach wird der Begriff des Cyberangriffs herangezogen, weil Cyberkriminelle mit verschiedenen Angriffsmustern das Krankenhaus oder die MVZ-Struktur attackieren. Doch hier sind Cyberkriminelle vielfach auf die »Mit-

5 https://www.suedkurier.de/region/hochrhein/bad-saeckingen/cyberangriff-hacker-legen-bad-saeckinger-reha-klinik-lahm;art372588,11342157.

6 https://www.suedkurier.de/region/hochrhein/bad-saeckingen/so-schuetzen-sich-rehaklinik-und-mvz-nach-dem-massiven-hackerangriff;art372588,11430146.

hilfe« aus dem Krankenhaus angewiesen. So bedarf es bei *Phishing-Attacken* (► Kap. 3.1.2) regelmäßig der Mitwirkung von Beschäftigten, damit die Cyberkriminellen ihr Ziel erreichen können, indem Beschäftigte bspw. mit einer Schadsoftware infizierte E-Mail-Anhänge öffnen. Ein weiteres Risiko geht von Sicherheitslücken in den IT-Systemen aus, die Cyberkriminelle für ihre Angriffe ausnutzen können. Hier kann ein Fehlverhalten der Leitungsebene, der IT-Abteilung oder eines sonstigen Anwenders begünstigend sein. Die Cybersicherheit wird daher stets durch den *Risikofaktor Mensch* maßgeblich beeinflusst. Es bietet sich daher die Verwendung allgemeinerer Begriffe an, etwa des *Cybervorfalls* bzw. Cybersicherheitsvorfalls oder der Störung für die Cybersicherheit. Eine weitere Herausforderung ergibt sich aus *den Variationen möglicher Folgen* durch einen Cybervorfall. Dies liegt am aufgezeigten Einsatzgebiet von vernetzten Systemen im Krankenhaus und in MVZ-Strukturen. Durch einen Cybervorfall kann unmittelbar die Gesundheitsversorgung der Patientinnen und Patienten betroffen sein. Die Gesundheitsversorgung kann aber auch durch weitere Einschränkungen beeinflusst werden: Weil der Zugriff auf notwendige Daten nicht möglich ist, wenn die Kommunikation im Krankenhaus und mit Dritten nicht mehr funktioniert, der Nachschub an notwendigem Material nicht mehr gelingt oder die Planung von Operationen außer Kraft gesetzt ist und mithin planbare und elektive Eingriffe verschoben werden müssen. Zudem kann ein Abfluss von Daten über Patienten- und Mitarbeiter stattfinden, wodurch ein erheblicher Reputationsschaden neben weiteren wirtschaftlichen Folgen (► Kap. 3.2.5) droht.

1.2.4 Schadensszenario Lieferkette

Ein weiterer »moderner« Gefahrenbereich für Krankenhäuser und MVZ-Strukturen, der nicht auf eine einzige Gefahrenquelle reduziert werden kann, betrifft *die Gefährdung von Lieferketten*, die sich in unterschiedlichsten Auswirkungen zeigt. Als Beispiele der jüngeren Vergangenheit kann auf Lieferengpässe in der Corona-Pandemie oder infolge der Schiffshavarie im Suez-Kanal Ende März 2021 oder den im Februar 2022 ausgebrochenen Russland-Ukraine-Krieg verwiesen werden. Viele Gebrauchsgegenstände für Krankenhäuser werden nicht in Deutschland produziert, sondern im Ausland und haben einen langen Lieferweg. Zudem haben sich wirtschaftliche Vorgänge so entwickelt, dass keine große Rückfall-Mengen in Lagern vorgehalten werden, weshalb auch bei in Deutschland produzierten Produkten Lieferschwierigkeiten drohen können bzw. die inländischen Hersteller oft auf internationale Produkte angewiesen sind. In der Lieferkette (engl.: *Supply Chain*) bedarf es einer besonderen Zusammenarbeit zwischen den Geschäftspartnern, um kontinuitätsbeeinträchtigende Ereignisse frühzeitig zu erkennen und auf Ausweichpläne zurückgreifen zu können, damit nicht die Gesundheitsversorgung in Mitleidenschaft gezogen wird. Dies muss zwingend auch in den jeweiligen Vertragswerken berücksichtigt werden (► Kap. 6.3.3, Abschnitt »Dienstleister-/Lieferantenausfall«). Doch nicht nur bei medizinischen Produkten können Engpässe auftreten. So betraf der weltweite Chipmangel, ausgelöst durch die Corona-Pan-

demie, auch die Brandmeldeanlagen in Krankenhäusern.[7] Ebenso sind Lieferketten unter dem Blickwinkel der IT-Sicherheit bedroht. Sichtbar wurde dies etwa bei der »Log4Shell«-Schwachstelle in der weit verbreiteten Java-Bibliothek Log4, vor der das BSI Ende 2021 warnte.[8] Die in den Krankenhäusern und MVZ-Strukturen verwendeten Systeme und Prozesse setzen sich oft aus vielen Lösungen und Bestandteilen zusammen, die von unterschiedlichen Herstellern stammen. Eine Schwachstelle in einem solchen Bauteil kann zur Beeinträchtigung des verwendeten Systems oder Prozesses und damit zur Beeinträchtigung der Gesundheitsversorgung und der Verwaltung führen. Die Supply Chain betrifft daher gegenständliche, aber auch technische/digitale Bestandteile. Sie ist daher nicht nur aufgrund des Lieferkettensorgfaltspflichtengesetzes, das Krankenhäuser zu einem menschenrechts- und umweltbezogenen Handeln verpflichtet[9], sondern auch aus dem Blickwinkel der Krisenresilienz relevant. Hierfür hat sich der Begriff der *Supply Chain Resilience* durchgesetzt.[10] Letztlich führt kein Weg an einem ganzheitlichen Lieferketten-Management vorbei.

1.2.5 Schadensszenario Umweltkatastrophe

Dramatische Bilder zeigten sich im Sommer 2021 bei der Flutkatastrophe im Westen Deutschlands. Sie forderte eine Vielzahl an Todesopfern und führte zu Schäden und Beeinträchtigungen in vielen Regionen, deren Aufarbeitung noch mehrere Jahre dauern wird. Experten gehen davon aus, dass die Zahl solcher Naturereignisse im Zuge des *Klimawandels* zunehmen wird. Offenkundig betraf die Flutkatastrophe auch die Gesundheitsversorgung. Trotz der Offenkundigkeit lohnt ein genauerer Blick auf die Auswirkungen solcher Naturereignisse, um hieraus notwendige Maßnahmen für den Gesundheitsbereich ableiten zu können. So kann die Gesundheitseinrichtung selbst Schaden nehmen, etwa durch Flutereignisse, Erdbeben und sonstige Gefahren. Zudem kann plötzlich die Zahl der Patientinnen und Patienten ansteigen. Für solche Massenereignisse sind die Krankenhäuser per Gesetz verpflichtet, Notfallpläne vorzuhalten und Übungen durchzuführen. Dies fällt in den Bereich der *Krankenhausalarm- und -einsatzplanung (KAEP)* (▶ Kap. 3.5). Die Arbeit der Gesundheitseinrichtungen wird weiterhin dadurch erschwert, dass die Infrastruktur in der Gegend gestört wird. So musste in einem betroffenen Krankenhaus im Ahrtal nach der Räumung der Einrichtung zunächst die Strom- und Trinkwasserversorgung in Zusammenarbeit mit einer Hilfsorganisation wieder-

7 Vgl. den Bericht von Focus Online v. 09.02.2022, in dem ein Hersteller nur durch Umplanungen der Produktion die für die Inbetriebnahme eines Krankenhauses notwendigen Brandmelder und Notrufanlagen liefern konnte (der Bericht ist abrufbar unter: https://www.focus.de/finanzen/news/unternehmen-in-existenznot-durch-halbleitermangel-chip-engpass-unternehmen-schlachten-jetzt-schon-waschmaschinen-aus_id_46612530.html).

8 Die überarbeitete Pressemeldung des BSI v. 16.12.2021 ist abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html.

9 Dittrich/Etterer, KH-J 2022, 11 ff.; Dittrich/Lippert, MedR 2023, 638 (639); Wagner/Ruttloff/Schuler, GuP 2023, 41.

10 Köhler/Schlüchtermann, Klinik Management aktuell 2021, 57 ff.

hergestellt werden. Auch die Kommunikation wurde durch den Ausfall des Telefonnetzes erschwert.[11] Zudem waren die Zufahrtswege für Personal, Rettungsdienste, Lieferanten und andere Dienstleister eingeschränkt.

1.2.6 Szenario Pandemie

Die Corona-Pandemie führte im Dezember 2021 dazu, dass kaum einer Bürgerin oder einem Bürger der Begriff der *Kritischen Infrastruktur* unbekannt blieb. So wurde die Arbeitsbelastung für das Ärzte- und Pflegepersonal öffentlich diskutiert. Auch vereinzelte vorübergehende (Teil-)Schließungen von Einrichtungen wurden bereits bekannt:

Fallbeispiel Klinikschließung Bayreuth 2021

Das Klinikum Bayreuth gab, wie bereits erwähnt, im Januar 2021 die vorübergehende Schließung von Stationen bekannt.[12] Hintergrund war der Verdacht des Ausbruchs einer hochansteckenden Coronavirus-Variante. Rund 3000 Mitarbeitenden des Klinikums wurde untersagt, mit öffentlichen Verkehrsmitteln den Arbeitsweg anzutreten. Sie mussten sich in häusliche Quarantäne begeben. Eine Aufnahme von Notfallpatienten erfolgte nur in absoluten Ausnahmefällen, und Entlassungen bedurften zweier negativer Corona-Tests. Von Seiten des Klinikums beurteilte man die Lage als angespannt, aber unter Kontrolle. Als Krisenmaßnahme fanden u. a. Reihentestungen statt.

Eine solch flächendeckende Gefährdung, wie sie aufgrund der »Omikron-Variante« für Kritische Infrastrukturen kurzzeitig angenommen wurde, stellte jedoch eine Besonderheit dar.[13] Unabhängig davon waren im Zuge der Pandemie umfassende und herausfordernde Personalmanagement-Maßnahmen notwendig, um die Betriebsfähigkeit der Gesundheitseinrichtungen kontinuierlich zu gewährleisten (► Kap. 6.3.3, Abschnitt »Personalausfall«).

1.3 Die Verantwortung der Krankenhäuser

Nach § 27 Abs. 1 S. 1 SGB V haben Versicherte einen Anspruch auf Krankenbehandlung. Diese umfasst nach § 27 Abs. 1 S. 2 Nr. 5 SGB V auch die *Krankenhaus-*

11 Dittrich/Müller, KH-J 4/2021, 105 (106).
12 https://www.aerzteblatt.de/nachrichten/120545/Klinikum-Bayreuth-Rund-3-000-Mitarbeiter-unter-Quarantaene.
13 https://www.handelsblatt.com/unternehmen/mittelstand/familienunternehmer/corona pandemie-4-2-millionen-infizierte-wie-die-omikron-welle-aktuell-firmen-und-kliniken-lahmlegt/28232906.html.

behandlung. Die Leistungen aus der GKV unterstehen nach §§ 2 Abs. 1, Abs. 4; 12 Abs. 1 SGB V dem *Wirtschaftlichkeitsgebot* und müssen daher ausreichend, zweckmäßig und wirtschaftlich sein. Hinzu kommt das Qualitätsgebot: Nach § 2 Abs. 1 S. 3 SGB V i. V. m. § 135a Abs. 1 S. 2 SGB V müssen *Qualität und Wirksamkeit der Leistungen* dem allgemein anerkannten Stand der medizinischen Erkenntnisse entsprechen und den medizinischen Fortschritt berücksichtigen.

Aus dem Wirtschaftlichkeits- und Qualitätsgebot ergeben sich für Krankenhäuser vielfältige Rechtspflichten und Herausforderungen. Diese Gebote dienen der *Steuerung und Rationalisierung* der Leistungspflicht in der GKV. Hierbei geht es darum, Prozesse und Abläufe zu optimieren, die noch vorhandenen Mittel effizient einzusetzen und einer Verschwendung entgegenzuwirken. Notwendige und zweckmäßige Maßnahmen sind nicht zu rationalisieren, wohl aber darüber hinausgehende Maßnahmen, um so objektiv zu hohe Beitragszahlungen der Versicherten und einen damit einhergehenden unverhältnismäßigen Grundrechtseingriff zu verhindern und für alle Versicherten eine standardmäßige Grundversorgung zu sichern.[14] Das Wirtschaftlichkeits- und das Qualitätsgebot betreffen zum einen unmittelbar die eigentliche Behandlung, indem u. a. der Aspekt der fachlichen Qualität sowie der Grad des medizinischen Nutzens bei der Entscheidung über eine Behandlung zulasten der GKV zu beachten sind.[15] Zum anderen ergeben sich Anforderungen an den »Hintergrund« einer Behandlungsleistung. So fallen hohe Standards im Bereich der Hygiene sowie beim Einsatz von Medizinprodukten in den Bereich des Qualitätsgebots. Insbesondere aus der Pflicht, den medizinischen Fortschritt bei der Leistungserbringung zu berücksichtigen, folgt aber auch, dass beim Einsatz von IT-Systemen im Krankenhaus, deren Ausfall oder Beeinträchtigung aufgrund eines Cybervorfalls sich nachteilig auf den Behandlungserfolg und die Patientengesundheit auswirken können, ebenfalls zumindest die sich *aus § 8a BSIG und § 391 SGB V ergebenden Anforderungen an den Schutz der IT-Sicherheit in allen Krankenhäusern als Teilaspekt des Qualitätsgebots* umgesetzt werden.[16]

Der medizinische Standard spielt aber nicht nur beim Wirtschaftlichkeits- und Qualitätsgebot des Sozialrechts eine Rolle, sondern nimmt auch im zivilrechtlichen Arzthaftungsrecht eine herausragende Stellung ein. Denn die Behandlung hat nach § 630a Abs. 2 BGB nach dem zum Zeitpunkt der Behandlung bestehenden allgemein anerkannten fachlichen Standard zu erfolgen. Hierzu zählt, dass das eingesetzte Personal ausreichend qualifiziert ist sowie dass bei der Behandlung eingesetzte technische Geräte vor Beeinflussungen durch Dritte geschützt sind – bspw. ein System zur Überwachung von Patienten ausreichend vor Cyberangriffen geschützt und in ein krankenhausweites Informationssicherheits-Managementsystem (ISMS) aufgenommen ist. Gleiches gilt für den aufkommenden Einsatz von *Künstlicher Intelligenz* im Gesundheitswesen, wenn bspw. Systeme der Radiologie mit Künstlicher Intelligenz arbeiten (► Kap. 3.2.1).

In Krisensituationen wächst die Verantwortung der Krankenhäuser. Sie müssen dementsprechend auf solche Schadenslagen vorbereitet sein. So sind sie durch die

14 Nebendahl in: Spickhoff, SGB V, § 2 Rn 18; Scholz in: Becker/Kingreen, § 2 Rn. 16.
15 Barkow-von Creytz in: Spickhoff, SGB V, § 12 Rn. 4.
16 Dittrich, GuP 2021, 165.

Landeskrankenhausgesetze zur Erstellung und Einübung von Notfallplänen verpflichtet. Konkretisierende Vorgaben ergeben sich aus dem »Handbuch Krankenhausalarm- und -einsatzplanung KAEP« des BBK.[17]

Eine solche Verantwortung betrifft nicht nur Plankrankenhäuser nach dem SGB V, sondern auch Privatkliniken. Die Betreiber von Privatkrankenanstalten bedürfen einer Konzession der zuständigen Behörde nach § 30 Abs. 1 GewO. Eine erteilte Konzession kann auch wieder nach § 48 VwVfG zurückgenommen werden, wenn sich nachträglich herausstellt, dass ein Versagungsgrund i. S. d. § 30 Abs. 1 S. 2 GewO vorgelegen hat.[18] Als Versagungsgrund im Hinblick auf die Krisenfestigkeit von Privatkliniken kommt v. a. § 30 Abs. 1 S. 2 Nr. 1a GewO in Betracht, wenn Tatsachen vorliegen, welche die ausreichende medizinische oder pflegerische Versorgung der Patienten als nicht gewährleistet erscheinen lassen. Hierzu gehört auch, dass hygienische Standards und solche bei der medizinisch-technischen Ausstattung gewährleistet werden, also auch Ereignisse mit betriebsbeeinträchtigenden Auswirkungen aus diesen Bereichen oder für diese Bereiche vermieden werden.[19]

1.4 Die Einbindung in die Krankenhaus-Compliance

Im Verlauf des hier vorliegenden Handbuchs wird deutlich, dass insbesondere im Bereich der Cybersicherheit im Gesundheitswesen eine zunehmende Verrechtlichung stattfindet, welche die Krankenhäuser und MVZ-Strukturen vor immer höhere Herausforderungen stellt, um den rechtlichen Anforderungen gerecht zu werden und negative Rechtsfolgen zu vermeiden. Seit etwa einem Vierteljahrhundert wird der Verantwortung von Leitungspersonen für das eigene rechtskonforme Verhalten und das des Unternehmens im Bereich der *Compliance* große Aufmerksamkeit gewidmet.

Diese Entwicklung hat dazu beigetragen, dass mehrere Gesetzgebungsvorstöße zur Einführung eines Unternehmensstrafrechts, auch als *Verbandssanktionengesetz* bezeichnet, unternommen, aber bislang nicht umgesetzt wurden. Dieses Schicksal traf zuletzt den Entwurf für ein Gesetz zur Stärkung der Integrität in der Wirtschaft der großen Koalition im Jahr 2020.[20] Im Koalitionsvertrag der »Ampel-Koalition« aus dem Jahr 2021 sind ebenfalls Unternehmenssanktionen angesprochen.[21] Es zeichnet sich aber gegenwärtig keine Umsetzung dieses Gesetzesvorhabens ab.

17 Das Handbuch des BBK ist abrufbar unter: https://www.bbk.bund.de/DE/Themen/Gesundheitlicher-Bevoelkerungsschutz/Krankenhausalarmplanung/krankenhausalarmplanung_node.html.

18 Marcks in: Landmann/Rohmer, GewO, § 30 Rn. 26.

19 Marcks in: Landmann/Rohmer, GewO, § 30 Rn. 20a; vgl. hierzu den Gem. RdErl. d. Ministers für Arbeit, Gesundheit und Soziales und des Ministers für Wirtschaft, Mittelstand und Technologie des Landes NRW v. 03. 01. 1989 (MBl. NRW S. 68), Punkte 2.14 und 2.16.

20 BT-Drs. 19/23568.

21 Schneider/Albert, KH-J 1/2022, 9.