Ethik in der Medizin
https://doi.org/10.1007/s00481-025-00895-0

ORIGINALARBEIT

Cyberangriffe auf Kliniken: Patientengefährdung, rechtliche Pflichten und ethische Herausforderungen

Fabian M. Teichmann

Eingegangen: 22. Mai 2025 / Angenommen: 14. November 2025

Zusammenfassung Cyberangriffe auf Kliniken gefährden Versorgungskontinuität und Patientensicherheit unmittelbar. Der Beitrag verdichtet die empirische Lage, systematisiert Pflichten (BSIG/BSI-KritisV, § 75c SGB V, DSGVO) und analysiert Haftungsfragen einschließlich objektiver Sorgfaltspflichtverletzung, Pflichtwidrigkeitszusammenhang und objektiver Zurechnung. Aus Governance-Perspektive werden antizipierte Sachverständigenstandards (B3S/ISMS, „Stand der Technik“) als Konkretisierung des Sorgfaltsmaßstabs diskutiert. Die medizinethische Bewertung bündelt zentrale Dilemmata – insbesondere Lösegeldforderungen und Ressourcenkonflikte zwischen IT-Sicherheit und unmittelbarer Patientenversorgung – entlang der Vier-Prinzipien-Ethik und einer Verantwortungsethik. Abschließend folgen prägnante Handlungsempfehlungen für Klinikträger, Aufsicht und Ethikgremien. Kernthese: IT-Sicherheit ist Patientensicherheit; präventive Dokumentation und geübte Notfallverfahren sind rechtlich wie ethisch geboten.

Schlüsselwörter Cyberangriff · Krankenhaus · IT-Sicherheit · Patientenwohl

✉ RA Dr. iur. Dr. rer. pol. Fabian M. Teichmann, LL.M. (London), EMBA (Oxford)
London School of Economics and Political Science, London, United Kingdom
E-Mail: F.M.Teichmann@lse.ac.uk

Published online: 06 January 2026

Cyberattacks on hospitals: patient safety, legal obligations, and ethical challenges

Abstract
Background Cyberattacks on hospitals directly threaten continuity of care and patient safety. This article synthesizes the empirical evidence on cyber incidents in healthcare and maps core legal obligations, in particular under the German IT Security Act and the associated ordinance regarding critical infrastructure (BSIG/BSI-KritisV), § 75c of the Fifth Book of the German Social Code (SGB V), and the EU General Data Protection Regulation (GDPR).
Arguments The article examines liability with a focus on objective breach of duty, the causal nexus between inadequate cybersecurity and patient harm, and legal attribution. From a governance angle, anticipated expert standards (B3S/ISMS, "state of the art") are analyzed as instruments to operationalize and concretize the duty of care for hospital operators and management. The ethical analysis consolidates core dilemmas—especially ransom payments and resource allocation trade-offs between cybersecurity and immediate clinical care—using the frameworks of principlism and an ethics of responsibility.
Conclusion Cybersecurity is patient safety. Preventive documentation, risk-adequate technical and organizational safeguards, and rehearsed contingency procedures are not only legal requirements but also ethical imperatives. The article concludes with concise recommendations for hospital owners, supervisory bodies, and ethics boards on how to strengthen digital resilience without compromising the core mandate of patient care.

Keywords Cyberattack · Hospitals · Information technology security · Patient welfare

Einleitung

Krankenhäuser und Kliniken sind im digitalen Zeitalter zu hochgradig vernetzten Einrichtungen geworden, in denen Informationstechnologie essenziell für Diagnose, Behandlung und Verwaltung ist. Gleichzeitig rückt der Gesundheitssektor ins Visier von Cyberkriminellen: *Cyberangriffe auf Kliniken* – insbesondere in Form von Ransomware-Attacken, bei denen Daten verschlüsselt und Lösegeld gefordert wird – haben weltweit und in Deutschland in jüngster Zeit deutlich zugenommen. Die IT-gestützte Medizin erhöht zwar die Effizienz und Qualität der Versorgung, schafft aber auch neue Verwundbarkeiten. Ein erfolgreicher Hackerangriff kann nicht nur Daten kompromittieren, sondern ganze Versorgungsprozesse lahmlegen. Damit werden Cyberangriffe zu einem unmittelbaren Risiko für das Patientenwohl und werfen neuartige ethische und rechtliche Fragen auf.

Die ethisch-normative Relevanz des Themas ist offensichtlich: Wenn infolge eines IT-Ausfalls Operationen verschoben, Notaufnahmen geschlossen oder vertrauliche Patientendaten veröffentlicht werden, stehen zentrale Werte wie das Nicht-Schaden-Prinzip, die Fürsorge und die Vertraulichkeit medizinischer Informationen auf dem

Spiel. In diesem Beitrag wird daher eine interdisziplinäre Analyse unternommen, die technische, rechtliche und medizinethische Perspektiven systematisch verbindet. Zunächst wird die empirische Ausgangs- und Bedrohungslage skizziert, um das Ausmaß der Gefahr im Gesundheitswesen greifbar zu machen. Daran schließt sich eine Übersicht über den rechtlichen Rahmen an – von IT-Sicherheitsgesetzen bis zu Datenschutzvorgaben – sowie eine Diskussion von Verantwortlichkeits- und Haftungsfragen bei Cybervorfällen in Kliniken. Ein besonderes Schlaglicht wirft der Beitrag auf den Hackerangriff auf die Uniklinik Düsseldorf 2020 als Fallbeispiel, das die möglichen Konsequenzen eindrücklich vor Augen führt. Vor diesem Hintergrund werden dann zentrale normative Dilemmata analysiert, etwa ob die Zahlung von Lösegeld ethisch vertretbar sein kann oder wie Kliniken mit dem Spannungsfeld zwischen begrenzten Ressourcen für IT-Sicherheit und dem unmittelbaren Patientenbedarf umgehen sollen. Schließlich erfolgt eine medizinethische Bewertung unter Rückgriff auf anerkannte Theorierahmen (Prinzipienethik und Verantwortungsethik), um Orientierungen im Umgang mit diesen Herausforderungen zu bieten. Abschließend werden Handlungsempfehlungen formuliert, die Entscheidungsträgern auf verschiedenen Ebenen – von der Klinikleitung bis zur Gesetzgebung und Ethikkommissionen – Anhaltspunkte liefern, wie der Schutz vor Cyberangriffen verbessert werden kann, ohne den Versorgungsauftrag und das Patientenwohl zu vernachlässigen.

Empirische Bedrohungslage im Gesundheitswesen

Zunahme von Cyberangriffen

Die vergangenen Jahre haben einen deutlichen Anstieg von Cyberangriffen auf Einrichtungen des Gesundheitswesens verzeichnet, sowohl im deutschsprachigen Raum als auch international. Allein im Jahr 2022 waren drei Viertel der Gesundheitseinrichtungen in Deutschland Opfer von Cyberattacken (Dettling und Ekkernkamp 2024). Ransomware gilt dabei aktuell als die größte Bedrohungslage, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) feststellt. Immer häufiger werden Kliniken gezielt attackiert, da Angreifer wissen, wie kritisch die ständige Verfügbarkeit von IT-Systemen für die Patientenversorgung ist. Viele Krankenhäuser sind bereit, erhebliche Summen in ihre Digitalisierung zu investieren, was jedoch auch die Angriffsfläche vergrößert. Die COVID-19-Pandemie hat diesen Trend noch verstärkt, da in der Krise zahlreiche Abläufe digitalisiert wurden (Kell 2024). Das BSI spricht von einer Gefährdungslage, die *„so hoch wie noch nie“* ist (BSI 2024). Neben kriminellen Gruppen nutzen auch staatliche Akteure und Terrororganisationen Cyberangriffe als Mittel – teils im Rahmen hybrider Kriegsführung, wie Angriffe auf Gesundheitseinrichtungen in Konfliktgebieten zeigen (Dettling und Ekkernkamp 2024).

Auswirkungen auf die Patientenversorgung

Cyberangriffe auf Kliniken sind keine bloß virtuellen Ereignisse, sondern sie haben handfeste Auswirkungen auf den Klinikalltag und die Patientensicherheit. Frühere

Fälle zeigen, dass ein erfolgreicher Angriff eine Klinik nahezu vollständig lahmlegen kann. In einem der ersten bekannt gewordenen Fälle in Deutschland – dem Angriff auf das Lukaskrankenhaus Neuss 2016 – führte ein Trojanerbefall dazu, dass Laborbefunde nicht mehr übermittelt werden konnten und das gesamte IT-System zum Schutz der Patientendaten heruntergefahren werden musste; in der Folge *„ging […] lange gar nichts mehr“*, vom Zugriff auf radiologische Befunde bis zur Medikamentenverwaltung. Dieses Beispiel machte deutlich, dass digitale Infrastrukturen in Kliniken verwundbar sind und ihr Ausfall die Versorgung akut beeinträchtigt (Kell 2024; Dose 2019).

Neuere Daten bestätigen, dass Cybervorfälle häufig direkte Einschnitte in die Versorgung bedeuten

Beim großen *WannaCry*-Angriff im Mai 2017, der den britischen National Health Service (NHS) traf, wurden innerhalb weniger Tage tausende Termine und Operationen abgesagt; in fünf Regionen konnten Notaufnahmen zeitweise keine Patienten aufnehmen, so dass Rettungswagen weitere Entfernungen zurücklegen mussten (National Audit Office 2025; Müller et al. 2024; Briegleb 2017). Ähnliches geschah 2021 in Irland, als ein Ransomware-Angriff das IT-System des nationalen Gesundheitsdienstes (HSE) wochenlang beeinträchtigte, was zu landesweiten Störungen führte (z. B. mussten Laborbefunde wieder manuell erhoben und Termine abgesagt werden). Diese Beispiele verdeutlichen, dass Cyberangriffe im Gesundheitswesen nicht nur ein Datenproblem sind, sondern *Leib und Leben* betreffen können (Dittrich und Dann 2025).

Konkrete Gefahrenfälle und erste Todesopfer?

Besonders alarmierend sind Fälle, in denen ein Cyberangriff in einen potenziellen Patientenschaden bis hin zum Todesfall mündet. Lange Zeit wurde die Möglichkeit direkter tödlicher Folgen eher theoretisch diskutiert. Doch 2020 ereignete sich in Deutschland der mutmaßlich erste derartige Vorfall: Der *Cyberangriff auf die Universitätsklinik Düsseldorf* im September 2020 zwang die Klinik, ihre Notaufnahme abzumelden (Pfenninger et al. 2023). Eine Notfallpatientin – eine 78-jährige Frau mit einem lebensbedrohlichen Aorta-Aneurysma – konnte nicht wie vorgesehen in Düsseldorf aufgenommen werden; der Rettungswagen musste in ein weiter entferntes Klinikum (Wuppertal) ausweichen, was zu einer Verzögerung der Behandlung um etwa eine Stunde führte. Die Patientin verstarb kurz darauf (William 2020; Pfenninger et al. 2023). Dieser tragische Fall erregte internationales Aufsehen, da zum ersten Mal ein direkter Zusammenhang zwischen einem Hackerangriff und einem Todesfall in Betracht gezogen wurde. Die Staatsanwaltschaft Düsseldorf leitete daraufhin Ermittlungen wegen fahrlässiger Tötung gegen Unbekannt ein. Auch wenn das Verfahren letztlich eingestellt wurde, da der kausale Zusammenhang nicht mit der nötigen Sicherheit nachzuweisen war, hat der Fall ein deutliches Warnsignal gesendet: Cyberangriffe auf kritische Klinik-IT sind *potentiell lebensgefährlich*. Dies unterstreichen die Dringlichkeit, Cyberangriffe als Problem der Patientensicherheit ernst zu nehmen (Dittrich und Dann 2025).

Steigende Schäden und Meldefälle

Neben Risiken für Patienten führen Cyberangriffe auch zu erheblichen finanziellen und organisatorischen Schäden für die Einrichtungen. Laut BSI-Lagebericht 2022 liegt der Gesundheitssektor bei den Meldungen von IT-Störfällen unter den kritischen Infrastrukturen an zweiter Stelle (BSI 2022) – ein Hinweis darauf, dass Kliniken sehr häufig betroffen sind. In den letzten Jahren mussten mehrere deutsche Krankenhäuser nach Attacken den Katastrophenfall ausrufen (eine Maßnahme, die sonst eher bei Naturkatastrophen oder Großschadenslagen zum Einsatz kommt). Beispielhaft sei die Stadtverwaltung Potsdam genannt, bei der Ende 2022 ein Hackerangriff das städtische Klinikum Ernst von Bergmann traf und wochenlang vom Internet trennte (Potsdam 2023). Im Oktober 2023 wurde das Universitätsklinikum Frankfurt durch einen Angriff gezwungen, seine gesamte IT-Infrastruktur neu aufzusetzen (Kma online 2024); dank Notfallplänen konnte dort Schlimmeres abgewendet werden. Dennoch zeigen solche Vorfälle, dass neben dem unmittelbaren Versorgungsgeschehen auch Vertrauen und Reputation der Einrichtungen leiden: Patienten und Bevölkerung verlieren das Vertrauen, wenn Kliniken wochenlang digital handlungsunfähig sind (Dettling und Ekkernkamp 2024).

Rechtliche Rahmenbedingungen und Pflichten zur IT-Sicherheit

Angesichts der skizzierten Bedrohungslage stellt sich die Frage, welche rechtlichen Pflichten Krankenhäuser haben, um Cyberangriffe abzuwehren oder deren Folgen zu minimieren. In den letzten Jahren wurden in Deutschland auf verschiedenen Ebenen gesetzliche Grundlagen geschaffen oder verschärft, die IT-Sicherheit im Gesundheitswesen betreffen. Wichtige Komponenten des rechtlichen Rahmens sind:

BSI-Gesetz und KRITIS-Verordnung

Größere Krankenhäuser gelten in Deutschland als *Kritische Infrastrukturen* (KRITIS) im Sektor Gesundheit. Konkret definiert die KRITIS-Verordnung (BSI-KritisV)[1] Schwellenwerte – aktuell etwa 30.000 vollstationäre Fälle pro Jahr – ab denen ein Krankenhaus als KRITIS-Betreiber eingestuft wird. Rund 5–10 % der Kliniken erfüllen diese Voraussetzung. Für sie gilt § 8a des *BSI-Gesetzes (BSIG)*: Sie sind verpflichtet, *„angemessene organisatorische und technische Vorkehrungen"* zur Vermeidung von IT-Sicherheitsvorfällen zu treffen, und diese Maßnahmen alle zwei Jahre nach dem Stand der Technik zu überprüfen (Carmasec o.J.). Zudem müssen *schwerwiegende IT-Störungen* unverzüglich an die Behörde (BSI) gemeldet werden. Die Einhaltung dieser Vorgaben wird vom BSI überwacht. Durch das IT-Sicherheitsgesetz 2.0 (2021) wurden die Befugnisse und Sicherheitsanforderungen noch erweitert, z. B. können bei Verstößen Bußgelder verhängt werden. Die KRITIS-Einstufung großer Kliniken hat dazu geführt, dass in vielen Krankenhäusern

[1] BSI-KritisV vom 22. April 2016. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz.

Informationssicherheits-Managementsysteme (ISMS) eingeführt und branchenspezifische Sicherheitsstandards (B3S Medizin) erarbeitet wurden, um einheitliche Schutzmaßnahmen zu etablieren (BSI 2020).

§ 75c SGB V – IT-Sicherheit in Krankenhäusern

Seit dem 1. Januar 2022 sind *alle* Krankenhäuser – also auch solche, die unterhalb der KRITIS-Schwelle liegen – gesetzlich verpflichtet, angemessene IT-Sicherheitsvorkehrungen zu treffen. Diese Regelung wurde durch das Patientendaten-Schutz-Gesetz (PDSG) 2020 neu im Sozialgesetzbuch V verankert. § 75c SGB V verlangt, Sicherheitsmaßnahmen *„nach dem Stand der Technik"* umzusetzen, um Störungen der IT-Systeme vorzubeugen und personenbezogene (insbesondere Gesundheits-)Daten zu schützen (Becker und Kingreen 2024; Hänlein und Schuler 2022). Zudem müssen die Systeme regelmäßig – mindestens alle zwei Jahre – an den aktuellen Stand der Technik angepasst werden. Bemerkenswert ist, dass der Gesetzgeber den Krankenhäusern explizit empfiehlt, sich an den Anforderungen des BSI für Kritische Infrastrukturen (§ 8a BSIG) zu orientieren (Carmasec o.J.). Damit werden praktisch KRITIS-Standards für alle Kliniken zum Maßstab erklärt. Mit § 75c SGB V existiert somit eine gesetzliche IT-Sicherheitsverpflichtung für das gesamte Gesundheitswesen, welche die zuvor bestehende Lücke (denn zuvor galten für kleinere Häuser keine speziellen IT-Sicherheitsgesetze) schließt (Becker und Kingreen 2024; Hänlein und Schuler 2022). In der Praxis bedeutet dies z. B., dass nun jedes Krankenhaus ein Basissicherheitskonzept implementieren, Notfallpläne vorhalten und regelmäßig Schwachstellenprüfungen durchführen muss. Die Deutsche Krankenhausgesellschaft hat in Zusammenarbeit mit dem BSI branchenspezifische Sicherheitsstandards (B3S) veröffentlicht, die Krankenhäusern als Orientierung dienen, um die gesetzlichen Vorgaben zu erfüllen (Dittrich und Dann 2025).

Datenschutzrecht (DSGVO und BDSG)

Patientendaten gehören zu den sensibelsten personenbezogenen Daten und genießen in Europa einen hohen rechtlichen Schutz. Die Datenschutz-Grundverordnung (DSGVO) der EU verpflichtet Krankenhäuser als Datenverarbeiter, technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit personenbezogener Daten zu gewährleisten (Art. 32 DSGVO) (Kühling und Buchner 2024; Ehmann und Selmayr 2024; Gola und Heckmann 2022). Ein Cyberangriff, der zu einer Datenpanne führt – etwa die unbefugte Offenlegung oder der Verlust von Patientendaten – kann somit neben Versorgungsproblemen auch *datenschutzrechtliche Konsequenzen* haben. Krankenhäuser müssen solche Verstöße innerhalb von 72 h an die Aufsichtsbehörde melden (Art. 33 DSGVO) und betroffene Personen informieren, sofern ein hohes Risiko für ihre Rechte besteht (Art. 34 DSGVO) (Kühling und Buchner 2024; Ehmann und Selmayr 2024; Gola und Heckmann 2022). Hohe Bußgelder drohen, wenn ein Krankenhaus nachlässig im Schutz der Daten war. Die DSGVO sieht Strafen von bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes vor – je nachdem, was höher ist (Strassmann 2025; Kühling und Buchner

2024; Ehmann und Selmayr 2024; Gola und Heckmann 2022). Tatsächlich wurden bereits einige Kliniken und Gesundheitsanbieter in Europa zu empfindlichen Geldstrafen verurteilt. Ein bekanntes Beispiel ist das Haga-Krankenhaus in Den Haag, das 2019 eine Strafe von 460.000 € zahlen musste, weil Mitarbeiter unbefugt auf die elektronische Patientenakte einer prominenten Patientin zugriffen und das Haus keine ausreichenden Zugriffskontrollen etabliert hatte. Auch in Deutschland gab es Bußgelder, z. B. 105.000 € gegen das Universitätsklinikum Mainz im Jahr 2020, nachdem durch organisatorische Mängel falsche Patientendaten verschickt wurden. Diese Fälle verdeutlichen, dass Kliniken bei unzureichender Datensicherheit neben dem Vertrauensverlust auch juristische Folgen in Form von Datenschutzstrafen und Schadensersatzforderungen (gemäß Art. 82 DSGVO) zu gewärtigen haben (Kühling und Buchner 2024; Ehmann und Selmayr 2024; Gola und Heckmann 2022).

Bei patientenbezogenen Schäden infolge IT-Ausfällen kommen fahrlässige Körperverletzungs-/Tötungsdelikte in Betracht. Maßgeblich ist die objektive Sorgfaltspflichtverletzung ex ante gegenüber vorhersehbaren Risiken (z. B. fehlende Segmentierung, veraltete Systeme, unterlassenes Patch-/Backup-/Monitoring, unzureichende Fallback-Prozesse), die subjektive Vorwerfbarkeit, der Pflichtwidrigkeitszusammenhang sowie die objektive Zurechnung (Schaffung/Erhöhung eines rechtlich missbilligten Risikos, das sich im Erfolg realisiert). In arbeitsteilig organisierten Kliniken bestehen Organisations- und Überwachungspflichten auf Leitungsebene; B3S/ISMS/„Stand der Technik“ konkretisieren den Maßstab. Drittverursachung durch Täterangriffe entlastet nicht, wenn Auswahl-, Überwachungs- oder Reaktionspflichten verletzt wurden; rechtmäßiges Alternativverhalten ist gesondert zu würdigen. Konsequenz: Kliniken müssen präventiv dokumentieren, dass risikoadäquate Schutz- und Notfallmaßnahmen eingerichtet, Warnungen/Updates zeitnah umgesetzt und Abwägungen nachvollziehbar getroffen wurden; andernfalls droht straf- und zivilrechtlich Organisationsverschulden.

Weitere relevante Vorschriften

Neben den genannten Kernregelungen gibt es weitere Rechtsnormen, die im Kontext der IT-Sicherheit im Gesundheitswesen eine Rolle spielen. So verpflichtet § 75a SGB V die Leistungserbringer zur Interoperabilität und IT-Ausstattung nach Stand der Technik – was zwar primär die Funktionalität betrifft, aber implizit auch Sicherheitsaspekte streift (Becker und Kingreen 2024; Hänlein und Schuler 2022). Das *Krankenhauszukunftsgesetz (KHZG)* von 2020 stellte Fördermittel in Milliardenhöhe bereit, um die digitale Infrastruktur und IT-Sicherheit der Krankenhäuser zu verbessern. Allerdings ist das KHZG befristet und primär finanzierungs- und projektorientiert; es soll jedoch dazu beitragen, die gesetzlich geforderten Sicherheitsstandards praktisch umzusetzen. Schließlich sind ärztliche Schweigepflicht und Berufsgesetze zu nennen: Ein Verstoß gegen die Schweigepflicht (§ 203 StGB) kann auch durch mangelhaften technischen Datenschutz erfolgen (von Heintschel-Heinegg und Kudlich 2025; Lackner et al. 2025) – z. B. wenn unverschlüsselte Patientendaten abgegriffen werden. Somit besteht auch strafrechtlich ein indirekter Schutz der Vertraulichkeit.

Haftungsfragen und Governance in der IT-Sicherheit

Die Existenz rechtlicher Verpflichtungen bedeutet in der Praxis, dass bei Cybervorfällen in Kliniken die Frage nach der Verantwortung und Haftung gestellt wird. Unterschiedliche Akteure – von den Cyberkriminellen über die Krankenhausleitungen bis hin zu staatlichen Stellen – stehen dabei im Fokus. Im Folgenden werden die wichtigsten Aspekte von Haftung und Governance skizziert.

Strafrechtliche Verantwortung

Unstrittig ist, dass die *Täter* eines Cyberangriffs – also die Hacker – sich wegen verschiedenster Delikte strafbar machen (z. B. Computersabotage, Erpressung, ggf. Körperverletzung) (Peters 2022). Neu und juristisch komplex ist allerdings die Frage, ob auch *Verantwortliche auf Seiten des Krankenhauses* strafrechtlich zur Rechenschaft gezogen werden können, falls Patienten durch einen Angriff zu Schaden kommen. Im Düsseldorfer Fall 2020 wurde dieses Szenario real: Die Ermittlungen wegen des Todes der Patientin richteten sich zunächst gegen die unbekannten Hacker, wurden aber auch auf ein mögliches Mitverschulden der Klinik ausgedehnt (William 2020; Pfenninger et al. 2023). Zwar konnte hier kein konkreter Klinikmitarbeiter haftbar gemacht werden, doch der Vorgang illustriert ein Prinzip: Wenn ein Patientenschaden eintritt, rückt die Frage ins Zentrum, ob die Klinikleitung ihrer Sorgfaltspflicht nachgekommen ist. Fahrlässigkeitsdelikte wie fahrlässige Tötung oder Körperverletzung könnten im Raum stehen, wenn grobe Versäumnisse in der IT-Sicherheit festgestellt würden, die kausal zum Schaden beigetragen haben (Nadeborn und Dittrich 2022; Dittrich und Dann 2025). Ein vorsätzliches Handeln der Krankenhausführung wird man zwar kaum je unterstellen können – kein Entscheider möchte absichtlich die Sicherheit vernachlässigen –, aber Strafrecht kennt auch fahrlässiges Unterlassen (Rengier 2025). Entscheidend wäre, welcher *Sorgfaltsmaßstab* gilt: Hier kämen die oben genannten Standards (BSIG, § 75c SGB V, anerkannte B3S-Richtlinien) als objektiver Maßstab ins Spiel. Wenn z. B. ein Krankenhaus kritische Sicherheitsupdates monatelang verschleppt oder keine Notfallpläne vorhält und es deshalb zu vermeidbaren Schäden kommt, könnte man von verletzter Verkehrssicherungspflicht sprechen (Rengier 2025; OLG Celle vom 7. September 2023 – 2 Ws 244/23). Noch ist in Deutschland kein Klinikmanager strafrechtlich wegen eines Cybervorfalls verurteilt worden, doch Experten halten es für *„nur eine Frage der Zeit“*, bis ein solcher Fall eintritt. Strafrechtlich würde dann geprüft, ob ein *individueller* Vorwurf gemacht werden kann – etwa ob ein IT-Leiter oder Geschäftsführer fahrlässig gehandelt hat, indem er bekannte Risiken ignorierte. Die normative Botschaft ist jedenfalls klar: Krankenhausleitungen müssen Cybersicherheit als Teil ihrer Verantwortung für Leib und Leben der Patienten verstehen (Dittrich und Dann 2025).

Zivilrechtliche Haftung

Unabhängig vom Strafrecht stellt sich die zivilrechtliche Haftung. Sollte ein Patient aufgrund eines Cyberangriffs zu Schaden kommen (etwa Komplikationen durch

verzögerte Behandlung), könnte er oder seine Angehörigen Schadensersatz vom Krankenhaus fordern (Nadeborn und Dittrich 2022; Dittrich und Dann 2025). Juristisch würde man prüfen, ob das Krankenhaus seine vertraglichen oder deliktischen Pflichten verletzt hat. Im Behandlungsvertrag schuldet die Klinik grundsätzlich eine nach aktuellen Standards sichere Organisation. Hier kommt der Begriff der *Organisationshaftung* ins Spiel: Kliniken haften für Organisationsverschulden, wenn sie nicht die erforderlichen organisatorischen Vorkehrungen treffen, um Schäden zu vermeiden (BGH vom 18 Juni 1985 – VI ZR 234/83). Traditionell denkt man dabei an Hygienemängel oder mangelhafte Notfallroutinen; mittlerweile zählen aber adäquate IT-Sicherheitsmaßnahmen ebenfalls zur Organisation. Wenn z. B. ein fehlendes Backup oder unzureichende Netzwerksegmentierung dazu führt, dass Patientendaten verloren gehen oder Intensivgeräte ausfallen, könnten Gerichte dies als Pflichtverletzung werten. Ein weiteres zivilrechtliches Risiko ergibt sich aus dem Datenschutz: Artikel 82 DSGVO gewährt Betroffenen ein Recht auf Schadenersatz bei Datenschutzverstößen. Interessanterweise hat der Europäische Gerichtshof klargestellt, dass ein Unternehmen sich nicht allein dadurch exkulpieren kann, dass es Opfer eines Hackerangriffs wurde – es bleibt verantwortlich, *sofern* nicht nachgewiesen wird, dass keinerlei Pflichtverletzung seinerseits vorlag (Kühling und Buchner 2024; Ehmann und Selmayr 2024; Gola und Heckmann 2022). Übersetzt heißt das: Wenn eine Klinik gehackt wird und dabei Patientendaten abfließen, trägt sie die Beweislast zu zeigen, dass sie alle angemessenen Schutzvorkehrungen getroffen hatte. Gelingt ihr das nicht, haftet sie für immaterielle Schäden der Patienten (z. B. für den Vertrauensverlust oder die verletzte Privatsphäre). Dieses Haftungsrisiko ist ein starker Anreiz, präventiv zu handeln (Kempermann und Rosenfeld 2023).

Governance und organisatorische Verantwortung

Die genannten rechtlichen Anforderungen werfen in der Praxis Governance-Probleme auf. Viele Krankenhäuser standen bis vor wenigen Jahren vor der Herausforderung, dass IT-Sicherheit nicht als Teil der Kernaufgaben angesehen wurde. Die Prioritäten lagen im klinischen Betrieb, Investitionen flossen eher in medizinische Geräte oder Gebäude als in „unsichtbare“ Infrastruktur. Entsprechend waren IT-Abteilungen oft knapp bemessen und den Geschäftsleitungen untergeordnet. Dies ändert sich nun: Regulatorische Vorgaben zwingen Kliniken, formelle Verantwortlichkeiten festzulegen, z. B. einen Informationssicherheitsbeauftragten zu benennen und IT-Risiken regelmäßig auf Leitungsebene zu erörtern. Doch es bleibt die Frage der kulturellen Verankerung. *IT-Sicherheit ist Chefsache* – dieses Motto muss gelebt werden, um wirksam zu sein. Wenn etwa die Klinikleitung Warnungen der IT ignoriert oder notwendige Ausgaben ständig herunterkürzt, besteht ein Governance-Versagen. Ein Beispiel ist der im Düsseldorfer Fall verwendete Angriffspunkt: eine seit langem bekannte Schwachstelle in einer VPN-Software (Citrix), für die es einen Patch gab (BSI 2020). Wird eine solche Schwachstelle nicht zeitnah geschlossen, stellt sich im Nachhinein die Frage, ob hier auf Leitungsebene Risikoabwägungen versäumt wurden. Gute Governance würde verlangen, dass Sicherheitsupdates höchste Priorität haben, selbst wenn dies kurzfristig Betriebsstörungen (z. B. durch Neustarts) bedeutet.

Ein weiteres Problemfeld ist die Zusammenarbeit mit IT-Dienstleistern. Viele Kliniken lagern Teile ihrer IT aus oder nutzen Standardsoftware von Drittanbietern (Grotelueschen 2024). Im Angriffsfalle ist jedoch die Klinik gegenüber Patienten verantwortlich – sie kann die Verantwortung nicht einfach auf den Dienstleister abwälzen. Governance bedeutet hier, für klare Verträge (inkl. Sicherheitsanforderungen, Reaktionszeiten etc.) zu sorgen und die Dienstleisterauswahl sorgfältig zu treffen. Zudem müssen regelmäßige Audits und Notfallübungen durchgeführt werden, idealerweise auch gemeinsam mit externen Partnern.

Haftpflicht- und Versicherungsaspekte

Ein praktischer Aspekt der Governance ist schließlich, wie man das finanzielle Risiko managt. Cyberangriffe können Millionenschäden verursachen (z. B. Wiederherstellungssysteme, Ausfallkosten, Schadenersatz). Hier kommen *Cyber-Versicherungen* ins Spiel, die allerdings in jüngster Zeit teurer und restriktiver geworden sind. Versicherer verlangen meist den Nachweis bestimmter Sicherheitsmaßnahmen, bevor sie Risiken zeichnen – dies kann indirekt den Kliniken helfen, ihren Sicherheitsstatus kritisch zu prüfen. Jedoch ersetzen Versicherungen nicht die persönliche Verantwortung der Entscheidungsträger: Sollte es zu einem Patientenschaden kommen, steht – wie oben beschrieben – auch ihre persönliche Haftung im Raum (bei grober Fahrlässigkeit hilft keine D&O-Versicherung). Daher lautet eine wichtige Governance-Empfehlung: präventive Dokumentation. Entscheidende Weichenstellungen im IT-Sicherheitsmanagement sollten transparent begründet und dokumentiert sein (Dittrich und Dann 2025). So kann im Ernstfall gezeigt werden, dass nach bestem Wissen gehandelt wurde (z. B. Risikoanalysen durchgeführt, Prioritäten abgewogen). Eine lückenlose Dokumentation kann Haftungsrisiken senken, weil sie Fahrlässigkeitsvorwürfen entgegenwirkt.

Ressourcenkonflikt: IT-Sicherheit vs. unmittelbare Patientenversorgung

Neben dem akuten Erpressungsdilemma gibt es ein ständiges Allokations- und Prioritätsdilemma im Klinikalltag: *Wie viel soll in IT-Sicherheit investiert werden im Vergleich zu unmittelbaren Mitteln für die Patientenversorgung?* Krankenhäuser verfügen über begrenzte Budgets und Personalressourcen. Jeder Euro und jede Stunde, die in Cybersecurity fließen, steht nicht direkt für Pflegepersonal, Medizinprodukte oder Therapieangebote zur Verfügung. Dieses Spannungsfeld führt zu Verteilungskonflikten und teils widerstreitenden Interessen innerhalb der Organisation.

Status quo der Investitionen

Traditionell haben Krankenhäuser deutlich weniger in IT und Sicherheit investiert als andere kritische Branchen (z. B. Banken oder Energie). Empfohlen wird, etwa 5–7 % des IT-Budgets für Security aufzuwenden, tatsächlich lag dieser Anteil in vielen Kliniken aber lange bei unter 1 % (Lorenz et al. 2022; Claroty 2023). Konkret bedeutet dies: Von 100 € Gesamtbudget flossen nur < 1 € in die IT-Si-

cherheit. Diese Unterfinanzierung erklärt teilweise, warum die Angriffsflächen so groß sind (unzureichend gewartete Systeme, veraltete Hardware, zu wenig Security-Experten). Gleichzeitig wird argumentiert: Krankenhäuser sind ohnehin chronisch unterfinanziert, überall fehlt es an Geld – wenn wir jetzt Millionen in Firewalls und hochverfügbare Rechenzentren stecken, fehlen diese Mittel womöglich an anderer Stelle, z. B. für zusätzliche Intensivbetten oder moderne Operationstechnik. Dieser Konflikt ist real, denn gerade in öffentlichen Häusern herrscht ein Spardruck, der oft bei „verwaltenden" Bereichen (wozu IT oft gezählt wird) ansetzt (PwC 2023; DKG 2025; Oswald und Goedereis 2019).

Qualität vs. Sicherheit

Ein weiterer Aspekt ist der Zielkonflikt zwischen maximaler medizinischer Leistungsfähigkeit und Sicherheit. Beispielsweise könnten strenge Sicherheitsmaßnahmen die *Usability* für Ärzte und Pfleger beeinträchtigen (z. B. komplexe Anmeldeprozeduren, Zugriffsbegrenzungen, regelmäßige Unterbrechungen für Updates) (Institute of Medicine 2012; Jabin 2024). Wenn in der Notaufnahme jede Minute zählt, kann ein IT-System, das wegen Sicherheitspatches gerade neu startet, zum Problem werden. Umgekehrt birgt ein Verzicht auf solche Maßnahmen Risiken. Dieser Konflikt zeigt sich auch bei der Einführung neuer digitaler Tools (Institute of Medicine 2012; Jabin 2024): Möchte man schnell telemedizinische Services anbieten, kann man diese vielleicht nicht sofort perfekt absichern – wartet man mit der Einführung bis alles sicher ist, könnte man wertvolle Versorgungsfortschritte verzögern. Es gibt hier einen Trade-off zwischen Innovation und Sicherheit.

Ethische Bewertung des Ressourceneinsatzes

Aus ethischer Sicht ist der Ressourcenkonflikt eine Frage der *Gerechtigkeit und der Sorgfaltspflicht*. Jeder Patient hat das Recht auf eine Behandlung nach aktuellem medizinischen Standard. Dazu gehört heutzutage implizit auch, dass die Behandlung nicht durch vorhersehbare technische Pannen gefährdet wird. Patientensicherheit umfasst also auch IT-Sicherheit (Formosa et al. 2021). Man kann argumentieren, dass Ausgaben für Cybersecurity letztlich *Ausgaben für Patientensicherheit* sind und daher nicht in Konkurrenz zu klinischen Ausgaben stehen, sondern ein Teil davon sein müssen. Ähnlich wie Investitionen in Hygiene oder Medikamentensicherheit (z. B. Apotheker, die Wechselwirkungen prüfen) Geld kosten, aber unabdingbar sind, sollte IT-Sicherheit als Qualitätsmerkmal von Versorgung betrachtet werden, nicht als Luxus. Das Nicht-Schaden-Prinzip verpflichtet ein Krankenhaus, vermeidbare Schäden von Patienten abzuwenden (Formosa et al. 2021) – ein durch Nachlässigkeit ermöglichter Cyberangriff, der Patienten schadet, wäre ein vermeidbarer Schaden. Aus diesem Blickwinkel ist Geld, das präventiv in IT-Sicherheit fließt, ethisch gerechtfertigt, weil es zukünftiges Leid verhindert (Formosa et al. 2021).

Konflikt in der Akutsituation

Der Verteilungskonflikt zeigt sich auch in Echtzeit während eines Angriffs: Wenn ein Virus im Netzwerk ist, steht man vor der Wahl, *Systeme sofort vom Netz zu trennen* (um den Angriff einzudämmen) vs. *sie weiterlaufen zu lassen* (um laufende Behandlungen nicht abzubrechen). Das Lukaskrankenhaus 2016 entschied sich z. B., sofort alles herunterzufahren, um Daten zu schützen – ein ehrenwertes Ziel, aber dadurch wurde die Versorgung extrem eingeschränkt (Kell 2024; Hartmannbund 2022). Hätte man länger gewartet, wären evtl. mehr Daten kompromittiert worden. Dieser Zielkonflikt zwischen Datenschutz/Sicherheit und Versorgungscontinuity erfordert situative Abwägung: Hier sollten Ethik- und Krisenteams gemeinsam Entscheidungen treffen, da es um Abwägungen zwischen verschiedenen Schadenarten geht (Datenintegrität vs. Patientenwohl unmittelbar).

Fallbeispiel: Der Cyberangriff auf die Uniklinik Düsseldorf (2020)

Am 10. September 2020 kam es am UKD zu einem schwerwiegenden IT-Sicherheitsvorfall. Späteren Analysen zufolge drangen Hacker durch Ausnutzung einer bekannten Schwachstelle in einer VPN-Software (Citrix) in das Kliniknetz ein (Pfenninger et al. 2023). Bemerkenswert ist, dass die Schwachstelle (CVE-2019-19781) und der entsprechende Patch bereits seit Januar 2020 bekannt waren (BSI 2020). Offenbar waren jedoch einige Server der Uniklinik zu diesem Zeitpunkt – neun Monate später – noch verwundbar oder bereits zuvor kompromittiert worden (Pfenninger et al. 2023). Die Angreifer installierten die Ransomware DoppelPaymer, die Dateien verschlüsselte und das IT-System großteils lahmlegte (Buhtz 2020). Interessant ist ein Detail: Die Erpresser hatten in ihrer Lösegeldforderung ursprünglich die „Heinrich-Heine-Universität“ adressiert (zu der die Klinik gehört). Das lässt vermuten, dass die Täter dachten, sie hätten ein reines Hochschulnetz verschlüsselt – als sie jedoch erfuhren, dass sie ein Krankenhaus getroffen hatten, zogen sie sich teilweise zurück (Pfenninger et al. 2023). Tatsächlich stellten die Hacker nach Kontaktaufnahme durch die Behörden einen Entschlüsselungscode zur Verfügung und verzichteten auf die Lösegeldforderung. Diese ungewöhnliche Wendung zeigt, dass selbst Cyberkriminelle die moralische Grenze spürten, als ein Krankenhaussystem betroffen war. Gleichwohl war der Schaden bereits eingetreten.

Die Uniklinik Düsseldorf sah sich gezwungen, den IT-Betrieb weitgehend herunterzufahren. *Alle planbaren Aufnahmen, Operationen und Verfahren wurden abgesagt*, da keine Zugriffsmöglichkeiten auf digitale Patientenakten, Labordaten oder Terminpläne bestanden (Pfenninger et al. 2023). Insgesamt mussten schätzungsweise hundert Operationen und Eingriffe verschoben werden. Besonders kritisch war die Situation in der Notfallversorgung: Die *Notaufnahme der UKD wurde komplett abgemeldet*, da weder eine sichere Patientenaufnahme noch eine rasche Labordiagnostik gewährleistet werden konnte. Über 13 Tage hinweg (bis zum 23. September 2020) blieb die Notaufnahme geschlossen (Pfenninger et al. 2023) – ein beispielloser Zeitraum für ein Maximum-Care-Krankenhaus. In dieser Zeit mussten *Notfallpatienten auf andere Kliniken verteilt* werden, was die umliegenden Häuser zusätzlich

belastete. Die UKD selbst konnte in diesem Zeitraum nur etwa 50 % ihrer üblichen Patienten versorgen; der Rest musste abgewiesen oder verlegt werden. Es handelt sich also um einen teilweisen Zusammenbruch der Versorgungsleistung (William 2020). Parallel dazu arbeitete ein mobiles Einsatzteam des BSI vor Ort, um die Netzwerke zu analysieren und zu reinigen (BSI 2020).

Ethische Dilemmata: Lösegeldzahlungen und Umgang mit Erpressern

Cyberangriffe auf Kliniken werfen spezifische ethische Dilemmas auf, weil sie Akteure in Zwangslagen versetzen, für die es keine einfachen Lösungen gibt. Eines der zentralen Dilemmata betrifft den Umgang mit den Forderungen der Angreifer – typischerweise der Lösegeldforderung bei Ransomware. Krankenhäuser stehen hier zwischen zwei schlechten Optionen: Zahlen sie das Lösegeld, unterstützen sie kriminelle Machenschaften und möglicherweise zukünftige Angriffe; zahlen sie nicht, riskieren sie verlängerte Ausfallszeiten, Datenlecks und damit potentielle Schäden für Patienten.

Behörden und Sicherheitsexperten raten in aller Regel strikt davon ab, Lösegeld an Cyberkriminelle zu zahlen (Koch 2024). Aus guten Gründen: Eine Zahlung würde das *Geschäftsmodell Ransomware* weiter befeuern – jeder Erfolg der Täter motiviert sie und andere, vermehrt Angriffe durchzuführen. Zudem ist eine Zahlung keine Garantie für vollständige Wiederherstellung: Es kam vor, dass trotz Zahlung die Systeme nicht wiederhergestellt wurden oder die Hacker später erneut zuschlugen, weil sie Hintertüren hinterlassen hatten. Grundsätzlich gilt das Prinzip *„Nicht mit Terroristen verhandeln“* als ethische Richtschnur, hier übertragen auf digitale Erpressung. Es entspricht einer pflichtorientierten Haltung (Gesinnungsethik): Man verzichtet aus Prinzip darauf, Unrecht nachzugeben, selbst wenn es kurzfristig vorteilhaft erschiene (Höffe 2023; Hoffman und Baker 2023). Auch das Gerechtigkeitsprinzip spricht gegen Zahlungen: Die finanziellen Mittel eines Krankenhauses sollten eigentlich der Patientenversorgung zugutekommen, nicht Verbrechern. Zudem könnten Zahlungen indirekt anderen Patienten schaden, weil sie weitere Angriffe anreizen, die dann vielleicht weniger glimpflich verlaufen (Höffe 2023; Hoffman und Baker 2023). Die DSGVO könnte im Falle einer Zahlung an Erpresser, die personenbezogene Daten erbeutet haben, ebenfalls relevant werden: Es ist fraglich, ob eine solche „Lösegeldzahlung“ mit den Compliance-Pflichten vereinbar wäre, da man ja einem Datenschutzverstoß nachgibt, anstatt ihn zu melden und abzustellen.

Auf der anderen Seite steht die harte Realität: Wenn ein Krankenhaus akut lahmgelegt ist und Menschenleben am seidenen Faden hängen, kann die Versuchung groß sein, durch Zahlung den Betrieb schneller wiederherzustellen. Aus der Sicht der Verantwortungsethik oder utilitaristischer Abwägung könnte argumentiert werden: Die unmittelbaren Konsequenzen des Nicht-Zahlens – z. B. Intensivpatienten ohne Monitor, nicht durchführbare Operationen – wiegen schwerer als das abstrakte Fernziel, Kriminalität langfristig nicht zu fördern. Die Fürsorgepflicht gegenüber aktuellen Patienten könnte als höher gewertet werden als die allgemeine Pflicht, Kriminelle nicht zu unterstützen. In extremen Fällen, wenn etwa die IT-Ausfälle keinen anderen Ausweg lassen und das Leben vieler Patienten akut bedroht ist, mag eine

Zahlung als „geringeres Übel“ erscheinen. Es gibt Berichte (insbesondere aus den USA), dass Krankenhäuser im Geheimen Lösegeld bezahlt haben, um ihre Systeme schneller entschlüsseln zu können – etwa weil die Datensicherungen unvollständig waren und jeder verlorene Tag hunderte Patienten gefährdete. So hat z. B. ein großes Universitätsklinikum in den USA 2020 über eine Million Dollar gezahlt, um Forschung und Klinikdaten zurückzubekommen (Winder 2020) (dies wurde erst später öffentlich bekannt). In Deutschland wurde bislang kein Fall öffentlich bestätigt, in dem ein Krankenhaus Lösegeld gezahlt hätte; Umfragen deuten aber darauf hin, dass rund 20 % der betroffenen Gesundheitseinrichtungen tatsächlich zahlen (Dettling und Ekkernkamp 2024).

Zwei klassische ethische Denkschulen bieten sich an, um Orientierung zu gewinnen: die Prinzipienethik (Beauchamp und Childress 2019) und die Verantwortungsethik (im Sinne einer konsequenzorientierten Führungsverantwortung, wie u. a. von Max Weber kontrastiert zur Gesinnungsethik beschrieben). Beide Perspektiven sollen hier angewandt werden, um zu einer umfassenden Bewertung zu gelangen.

Prinzipienethische Perspektive

Die Prinzipienethik basiert auf vier grundlegenden Prinzipien, die auch in der Medizinethik weithin anerkannt sind: *Respekt vor der Autonomie, Nichtschädigung, Wohltätigkeit* und *Gerechtigkeit* (Beauchamp und Childress 2019). Im Kontext von Cyberangriffen auf Kliniken lassen sich diese folgendermaßen auslegen:

Autonomie

Patienten vertrauen Krankenhäusern ihre Gesundheit und intimsten Daten an. Sie tun dies in der Annahme, dass ihre Autonomie und Persönlichkeitsrechte gewahrt bleiben. Ein Cyberangriff kann die Patientenautonomie in zweifacher Hinsicht tangieren: Zum einen durch den *Verlust von Kontrolle über persönliche Gesundheitsdaten* (wenn etwa diese entwendet und veröffentlicht werden – eine Verletzung der informellen Selbstbestimmung und Privatsphäre). Zum anderen durch die *Beeinträchtigung der Entscheidungsfreiheit in der Behandlung*, falls z. B. Behandlungsoptionen eingeschränkt sind oder Patienten verlegt werden, ohne dass sie mitbestimmen können (im Falle von Systemausfällen bleibt oft keine Wahl, als abzuwarten oder ins nächste Krankenhaus zu gehen). Prinzipienethisch ergibt sich hier die Forderung, dass Krankenhäuser alles Zumutbare tun müssen, um die informationelle Autonomie ihrer Patienten zu schützen (sprich: Datenschutz und Systemsicherheit gewährleisten). Es ist auch ein Gebot der Menschenwürde, Patienten nicht zu Objekten fremder Machenschaften werden zu lassen. Auch interne Entscheidungen wie das Offenlegen eines Angriffs gegenüber Patienten (Transparenz) sind unter Autonomie-Aspekten relevant: Patienten haben ein Recht zu erfahren, wenn z. B. ihre Daten betroffen sind oder sie wegen IT-Problemen anders disponieren müssen (Segawa 2020).

Nichtschädigung (Non-Maleficence)

Dieser Grundsatz – „primum non nocere“ (zuallererst nicht schaden) – ist zentral für das Gesundheitswesen (Gillon 1985). Bezogen auf Cybersecurity bedeutet er: Ein Krankenhaus darf durch seine *Unterlassungen oder Fahrlässigkeit* keinen vermeidbaren Schaden an Patienten verursachen. Das Versäumnis, Sicherheitsvorkehrungen zu treffen, könnte als solche fahrlässige Unterlassung interpretiert werden, wenn es zu Schaden kommt. In der modernen Medizin umfasst das Nichtschädigungsgebot demnach nicht nur, keine falschen Medikamente zu geben, sondern auch, keine unsicheren IT-Strukturen zu betreiben, die dann zu Gefährdungen führen. Wenn zum Beispiel ein lebensrettendes Gerät (etwa ein Beatmungsgerät oder Infusionspumpe) durch Malware ausfällt und ein Patient dadurch Schaden nimmt, so ist dies – aus prinzipienethischer Sicht – ein Verstoß gegen Non-Maleficence durch unzureichende Vorsorge. Kliniken haben also die moralische Pflicht zur *Gefahrenabwehr* im IT-Bereich, analog zu Brandschutz oder Hygiene. Das beinhaltet auch, im Krisenfall umsichtig abzuwägen: Beispielsweise kann die Entscheidung, sämtliche Systeme sofort vom Netz zu trennen (um die Ausbreitung der Malware zu stoppen), mit kurzzeitigen Schäden für einige Patienten verbunden sein (z. B. Diagnoseverzögerung) – hier muss man das kleinere Übel wählen, um größeren Schaden zu verhindern. Wichtig ist, dass solche Abwägungen immer im Lichte des Nichtschädigungsprinzips geschehen und nicht etwa aus primär ökonomischen Interessen.

Wohltätigkeit (Beneficence)

Dieses Prinzip gebietet aktives Handeln zum Wohl des Patienten (De Roubaix 2011). Übertragen auf die Cyber-Thematik heißt das: Es genügt nicht, nur Schäden zu vermeiden; Krankenhäuser sollen proaktiv Gutes tun, also die bestmögliche Versorgung bieten. Dazu gehört zunehmend, robuste *Resilienz* gegen Störungen aufzubauen, damit das Wohl der Patienten auch unter widrigen Umständen gewahrt bleibt. Man könnte sagen, dass die Etablierung guter IT-Sicherheit ein Akt der Beneficence ist, da man damit vorsorglich Patienten Gutes tut – nämlich die Versorgungskontinuität sicherstellt. Sollte ein Angriff passieren, verlangt Beneficence, dass man alle Kräfte mobilisiert, um die Versorgung aufrechtzuerhalten (z. B. Umverteilung von Patienten, Mobilisierung von analogen Alternativen). Ebenfalls relevant: Die Nachsorge für Patienten, die durch einen Angriff z. B. Datenschutzverletzungen erlitten haben (Betreuung, Beratung, Identitätsschutz etc.), fällt unter Wohltätigkeit. Insgesamt erinnert das Prinzip daran, dass die Patientenwohlfahrt der oberste Maßstab sein muss, auch bei Entscheidungen im Hintergrund (wie IT-Investitionen).

Gerechtigkeit

Das Gerechtigkeitsprinzip spielt auf mehreren Ebenen eine Rolle (Rawls 1977). Verteilungsgerechtigkeit stellt die Frage, ob Ressourcen fair verteilt werden – hier z. B. ob genügend Mittel in die weniger sichtbare, aber essentielle IT-Sicherheit fließen im Vergleich zu anderen Bereichen. Interne Budgetentscheidungen werden somit zu ethischen Entscheidungen: Es wäre ungerecht, IT-Sicherheit sträflich zu vernach-

lässigen, weil man kurzfristig andere Wünsche priorisiert, denn man setzt damit bestimmte Patientengruppen (diejenigen, die im Angriffsfall betroffen sein werden) einem höheren Risiko aus als andere. Gerechtigkeit hat aber auch eine globale bzw. zukünftige Dimension: Wenn ein Krankenhaus Lösegeld zahlt, mag es intern Nutzen stiften, aber es trägt womöglich zu mehr Angriffen auf andere Häuser (oder in Zukunft auf sich selbst) bei – das wäre gegenüber der Gesamtheit der potenziellen Opfer unfair. Hier prallen kurzfristige lokale Gerechtigkeit (unsere Patienten jetzt bestmöglich schützen) und längerfristige universelle Gerechtigkeit (keinen Anreiz für mehr Verbrechen schaffen) aufeinander. Gerechtigkeit beinhaltet ferner Gleichbehandlung: Alle Patienten sollen gleiche Chancen auf sichere Versorgung haben. Wenn einige Kliniken top ausgestattet und sicher sind, andere aber nicht, entsteht eine Ungleichheit. Aus ethischer Sicht wäre es geboten, dass Mindest-Sicherheitsstandards überall gelten (und ggf. von Staat/Kostenträgern unterstützt werden), damit nicht Patienten zufällig schlechter gestellt sind, je nachdem in welchem Krankenhaus sie behandelt werden. Diese Überlegung stützt z. B. regulatorische Eingriffe: Man schreibt Standards verbindlich fest, um Gerechtigkeit zwischen Einrichtungen und damit Patienten zu schaffen.

Verantwortungsethische Perspektive

Während die Prinzipienethik eher einen Katalog von einzuhaltenden Werten liefert, fokussiert die Verantwortungsethik auf die *Konsequenzen des Handelns* und die *Verantwortung der Handelnden*, insbesondere Entscheidungsträger (Weber 1919; Endress 2020). Im Kontext von Cyberangriffen auf Kliniken lassen sich einige Aspekte herausarbeiten:

Prospektive Verantwortung

Hans Jonas prägte in der Technikethik die Forderung, dass wir angesichts der potenziell katastrophalen Folgen moderner Technik eine neue, vorausschauende Verantwortung übernehmen müssen. Übertragen bedeutet das: Klinikleitungen und Gesundheitspolitiker tragen Verantwortung dafür, vorauszudenken und Prävention zu betreiben, um katastrophale Folgen von IT-Ausfällen zu verhindern. Das beinhaltet eine *Ethik der Vorsorge*: Es genügt nicht, ex post zu reagieren; proaktive Planung und Investition sind moralisch gefordert. Eine verantwortungsethische Maxime wäre hier: *Handle so, dass die Folgen deines Unterlassens nicht die Grundbedingungen der Patientenwohlfahrt zerstören.* Konkret: Sorge dafür, dass kein Szenario eintritt, in dem Patienten wegen vorhersehbarer IT-Probleme sterben oder erheblichen Schaden erleiden. Diese schwere moralische Vorpflicht liegt bei den Führungskräften, da sie die Macht haben, vorbeugende Maßnahmen umzusetzen.

Abwägung und Gesamtverantwortung

Max Webers Unterscheidung zwischen Gesinnungsethik (Handeln nach festen Überzeugungen ohne Blick auf Folgen) und Verantwortungsethik (Handeln nach Abwägung der Folgen und Übernahme der Haftung dafür) ist hier besonders einschlägig.

Ein Krankenhausmanager muss im Falle eines Cyberangriffs *Verantwortungsethiker* sein: Er kann nicht stur an einem Prinzip festhalten, wenn es die aktuelle Lage verschlimmern würde. Beispiel Lösegeld: Eine rein prinzipientreue Haltung („Wir verhandeln nicht mit Kriminellen, Punkt") entspricht der Gesinnungsethik. Die Verantwortungsethik würde sagen: *Ich übernehme die Verantwortung für alles, was aus meiner Entscheidung folgt.* Wenn also das Nicht-Zahlen zum Tod von Patienten führt, müsste der Entscheider dies vor seinem Gewissen und ggf. der Justiz vertreten können. Verantwortungsethik bedeutet nicht zwangsläufig, dass man immer zugunsten des kurzfristigen Nutzens (z. B. Patientenrettung durch Lösegeld) entscheidet – es bedeutet vielmehr, dass man die Konsequenzen in alle Richtungen berücksichtigt und bewusst die Bürde der Entscheidung trägt. Es könnte z. B. heißen: „Wir zahlen nicht, und ich trage die Verantwortung dafür, weil ich glaube, dass langfristig nur so die Sicherheit vieler gewährleistet ist." Oder umgekehrt: „Wir zahlen in diesem einen Fall, und ich stehe dafür gerade, weil akut sonst Menschen sterben." Wichtig ist, dass die Entscheidung *reflektiert und begründbar* ist, nicht dogmatisch. Verantwortungsethik in der Klinik verlangt somit eine *situative Ethik*: Jeden Vorfall sorgfältig analysieren, Experten und idealerweise auch Ethikkommissionen konsultieren, dann entscheiden – und anschließend transparent machen, warum so entschieden wurde, um die Verantwortung auch öffentlich zu schultern.

Organisationsethik und Kultur

Verantwortungsethik kann auch kollektiv interpretiert werden: Die Organisation als Ganzes trägt Verantwortung für ihre Risiken. In einer Ethik der Verantwortung wäre es unverantwortlich, Cybersecurity dem Zufall oder nur der IT-Abteilung zu überlassen. Stattdessen muss sie in die Corporate Governance integriert sein. Ein ethisch verantwortliches Krankenhaus wird z. B. eine Kultur fördern, in der Mitarbeitende Sicherheitsvorfälle sofort melden (statt sie aus Angst zu vertuschen), in der Trainings ernst genommen werden und in der bei strategischen Entscheidungen (etwa Einführung neuer IT-Systeme) immer die Frage nach der Sicherheit gestellt wird. Hier zeigt sich auch, dass Verantwortungsethik Hand in Hand mit *Transparenz* geht: Wer Verantwortung übernehmen will, darf Risiken nicht unter den Teppich kehren. Das bedeutet etwa, dass Kliniken offen mit Beinahe-Zwischenfällen umgehen sollten, um daraus zu lernen – ein Prinzip, das man aus der Patientensicherheit (CIRS-Systeme für Fehlerberichte) kennt, lässt sich auf Cybervorfälle übertragen.

Intergenerationelle Verantwortung

Ein weiterer Aspekt (auch bei Jonas) ist die Verantwortung gegenüber *zukünftigen Generationen*. Im IT-Kontext sind das die zukünftigen Patienten und Belegschaften. Wenn wir heute versäumen, robuste Strukturen zu schaffen, laden wir den kommenden Akteuren Probleme auf. Die fortschreitende Digitalisierung (Stichwort KI, vernetzte Medizingeräte) wird das Problem potenziell verschärfen. Verantwortungsethisch müsste man also jetzt die Grundlagen legen, damit auch morgen noch eine sichere Versorgung möglich ist. Das könnte beinhalten, frühzeitig in sichere Archi-

tekturen zu investieren, Bildung im Bereich Cyber-Hygiene in die Curricula von medizinischem Personal aufzunehmen etc.

Handlungsempfehlungen für Klinikleitungen, Gesetzgeber und Ethikkommissionen

Aus der vorangegangenen Analyse ergeben sich zahlreiche Ansatzpunkte, wie die Gefahren durch Cyberangriffe im Gesundheitswesen angegangen werden können. Zum Abschluss sollen konkrete Handlungsempfehlungen ausgesprochen werden, zugeschnitten auf verschiedene Akteursebenen:

Für Klinikleitungen und -träger

Priorisierung und Integration von IT-Sicherheit auf höchster Ebene. Sicherheitsrisiken gehören auf die Agenda von Vorstandssitzungen, vergleichbar mit Finanz- oder Qualitätskennzahlen. Führungskräfte sollten eine Sicherheitskultur vorleben, in der z. B. Phishing-Tests, Schulungen und Notfallübungen selbstverständlich sind (Pfenninger et al. 2023). Essenziell ist die *Implementierung eines ISMS* (Informationssicherheits-Managementsystems) nach etablierten Standards (B3S Krankenhaus, ISO 27001 o. ä.), wodurch Risiken systematisch erfasst und gemanagt werden. Investitionen in Redundanz (Backup-Systeme, zweite Rechenzentren), aktuelle Hard- und Software sowie in fachkundiges Personal (Security-Spezialisten, 24/7-Bereitschaften) sind nicht optional, sondern Teil der Daseinsvorsorge. Hier sollten Kliniktträger auch kreativ über Kooperationen nachdenken: Geteilte SOCs (Security Operation Centers) für mehrere Häuser oder die Nutzung von Branchen-CERTs (Computer Emergency Response Teams) können Effizienzgewinne bringen. Außerdem sollten Notfallpläne nicht nur auf dem Papier stehen: Jährliche praxisnahe Übungen (z. B. ein „Cyber-Alarm“ Szenario) mit Beteiligung der IT, Mediziner, Verwaltung und evtl. externer Partner (BSI, Landesbehörden) sind zu empfehlen, um im Ernstfall vorbereitet zu sein. Dokumentation ist ebenso wichtig: Sämtliche Entscheidungen rund um IT-Sicherheit sollten aufgezeichnet werden, um im Nachhinein die Sorgfalt belegen zu können (Dittrich und Dann 2025; Pfenninger et al. 2023). Schließlich sollten Kliniken intern Ethik-Boards oder Krisenstäbe haben, die bei Dilemma-Entscheidungen (z. B. Lösegeld) beratend hinzugezogen werden, damit diese Entscheidungen auf einer breiten und reflektierten Basis getroffen werden.

Für Gesetzgeber und Aufsichtsbehörden

Die Politik sollte weiterhin den Rahmen so setzen, dass IT-Sicherheit integraler Bestandteil der Gesundheitsversorgung ist. Dazu zählt erstens die ausreichende *Finanzierung* – etwa Verlängerung und Ausbau von Förderprogrammen wie dem KHZG speziell für Security-Upgrades, sowie die Berücksichtigung von IT-Sicherheitskosten in den Krankenhausbudgets (z. B. könnten definierte Sicherheitsstandards finanziert werden wie Pflegepersonalquoten). Zweitens sollten die *gesetzlichen Vorgaben regelmäßig aktualisiert* werden, um mit der Bedrohungslage Schritt zu halten. Die

Umsetzung der EU-Richtlinie NIS-2 in nationales Recht (bis 2024) sollte den Gesundheitssektor weiter stärken, möglicherweise durch Absenkung von Schwellenwerten, sodass mehr Einrichtungen unter kritische Regulierung fallen, sowie durch verschärfte Meldepflichten und Sanktionen bei Nachlässigkeit. Drittens wäre die Förderung von zentraler Expertise sinnvoll: Z. B. könnten spezialisierte Einheiten beim BSI oder Landesgesundheitsministerien geschaffen werden, die Kliniken beraten, Mindeststandards prüfen und im Ereignisfall koordinieren. Denkbar ist etwa ein *Cyber-TÜV* für Krankenhäuser – regelmäßige Audits, deren Ergebnisse auch Transparenz für Patienten schaffen (ähnlich wie Hygiene-Ampeln). Gesetzgeberisch könnte man ferner *klarstellen*, wie im Ernstfall mit Lösegeldforderungen umzugehen ist (derzeit gibt es kein ausdrückliches Verbot, aber auch keine Erlaubnis; hier könnten Leitlinien helfen, etwa ein Standard-Vorgehen mit Polizeieinschaltung und Entscheidungsalgorithmen). Haftungsrechtlich sollte überlegt werden, ob Krankenhausträger bei grober Vernachlässigung der IT-Sicherheit stärker in die Pflicht genommen werden – dies wäre aber das letzte Mittel; sinnvoller ist positive Anreizsetzung. Internationaler Austausch ist ebenfalls Aufgabe des Gesetzgebers: Angriffe machen nicht an Grenzen Halt, daher sind Abkommen zur Strafverfolgung und gemeinsame Übungen mit Partnerländern (z. B. im EU-Rahmen oder mit der NATO für Cyberverteidigung) wichtig. Schließlich könnten Gesetzgeber Ethikkommissionen beauftragen, Leitfäden zu erarbeiten (siehe unten), was die normative Orientierung stärkt.

Für Ethikkommissionen und -gremien

Medizinethische Kommissionen – sei es auf lokaler Ebene (Krankenhaus-Ethikkomitees) oder national (wie der Deutsche Ethikrat) – sollten das Thema *„Cybersecurity und Patientenwohl“* offensiv aufgreifen. Bisher standen klinisch-ethische Fragen (etwa am Lebensende) im Vordergrund, doch die Digitalisierung bringt neuartige ethische Herausforderungen, für die Leitlinien erarbeitet werden sollten. Eine Empfehlung ist, Handlungsempfehlungen für Dilemmasituationen zu entwickeln: z. B. ein ethisches Rahmenpapier zum Umgang mit Erpressungsfällen (Kriterien, wann allenfalls eine Zahlung erwogen werden kann, wie Transparenz herzustellen ist, wie hinterher Wiedergutmachung aussehen könnte). Ebenso könnten Ethikgremien definieren, was *„angemessenes“* Verhalten bei Ressourcenallokation ist – also ab welchem Punkt Unterinvestition in Sicherheit ethisch unverantwortlich wird. Krankenhaus-Ethikkomitees könnten in ihre Fallbesprechungen auch IT-Krisen aufnehmen und interdisziplinär bewerten, um Sensibilität zu schaffen. Wichtig ist zudem die Einbindung der Patientensicht: Ethikräte könnten erheben, welche Erwartungen und Ängste Patienten in Bezug auf digitale Sicherheit haben, um dies ins Kalkül zu ziehen. Der Deutsche Ethikrat oder ähnliche Gremien könnten eine Stellungnahme erarbeiten, die die Verantwortlichkeiten aller Akteure normativ einordnet – etwa zur Frage, ob Patientenschutz im Digitalen eventuell als Teil der ärztlichen Berufsethik explizit formuliert werden sollte. Außerdem könnten Ethiker im öffentlichen Diskurs helfen, Verständnis dafür zu wecken, dass gewisse Einschränkungen (z. B. erhöhte Sicherheitsprozeduren beim Klinikzutritt oder Verzögerungen durch IT-Wartung)

im Dienst des Patientenwohls stehen, und somit die Akzeptanz solcher Maßnahmen steigern.

Fazit

Cyberangriffe auf Krankenhäuser sind keine hypothetische Gefahr mehr, sondern bittere Realität – sie gefährden die Patientenversorgung, stellen Kliniken vor rechtliche und finanzielle Probleme und fordern die medizinethischen Grundsätze heraus. In diesem Beitrag wurde gezeigt, dass die Thematik nur interdisziplinär angemessen verstanden und bearbeitet werden kann: Technische Schutzmaßnahmen müssen mit rechtlichen Verpflichtungen und ethischen Überlegungen Hand in Hand gehen.

Aus der technisch-empirischen Perspektive wurde deutlich, dass die Bedrohungslage im Gesundheitswesen so ernst ist wie nie zuvor. Beispiele wie der Angriff auf die Uniklinik Düsseldorf 2020 haben greifbar gemacht, welche dramatischen Folgen eintreten können – bis hin zum möglichen Verlust von Menschenleben. Solche Ereignisse dürfen nicht als Ausnahmepech abgetan werden, sondern müssen als Warnsignal dienen, die digitale Resilienz von Kliniken zu erhöhen.

Mit § 75c SGB V und strengen KRITIS-Vorgaben wurde ein verbindlicher Rahmen geschaffen, der alle Krankenhäuser in die Pflicht nimmt, moderne IT-Sicherheit zu gewährleisten. Datenschutzrechtlich besteht ebenfalls ein engmaschiges Netz, das Patientendaten schützt und Nachlässigkeit sanktioniert. Dennoch sind Gesetze immer nur so wirksam, wie sie umgesetzt werden. Hier bestehen in der Praxis nach wie vor Lücken – nicht zuletzt wegen begrenzter Ressourcen, Wissensdefiziten und manchmal fehlender Priorisierung.

Die ethische Betrachtung untermauert, warum die Einhaltung dieser Pflichten nicht bloß juristische Erfüllung, sondern Kernbestandteil der medizinischen Ethik ist. Patientenwohl, Nicht-Schaden und Gerechtigkeit verlangen, dass Krankenhäuser auch im digitalen Raum sichere Zufluchtsorte sind. Jeder Cybervorfall ist damit auch ein Ethikfall. Die normative Auseinandersetzung mit Dilemmas – wie dem Umgang mit Lösegeldforderungen – offenbart, dass es zwar keine einfachen Antworten gibt, aber wohlabgewogene Entscheidungen getroffen werden können, die die Werte des Gesundheitswesens hochhalten.

IT-Sicherheit im Krankenhaus ist Fürsorgearbeit. Sie mag unsichtbar sein, aber sie rettet im Zweifel Leben, so wie ein stabiler OP-Tisch oder eine funktionierende Alarmkette auf der Intensivstation. Alle Beteiligten – Klinikleitungen, Gesetzgeber, Ethikgremien, aber auch jede/r Beschäftigte – tragen einen Teil der Verantwortung, diese Sicherheit zu gewährleisten. Die Digitalisierung der Medizin bietet enorme Chancen für bessere Versorgung, doch sie fordert uns zugleich heraus, neue Schutzmaßnahmen zu entwickeln und ethische Prinzipien auf ungewohntem Terrain anzuwenden. Der Spagat zwischen High-Tech-Medizin und Verwundbarkeit durch High-Tech-Verbrechen ist zu bewältigen, indem wir Technik, Recht und Ethik integriert denken. Nur so können wir dem Versorgungsauftrag gerecht werden und das Patientenwohl – unser oberstes Gut – auch im digitalen Zeitalter bewahren.

Einhaltung ethischer Richtlinien

Interessenkonflikt F.M. Teichmann gibt an, dass kein Interessenkonflikt besteht.

Ethische Standards Für diesen Beitrag wurden von den Autor/-innen keine Studien an Menschen oder Tieren durchgeführt. Für die aufgeführten Studien gelten die jeweils dort angegebenen ethischen Richtlinien.

Literatur

Beauchamp T, Childress J (2019) Principle of biomedical ethics. 19:9–12. https://doi.org/10.1080/15265161.2019.1665402

Becker U, Kingreen T (2024) SGB V Kommentar, 9. Aufl. C.H. Beck, München

Briegleb V (2017) WannaCry: Was wir bisher über die Ransomware-Attacke wissen. https://www.heise.de/news/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html. Zugegriffen: 4. Sept. 2025

BSI (2020) Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnt vor akuter Ausnutzung bekannter Sachstelle. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920. Zugegriffen: 4. Sept. 2025

BSI (2022) Die Lage der IT-Sicherheit in Deutschland 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8. Zugegriffen: 4. Sept. 2025

BSI (2024) Cybersicherheit im Gesundheitswesen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Gesundheitswesen_2024.pdf?__blob=publicationFile&v=3. Zugegriffen: 4. Sept. 2025

Buhtz A (2020) Ermittlung zu Hackerangriff auf Uniklinik führen nach Russland. Zeit. https://www.zeit.de/digital/datenschutz/2020-09/duesseldorf-uniklinik-hackerangriff-russland-ermittlungen-schadsoftware-trojaner. Zugegriffen: 4. Sept. 2025

Carmasec IT-Sicherheit für Krankenhäuser, der neue § 75c SGB V. https://www.carmasec.com/de/pdsg-it-sicherheit-fuer-krankenhaeuser/. Zugegriffen: 4. Sept. 2025

CLAROTY (2023) The Global Healthcare Cybersecurity Study 2023. https://claroty.com/resources/reports/the-global-healthcare-cybersecurity-study-2023. Zugegriffen: 4. Sept. 2025

De Roubaix JAM (2011) Beneficence, non-maleficence, distributive justice and respect for patient autonomy–reconcilable ends in aesthetic surgery? J Plast Reconstr Aesthetic Surg 64:11–16. https://doi.org/10.1016/j.bjps.2010.03.034

Dettling D, Ekkernkamp A (2024) Wie können Deutschlands Kliniken sich schützen? Komunal. https://kommunal.de/deutschlands-kliniken-bedroht-Cyberangriffe-krieg. Zugegriffen: 4. Sept. 2025

Dittrich T, Dann M (2025) Cyberangriffe auf Krankenhäuser: Was, wenn der Patient zu Schaden kommt? https://www.heise.de/hintergrund/Cybersicherheit-im-Krankenhaus-Was-passiert-wenn-der-Patient-zu-Schaden-kommt-10281077.html. Zugegriffen: 4. Sept. 2025

DKG (2025) IT-Ausgaben deutscher Kliniken im internationalen Vergleich besonders niedrig. https://www.dkgev.de/dkg/presse/details/it-ausgaben-deutscher-kliniken-im-internationalen-vergleich-besonders-niedrig/. Zugegriffen: 4. Sept. 2025

Dose J (2019) Interview: So verlief die Ransomware-Attacke im Lukaskrankenhaus. https://www.computerwoche.de/article/2791586/so-verlief-die-ransomware-attacke-im-lukaskrankenhaus.html. Zugegriffen: 4. Sept. 2025
Ehmann E, Selmayr M (2024) Datenschutz-Grundverordnung Kommentar, 3. Aufl. C.H. Beck, München
Endress M (2020) Ethik (Gesinnungs- und Verantwortungsethik). In: Müller H-P, Sigmund S (Hrsg) Max Weber. Handbuch: Leben – Werk – Wirkung, 2. Aufl. Springer, Stutgart, S 67–69
Formosa P, Wilson M, Richards D (2021) A principlist framework for cybersecurity ethics. Comput Secur 109:102382. https://doi.org/10.1016/j.cose.2021.102382
Gillon R (1985) "Primum non nocere" and the principle of non-maleficence. BMJ 291:130–131. https://doi.org/10.1136/bmj.291.6488.130
Gola P, Heckmann D (2022) Datenschutz-Grundverordnung Kommentar, 3. Aufl. C.H. Beck, München
Grotelueschen J (2024) Vernetzung, Kollaboration und Interoperabilität in der Krankenhausversorgung. https://www.rolandberger.com/de/Insights/Publications/Roland-Berger-Krankenhaus-IT-Monitor-2024.html. Zugegriffen: 4. Sept. 2025
Hänlein A, Schuler R (2022) Sozialgesetzbuch V Kommentar, 6. Aufl. Nomos, Baden-Baden
Hartmannbund (2022) Der unsichtbare Feind – Was Cyberangriffe für Praxen und Kliniken bedeuten. Hartmannbund, Köln
von Heintschel-Heinegg B, Kudlich H (2025) Strafgesetzbuch Kommentar, 5. Aufl. C.H. Beck, München
Höffe O (2023) Lexikon der Ethik, 8. Aufl. C.H. Beck, München
Hoffman T, Baker J (2023) Navigating our way through a hospital ransomware attack: ethical considerations in delivering acute orthopaedic care. J Med Ethics 49:121–124. https://doi.org/10.1136/medethics-2021-107876
Institute of Medicine (2012) Health IT and patient safety—Building safer systems for better care. National Academies Press, Washington
Jabin S (2024) Operational disruption in healthcare associated with software functionality issue due to software security patching: a case report. Froniters Digit Health 6:1367431. https://doi.org/10.3389/fdgth.2024.1367431
Kell M (2024) Nur eine Frage der Zeit. Tagesschau. https://www.tagesschau.de/inland/gesellschaft/cybersicherheit-krankenhaeuser-100. Zugegriffen: 4. Sept. 2025
Kempermann P, Rosenfeld J (2023) EuGH urteilt zur Haftung und Schadensersatz bei Cyberangriffen. https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/eugh-urteilt-zur-haftung-und-schadensersatz-bei-cyberangriffen. Zugegriffen: 4. Sept. 2025
Kma Online (2024) So geht es nach dem Hackerangriff in Frankfurt weiter. Thieme. https://www.kma-online.de/aktuelles/it-digital-health/detail/wie-es-nach-dem-hackerangriff-in-frankfurt-weitergeht-51376. Zugegriffen: 4. Sept. 2025
Koch M-C (2024) Cybervorfälle treffen Krankenhäuser in Deutschland, Kroatien und den USA. https://www.heise.de/news/Cybervorfaelle-treffen-Krankenhaeuser-in-Deutschland-Kroatien-und-den-USA-9785020. Zugegriffen: 4. Sept. 2025
Kühling J, Buchner B (2024) Datenschutz-Grundverordnung, 4. Aufl. C.H. Beck, München
Lackner K, Kühl K, Heger M (2025) Strafgesetzbuch Kommentar, 31. Aufl. C.H. Beck, München
Lorenz W-D, Finlayson D, Wehrs K (2022) KH-IT-Frühjahrstagung 2022, Kreativen Mehrwert schaffen in smarten Krankenhäusern. Krankenhaus-IT Journal, 2. Ausgabe. https://www.krankenhaus-it.de/shop/downloads/kh_it_2_22.pdf. Zugegriffen: 4. Sept. 2025
Müller P, Chamera V, Bodenstein M (2024) Datensicherung als Teil der IT- und Cybersecurity. Springer, Wiesbaden
Nadeborn D, Dittrich T (2022) Cybersicherheit in Krankenhäusern – Teil 1: IT-Compliance als Leitungsaufgabe. Int Cybersecur Law Rev 3:147–161. https://doi.org/10.1365/s43439-022-00049-8
National Audit Office (2025) Wanna Cry cyber attack and the NHS. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs.%20Gesehen%204.%20September%202025. Zugegriffen: 4. Sept. 2025
Oswald J, Goedereis K (2019) Voraussetzungen und Potenziale des digitalen Krankenhauses. In: Krankenhaus Report, S 49–66 https://doi.org/10.1007/978-3-662-58225-1_4
Peters K (2022) Cyberkriminalität im aktuellen Strafrecht. Cyberkriminalität. https://epub.ub.uni-muenchen.de/92172/1/Peters_Cyberkriminalitaet.pdf#page=7. Zugegriffen: 4. Sept. 2025
Pfenninger EG, Schmidt SA, Rohland C (2023) Resilienz gegen IT-Angriffe an Kliniken. Anaesthesiologie 72:852–862. https://doi.org/10.1007/s00101-023-01331-y
Potsdam (2023) Pressemitteilung Nr. 137 vom 30. März 2023. IT-Systeme der Landeshauptstadt wieder vollständig online. https://www.potsdam.de/de/137-it-systeme-der-landeshauptstadt-wieder-vollstaendig-online. Zugegriffen: 4. Sept. 2025

PwC (2023) Digitalisierung im Krankenhaus – Kosten und Nutzen in Theorie und Praxis. https://www.pwc.de/de/gesundheitswesen-und-pharma/krankenhaeuser/studie-digitalisierung-im-krankenhaus.html. Zugegriffen: 4. Sept. 2025
Rawls J (1977) Gerechtigkeit als Fairneß. Karl Alber, Freiburg
Rengier R (2025) Strafrecht Allgemeiner Teil: Strafrecht AT, 17. Aufl. C.H. Beck, München
Segawa S (2020) Der Respekt vor Autonomie. In: Segawa S. Der Begriff der Person in der biomedizinischen Ethik. Brill, Leiden, S 123–143
Strassmann J (2025) DSGVO-Bussgeld. https://www.datenschutz.org/dsgvo-bussgeld. Zugegriffen: 4. Sept. 2025
Weber M (1919) Politik als Beruf. Duncker & Humbolt, München
William R (2020) The untold story of a cyberattack, a hospital and a dying woman. https://www.wired.com/story/ransomware-hospital-death-germany/. Zugegriffen: 4. Sept. 2025
Winder D (2020) The University of California pays $ 1 million ransom following cyber attack. Forbes. https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/. Zugegriffen: 4. Sept. 2025