VDE Positionspapier

Vernetzte und intelligente Medizintechnik als Treiber eines modernen Gesundheitssystems

by VDE DGBMT

VDE

Empfohlene Zitierweise
VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.:
VDE Positionspapier, Vernetzte und intelligente Medizintechnik als Treiber eines modernen Gesundheitssystems, Offenbach am Main, April 2026

Dieses Positionspapier ist Arbeitsergebnis des VDE ITG Beirats „Qualifizierung HealthCare“ und dem VDE DGBMT Fachausschuss „Geschäftsmodelle Intelligenter Assistenzsysteme“

Sprecherteam:
Christina Rode-Schubert; ORANGE itb GmbH; Walldorf
Prof. Dr.-Ing. Kurt Becker; APOLLON Hochschule der Gesundheitswirtschaft GmbH; Bremen
Dipl.-Ing. Johannes Dehm; Digital eHealth Management; Freigericht

Autoren:
Torsten Anstädt; Care for Innovation – Innovation pflegen e.V.; Berlin
Prof. Dr.-Ing. Kurt Becker; APOLLON Hochschule der Gesundheitswirtschaft GmbH; Bremen
Bernhard Calmer; Sankt Wolfgang
Prof. Dr. Dr. Michael Czaplik; Docs in Clouds TeleCare GmbH; Aachen
Prof. Dr.-Ing. Petra Friedrich; Hochschule für angewandte Wissenschaften Kempten
Dr. Michael Hübschen; MH-Institut für Transformation und Innovation im Gesundheitswesen; Berlin
Andreas Kumbroch; adesso SE; Dortmund
Dr. Michael Meyer; Deutsche Gesellschaft für Integrierte Versorgung e.V. (DGIV); Berlin
Dr. Katherina Ruwwe-Glösenkamp; Hoffnungstaler Stiftung Lobetal; Bernau
Dr. David Schmoldt; smart medication eHealth Solutions GmbH; Frankfurt
Prof. Dr.-Ing. Jan-Niklas Voigt-Antons; University of Applied Sciences Hamm-Lippstadt
Peter Weber; Deutsche Telekom Healthcare; Bonn
Prof. Dr. Dietmar Wolff; FINSOZ – Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e.V.; Hochschule Hof

Redaktion
Dr. Thomas Becks
Deutsche Gesellschaft für Biomedizinische Technik (DGBMT) im VDE
thomas.becks@vde.com

Vorbemerkung
VDE Positionspapiere geben – entsprechend der Positionierung des VDE als neutraler, technisch-wissenschaftlicher Verband – gemeinsame Erkenntnisse der jeweiligen Arbeitsgruppen wieder. Die Gemeinschaftsergebnisse werden im konstruktiven Dialog aus häufig unterschiedlichen Positionen erarbeitet. Die Studien spiegeln daher nicht unbedingt die Meinung der durch ihre Mitarbeiterinnen und Mitarbeiter vertretenen Unternehmen und Institutionen wider.

Herausgeber:
VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Deutsche Gesellschaft für Biomedizinische Technik im VDE (VDE DGBMT)
Merianstraße 28
63069 Offenbach am Main
Tel. +49 69 6308-279
dgbmt@vde.com
www.vde.com/dgbmt

Titelbild: © yuriy_klochan / 123

Juni 2026

Inhalt

Executive Summary

Die Digitalisierung des Gesundheitswesens steht an einem Wendepunkt. Während administrative Prozesse zunehmend digitalisiert werden, bleibt das Potenzial vernetzter Medizintechnik in der klinischen Versorgung weitgehend ungenutzt. Dabei verfügen moderne Medizingeräte über die Fähigkeit, kontinuierlich hochwertige Vital-, Bild- und Sensordaten zu erfassen, lokal vorzuverarbeiten und zunehmend auch KI[1]-gestützt zu interpretieren. Diese Daten bilden die Grundlage für eine präzisere, schnellere und sicherere Patientenversorgung – vorausgesetzt, sie können interoperabel, sicher und kontextbezogen genutzt werden.

Zwei zentrale Anwendungsszenarien verdeutlichen das Potenzial: Erstens ermöglicht die kontinuierliche Überwachung von Vitalparametern eine frühzeitige Erkennung kritischer Zustände wie Sepsis, kardiale Dekompensation oder Ateminsuffizienz. KI gestützte Analysen identifizieren Muster und Abweichungen vom individuellen Patientenbaseline und priorisieren Alarme, wodurch Reaktionszeiten verkürzt und Komplikationen reduziert werden. Zweitens eröffnen adaptive Therapie- und Rehabilitationssysteme neue Möglichkeiten der personalisierten Versorgung. Neuroprothesen, Functional Electrical Stimulation (FES) Systeme oder Closed Loop Stimulationsverfahren passen Therapieparameter in Echtzeit an physiologische Veränderungen an und verbessern so Funktionalität, Therapieeffizienz und Patientenzufriedenheit.

Trotz dieser Potenziale ist die Einführung vernetzter Medizintechnik in Krankenhäusern bislang fragmentiert. Technische Heterogenität, fehlende Interoperabilität, organisatorische Trennlinien zwischen Medizintechnik und IT, Fachkräftemangel sowie unklare Verantwortlichkeiten erschweren Integration und Betrieb. Hinzu kommen regulatorische Anforderungen, Haftungsfragen und fehlende klinische Evidenz für KI basierte Anwendungen. Die Folge sind Insellösungen, lange Integrationszeiten und eine geringe Skalierung erfolgreicher Pilotprojekte.

Um Medizintechnik als Treiber der Digitalisierung zu etablieren, müssen Hersteller, Krankenhäuser und Politik gemeinsam handeln. Hersteller sollten offene, standardkonforme Schnittstellen (z. B. [HL7-FHIR], [SDC], [DIN EN ISO/IEEE 11073]), semantische Interoperabilität und robuste Security Lifecycle Prozesse bereitstellen. Krankenhäuser benötigen klare Digitalisierungsstrategien, Governance Strukturen, modulare Integrationsarchitekturen und gezielte Qualifizierungsmaßnahmen. Gemeinsame Pilotprojekte, standardisierte Testumgebungen und vertragliche Klarheit zu Updates, Security und Haftung sind entscheidend für eine erfolgreiche Skalierung.

Die Politik spielt eine zentrale Rolle, indem sie interoperabilitätsorientierte Rahmenbedingungen schafft, Investitionen in digitale Infrastruktur fördert und regulatorische Klarheit für KI basierte Medizinprodukte sicherstellt. Förderprogramme sollten stärker auf Interoperabilität, Standardisierung und nachhaltige Betriebsmodelle ausgerichtet werden. Gleichzeitig müssen Qualifizierungsprogramme für Medizintechnik, IT, Pflege und klinisches Personal ausgebaut werden, um die digitale Transformation im Versorgungsalltag zu verankern.

Ein besonderer Fokus liegt auf der elektronischen Patientenakte (ePA). Für das Ziel „ePA für alle“ müssen Krankenhäuser in Netz- und Serverinfrastruktur, FHIR Schnittstellen, Geräteadapter, Integrationsprojekte, Datenschutz und Schulungen investieren. Realistische Amortisationszeiträume liegen bei 6–36 Monaten, abhängig von IT Reifegrad, Prozessoptimierung und Abrechnungsgewinnen. Pilotprojekte mit klaren KPIs[2] – etwa zur Reduktion redundanter Diagnostik oder zur Beschleunigung der Entlassprozesse – können die ROI[3]-Zeit deutlich verkürzen.

Medizintechnikhersteller sind technisch grundsätzlich in der Lage, hochwertige Daten bereitzustellen. Die größten Lücken liegen jedoch in der Anwendung von einheitlichen standardisierten Schnittstellen, semantischer Konsistenz, Security Lifecycle Management und klinischer Validierung. Hersteller, die diese Lücken systematisch schließen, schaffen nicht nur Mehrwert für Kliniken, sondern reduzieren Integrationsaufwand, Supportkosten und Haftungsrisiken – und erhöhen damit die Marktakzeptanz ihrer Produkte.

Das Fazit ist eindeutig:

Vernetzte und intelligente Medizintechnik kann ein zentraler Treiber eines modernen, datengetriebenen Gesundheitssystems sein. Voraussetzung ist jedoch ein koordiniertes Vorgehen aller Akteure. Werden Interoperabilität, Sicherheit, klinische Evidenz und organisatorische Strukturen konsequent adressiert, lassen sich aus der vorhandenen technischen Dichte transparente, klinisch wirksame Versorgungsprozesse entwickeln. Medizintechnik wird damit nicht nur Teil der Digitalisierung, sondern ihr entscheidender Motor.

1 KI – Künstliche Intelligenz

2 KPI – Key Performance Indicator, auf Deutsch: Leistungskennzahl oder Schlüsselkennzahl

3 ROI – Return of Invest, auf Deutsch: Kapitalrendite, Investitionsrendite oder Wirtschaftlichkeit einer Investition

Impuls

1. Motivation

Die Digitalisierung des Gesundheitswesens befindet sich an einem entscheidenden Wendepunkt. Während administrative Prozesse in den vergangenen Jahren zunehmend digitalisiert wurden, bleibt die klinische Versorgung in vielen Bereichen von analogen Abläufen, fragmentierten Systemlandschaften und fehlender Interoperabilität geprägt. Gleichzeitig steigen die Anforderungen an Qualität, Effizienz und Sicherheit der Versorgung kontinuierlich. Demografischer Wandel, Fachkräftemangel, zunehmende Multimorbidität und wirtschaftlicher Druck führen dazu, dass bestehende Versorgungsmodelle an ihre Grenzen stoßen. Vor diesem Hintergrund gewinnt die Frage an Bedeutung, wie digitale Technologien – insbesondere vernetzte und intelligente Medizintechnik – dazu beitragen können, die Versorgung nachhaltig zu verbessern.

Medizintechnik nimmt eine besondere Rolle ein, da sie unmittelbar am Patienten eingesetzt wird und kontinuierlich klinisch relevante Daten erzeugt. Diese Daten bilden die Grundlage für moderne, datengetriebene Versorgungsprozesse: Sie ermöglichen die frühzeitige Erkennung kritischer Zustände, unterstützen klinische Entscheidungen, verbessern die Steuerung therapeutischer Maßnahmen und eröffnen neue Möglichkeiten der personalisierten Medizin. Moderne Medizingeräte sind heute in der Lage, Vital-, Bild- und Sensordaten nicht nur zu erfassen, sondern auch lokal vorzuverarbeiten, Ereignisse zu erkennen und zunehmend KI-gestützt zu interpretieren. Damit entsteht ein enormes Potenzial, klinische Prozesse effizienter, sicherer und präziser zu gestalten.

Gleichzeitig zeigt die Realität in vielen Krankenhäusern ein anderes Bild. Trotz hoher technischer Ausstattung – insbesondere in Intensivstationen und Notaufnahmen – bleibt die Vernetzung von Medizintechnik häufig unvollständig. Geräte unterschiedlicher Hersteller arbeiten mit proprietären Schnittstellen, Daten werden nicht standardisiert übertragen, und klinische IT-Systeme sind oft nicht in der Lage, diese Informationen interoperabel zu verarbeiten. Die Folge sind Insellösungen, redundante Dokumentation, ineffiziente Arbeitsabläufe und ein eingeschränkter Nutzen der vorhandenen Technologie. Hinzu kommen organisatorische Barrieren, etwa die Trennung von Medizintechnik und IT, fehlende Projektressourcen, unklare Verantwortlichkeiten und ein Mangel an qualifiziertem Personal für Integration, Cybersecurity und Datenmanagement.

Vor diesem Hintergrund ist es notwendig, Medizintechnik nicht nur als technische Komponente, sondern als strategischen Baustein der digitalen Transformation zu verstehen. Vernetzte und intelligente Medizintechnik kann ein zentraler Treiber eines modernen Gesundheitssystems sein – vorausgesetzt, Interoperabilität, Sicherheit, klinische Validierung und organisatorische Voraussetzungen werden konsequent adressiert. Die Digitalisierung der Versorgung gelingt nur, wenn Medizintechnik, klinische IT, Prozesse und Personal gemeinsam betrachtet werden.

Dieses Positionspapier verfolgt daher drei Ziele: Erstens zeigt es anhand konkreter Szenarien auf, wie vernetzte Medizintechnik die Patientenversorgung verbessern kann. Zweitens analysiert es die technischen, organisatorischen und regulatorischen Hemmnisse, die einer breiten Einführung im Weg stehen. Drittens formuliert es konkrete Handlungsempfehlungen für Hersteller, Krankenhäuser und politische Entscheidungsträger, um die Digitalisierung der klinischen Versorgung nachhaltig voranzutreiben.

Die zentrale Botschaft lautet:

Medizintechnik kann weit mehr sein als eine Komponente der Digitalisierung – sie kann ihr Motor sein. Damit dieses Potenzial gehoben werden kann, müssen alle Akteure gemeinsam handeln. Interoperabilität, Anwendungsregeln, klinische Evidenz und robuste Sicherheitsmechanismen sind dabei ebenso entscheidend wie Governance-Strukturen, Qualifizierung und nachhaltige Investitionen. Nur wenn diese Voraussetzungen erfüllt sind, lassen sich aus der vorhandenen technischen Dichte echte, klinisch wirksame, datengetriebene Versorgungsprozesse entwickeln.

2. Vernetzte und intelligente Medizintechnik als Treiber eines modernen Gesundheitssystems

Vernetzte und intelligente Medizintechnik bildet das Rückgrat eines modernen, datengetriebenen, nachhaltigen Gesundheitssystems. Sie verbindet die physische Patientenversorgung mit digitalen Informationsflüssen und ermöglicht damit eine neue Qualität klinischer Entscheidungsfindung. Während Medizingeräte traditionell als isolierte Mess- oder Therapieeinheiten betrachtet wurden, entwickeln sie sich zunehmend zu integralen Bestandteilen digitaler Versorgungsarchitekturen. Diese Entwicklung wird durch drei zentrale Funktionsdimensionen geprägt: Medizingeräte als Datenquellen, als

Vorverarbeitungseinheiten und als Aktuatoren innerhalb klinischer Regelkreise.

Medizingeräte als Datenquellen

Moderne Medizingeräte erfassen kontinuierlich oder ereignisgesteuert klinisch relevante Messwerte wie Vitalparameter, Beatmungs- und Infusionsdaten, Bilddaten oder neurophysiologische Signale. Diese Daten bilden die Grundlage für Befundung, Trendanalysen, klinische Entscheidungsunterstützung und Gestaltung der Patientenversorgung. Entscheidend ist dabei nicht nur die Messgenauigkeit, sondern auch die Qualität der Metadaten: Zeitstempel, Geräte-IDs, Messkontexte und Kalibrierungsinformationen sind notwendig, um Daten korrekt zu speichern, zu interpretieren und in klinische Prozesse einzubetten. Gut strukturierte, standardisierte Datenquellen ermöglichen darüber hinaus die nachgelagerte Nutzung für Qualitätsmanagement, Forschung und Versorgungsoptimierung.

Medizingeräte als Vorverarbeitungseinheiten

Viele Geräte führen bereits heute lokale Vorverarbeitungsschritte durch, darunter Signalfilterung, Artefaktentfernung, Ereigniserkennung, Datenkompression und erste Alarmlogik. Diese Vorverarbeitung reduziert Latenzen, entlastet zentrale IT-Systeme und liefert klinisch verwertbare Ereignisse statt roher Messreihen. Durch die lokale Analyse können kritische Zustände schneller erkannt und priorisiert werden, was insbesondere in zeitkritischen Situationen wie Sepsis, kardialer Dekompensation oder Störung der Atmungsfunktion (respiratorische Insuffizienz) entscheidend ist. Gleichzeitig verbessert die Vorverarbeitung die Datenqualität und schafft die Grundlage für robuste, interoperable Informationsflüsse.

Medizingeräte als Aktuatoren

Neben der Datenerfassung übernehmen Medizingeräte zunehmend aktive Rollen in der Therapie und Pflege. Sie steuern Beatmungsparameter, Dosierungen, Stimulationsimpulse oder Rehabilitationsprogramme und reagieren damit direkt auf physiologische Veränderungen des Patienten. Diese Aktuatorfunktion ist ein wesentlicher Baustein für geschlossene Regelkreise, die kurze Reaktionszeiten und eine hohe Präzision ermöglichen. Beispiele sind adaptive Beatmungssteuerungen, Closed-Loop-Stimulationssysteme in der Neurologie oder KI-gestützte Rehabilitationsgeräte, die Bewegungsmuster analysieren und Trainingsprogramme dynamisch anpassen.

Medizingeräte mit eingebetteter KI als Treiber der Digitalisierung

Mit der Integration eingebetteter KI entwickeln sich Medizingeräte zu aktiven Treibern digitaler Versorgungsprozesse zum Wohle der Patienten. Edge-Analytics ermöglicht die lokale Auswertung großer Datenmengen in Echtzeit und reduziert die Notwendigkeit, sensible Rohdaten an zentrale Systeme zu übertragen. Adaptive Regelkreise nutzen lokale Modelle, um Therapien dynamisch an physiologische Veränderungen anzupassen. Beispiele hierfür sind automatische Beatmungsanpassungen, adaptive Neurostimulation oder individualisierte Rehabilitationssteuerung. Diese Systeme erhöhen Effizienz und Reaktionsgeschwindigkeit, setzen jedoch voraus, dass KI-Modelle klinisch validiert, erklärbar und sicherheitszertifiziert sind. Zudem müssen Mechanismen für Modell-Updates, Monitoring und Interoperabilität mit klinischen IT-Systemen vorhanden sein.

Strategische Bedeutung für das Gesundheitssystem

Vernetzte und intelligente Medizintechnik kann die Versorgung nicht nur verbessern, sondern strukturell verändern. Sie ermöglicht eine präzisere Diagnostik, frühere Interventionen, effizientere Ressourcennutzung und eine bessere Patientenversorgung. Gleichzeitig schafft sie die Grundlage für neue Versorgungsmodelle, etwa telemedizinische Überwachung, KI-gestützte Entscheidungsunterstützung oder personalisierte Therapiepfade. Damit wird Medizintechnik zu einem zentralen Treiber der Digitalisierung – vorausgesetzt, Interoperabilität, Standards und klinische Validierung werden konsequent umgesetzt.

3. Ausgangssituation

Die Ausgangssituation im deutschen Gesundheitswesen ist geprägt von einer paradoxen Konstellation: Einerseits verfügen viele Krankenhäuser über eine hohe technische Ausstattung, insbesondere in Intensivstationen und Notaufnahmen. Moderne Beatmungsgeräte, Monitoring-Systeme, Infusionspumpen, bildgebende Verfahren und neurotechnische Geräte sind flächendeckend vorhanden und liefern kontinuierlich hochwertige Daten. Andererseits gelingt es bislang nur selten, diese Daten systematisch zu vernetzen, interoperabel zu nutzen und in klinische Entscheidungsprozesse einzubetten. Die Folge ist ein erheblicher Verlust an Effizienz, Qualität und Sicherheit, obwohl die technischen Voraussetzungen grundsätzlich vorhanden wären – was letztlich zulasten des Patientenwohls geht und die bestmögliche Versorgung der Patient*innen erschwert.

Diese Diskrepanz hat mehrere Ursachen. Technisch betrachtet sind viele Geräte nicht standardisiert angebunden, nutzen proprietäre Protokolle oder liefern Daten in uneinheitlichen Formaten. Organisatorisch bestehen häufig getrennte Verantwortlichkeiten zwischen Medizintechnik und IT, was zu Reibungsverlusten, unklaren Zuständigkeiten und ineffizienten Betriebsmodellen führt. Personell fehlt es an Fachkräften, die sowohl klinische als auch technische Expertise vereinen. Regulatorisch erschweren Haftungsfragen, Cybersecurity-Anforderungen und komplexe nationale Zertifizierungsprozesse die Einführung neuer digitaler Lösungen. Wirtschaftlich wiederum stehen Krankenhäuser unter hohem Kostendruck, wodurch Investitionen in digitale Infrastruktur oft nachrangig behandelt werden.

Zusätzlich spielt die ökonomische Perspektive der Krankenhäuser eine zentrale Rolle. Investitions- und Betriebsentscheidungen werden zunehmend unter Kosten-Nutzen-Gesichtspunkten getroffen, sodass Prioritäten nicht mehr ausschließlich durch technische oder medizinische Anforderungen bestimmt werden, sondern maßgeblich durch die jeweils erwartete Wirtschaftlichkeit. Diese Ausrichtung kann bestehende Schnittstellenprobleme weiter verstärken – insbesondere dann, wenn unterschiedliche Bereiche ihre Maßnahmen primär an aktuelle Budgetvorgaben und Effizienzkennzahlen orientieren, anstatt ganzheitliche und integrierte Lösungsansätze zu verfolgen.

Gleichzeitig steigt der Bedarf an datengetriebenen Versorgungsmodellen kontinuierlich. Die zunehmende Komplexität der Patientenversorgung, der Fachkräftemangel und die Notwendigkeit, Prozesse effizienter zu gestalten, machen digitale Unterstützungssysteme unverzichtbar. Frühwarnsysteme, KI-gestützte Entscheidungsunterstützung, telemedizinische Überwachung und adaptive Therapien können dazu beitragen, die Versorgung zu stabilisieren und Personal zu entlasten. Doch ohne interoperable Datenflüsse bleiben diese Potenziale ungenutzt.

Die Ausgangssituation lässt sich wie folgt zusammenfassen:

Die technische Basis ist vorhanden, aber die strukturellen, organisatorischen und regulatorischen Voraussetzungen für eine flächendeckende Vernetzung fehlen. Medizintechnik ist heute vielerorts ein „digitaler Rohdiamant" – wertvoll, aber nicht geschliffen. Um ihr Potenzial zu heben, müssen Interoperabilität, harmonisierte Standards, Governance und Qualifizierung konsequent adressiert werden.

3.1 Voraussetzungen für die Vernetzung

Eine erfolgreiche Vernetzung von Medizintechnik setzt mehrere technische, organisatorische und regulatorische Voraussetzungen voraus. Technisch ist eine robuste digitale Infrastruktur erforderlich, die stabile Netzwerke, ausreichende Server- und Speicherkapazitäten sowie sichere Kommunikationswege umfasst. Redundante LAN- und WLAN-Strukturen, VLAN-Segmentierung, Quality-of-Service-Mechanismen (QoS) und Zero-Trust-Architekturen (ZTA) bilden die Grundlage für eine **sichere und performante Datenübertragung.** Ohne diese Basis können selbst modernste Geräte ihre Daten nicht zuverlässig bereitstellen.

Ein zweiter zentraler Baustein ist die **Interoperabilität.** Sie umfasst sowohl syntaktische als auch semantische Aspekte. Syntaktische Interoperabilität bedeutet, dass Daten über standardisierte Schnittstellen wie HL7 FHIR oder DIN EN ISO/IEEE 11073 (SDC) übertragen werden. Semantische Interoperabilität stellt sicher, dass die Bedeutung der Daten eindeutig ist – etwa durch die Nutzung von LOINC[4]-Codes für Messgrößen oder SNOMED-CT-Konzepten[5] für klinische Befunde. Ohne semantische Konsistenz bleiben Daten zwar technisch übertragbar, aber klinisch nicht verwertbar.

Darüber hinaus sind klare **Metadatenstrukturen** erforderlich. Zeitstempel, Geräte-IDs, Messkontexte, Kalibrierungsinformationen und Einheiten müssen entsprechend den harmonisierten DIN EN Standards genutzt werden, damit Daten korrekt interpretiert werden können. Dies ist insbesondere für KI-gestützte Analysen und Closed-Loop-Systeme entscheidend, da diese auf konsistenten, hochwertigen Daten basieren.

Organisatorisch müssen **Verantwortlichkeiten** klar definiert sein. Die Trennung zwischen Medizintechnik und IT ist in vielen Häusern historisch gewachsen, aber für vernetzte Systeme nicht mehr zeitgemäß. Gemeinsame Governance-Strukturen, abgestimmte Betriebsmodelle und definierte Rollen für Updates, Security, Incident-Management und Validierung sind notwendig, um vernetzte Medizintechnik sicher zu betreiben.

Regulatorisch müssen Datenschutz, Cybersecurity und Haftungsfragen berücksichtigt werden. Die Verarbeitung sensibler Gesundheitsdaten erfordert transparente Einwilligungsprozesse, sichere Datenhaltung und dokumentierte Sicherheitsmaßnahmen. Cybersecurity-Anforderungen wie Verschlüsselung, Authentifizierung, Patch-Management und Logging müssen über den gesamten Lebenszyklus eines Geräts gewährleistet sein.

Zusammengefasst:

Vernetzung gelingt nur, wenn technische Standards, organisatorische Strukturen und regulatorische Anforderungen konsequent zusammengedacht und angewendet werden. Ohne diese Voraussetzungen bleibt Medizintechnik isoliert – und ihr Potenzial ungenutzt.

4 LOINC – Logical Observation Identifiers Names and Codes ist ein internationaler Standard, der medizinische Laboruntersuchungen, klinische Messwerte und Beobachtungen eindeutig codiert.

5 SNOMED-CT – Systematized Nomenclature of Medicine – Die heute relevante Version heißt SNOMED-CT (Clinical Terms) bezeichnet eine der weltweit umfassendsten klinischen Terminologien für Diagnosen, Befunde, Prozeduren und medizinische Konzepte.

3.2 Situation der Medizintechnikhersteller

Medizintechnikhersteller verfügen heute über leistungsfähige Geräte, die hochwertige Sensordaten liefern und zunehmend über Netzwerk- und API[6]-Funktionen verfügen. Dennoch variiert der Reifegrad erheblich zwischen Herstellern und Geräteklassen. Während einige Anbieter bereits offene Schnittstellen, standardisierte Datenmodelle und robuste Security-Mechanismen implementieren, setzen andere weiterhin auf proprietäre Protokolle und geschlossene Systeme. Diese Heterogenität erschwert die Integration in klinische IT-Landschaften erheblich.

Ein zentrales Problem ist die **Uneinheitlichkeit der Schnittstellen.** Viele Geräte unterstützen zwar Netzwerkkommunikation, jedoch nicht auf Basis offener Standards wie FHIR oder DIN EN ISO/IEEE 11073 (PoC). Stattdessen kommen proprietäre Formate zum Einsatz, die individuelle Adapter, Middleware oder Mapping-Tabellen erfordern. Dies erhöht den Integrationsaufwand, verlängert Projektlaufzeiten und führt zu höheren Betriebskosten.

Ein weiteres Defizit betrifft die **semantische Interoperabilität.** Selbst wenn Daten übertragen werden können, fehlt häufig eine einheitliche semantische Beschreibung. Messgrößen, Einheiten, Messkontexte oder Geräteparameter sind zwar standardisiert, aber nicht umgesetzt, was die klinische Interpretation erschwert. Für KI-basierte Anwendungen ist dies besonders kritisch, da sie auf konsistenten Datenmodellen basieren müssen.

Auch im Bereich **Cybersecurity und Lifecycle-Management** bestehen Unterschiede. Während einige Hersteller regelmäßige Sicherheitsupdates, Telemetrie-Funktionen und dokumentierte Patch-Prozesse anbieten, sind andere noch nicht ausreichend auf die Anforderungen vernetzter Systeme vorbereitet. Dies führt zu Sicherheitsrisiken und erschwert den klinischen Betrieb.

Schließlich ist die **klinische Validierung** ein zentraler Engpass. KI-basierte Funktionen, Closed-Loop-Systeme und adaptive Algorithmen erfordern robuste Evidenz, transparente Modelle und nachvollziehbare Entscheidungslogiken. Viele Geräte verfügen jedoch noch nicht über validierte End-to-End-Workflows, was die Akzeptanz im klinischen Alltag reduziert.

6 API – Application Programming Interface ist eine standardisierte Programmierschnittstelle, über die Software-Systeme miteinander kommunizieren können. Sie definiert klar, welche Funktionen, Daten und Endpunkte ein System bereitstellt und wie andere Programme darauf zugreifen dürfen.

Zusammengefasst:

Hersteller stehen damit vor der Herausforderung, ihre Produkte nicht nur technisch, sondern auch organisatorisch und regulatorisch auf die Anforderungen eines vernetzten Gesundheitssystems auszurichten. Wer frühzeitig in Interoperabilität, Security und klinische Validierung investiert, wird langfristig Wettbewerbsvorteile erzielen.

3.3 Herausforderungen in Krankenhäusern

Krankenhäuser stehen vor einer Vielzahl von Herausforderungen, die die Einführung vernetzter Medizintechnik erschweren. Technisch sind viele Häuser durch heterogene Systemlandschaften geprägt: Geräte unterschiedlicher Hersteller, proprietäre Schnittstellen, fragmentierte Middleware und unzureichende Netzwerkinfrastrukturen führen zu hohen Integrationsaufwänden. Ohne den nachhaltigen Nutzen standardisierter Architekturen zu erkennen, entstehen Insellösungen, die nachhaltig schwer zu betreiben und kaum skalierbar sind.

Organisatorisch ist die **Trennung zwischen Medizintechnik und IT** eines der größten Hindernisse. Unterschiedliche Zuständigkeiten, getrennte Budgets und divergierende Arbeitskulturen erschweren die Zusammenarbeit. Für vernetzte Systeme ist jedoch ein gemeinsames Betriebsmodell erforderlich, das klare Rollen für Updates, Security, Incident-Management und Validierung definiert.

Personell fehlt es an **Fachkräften mit kombinierter Expertise** in klinischer Medizintechnik, IT-Architektur, Cybersecurity und Datenintegration. Diese Profile sind auf dem Arbeitsmarkt schwer zu finden, und interne Weiterbildungsprogramme sind oft unzureichend. Der Fachkräftemangel führt dazu, dass Integrationsprojekte verzögert werden oder gar nicht erst beginnen, siehe VDE Positionspapier Gestaltung Digitalisierung im Gesundheitswesen [VDE 2022].

Klinisch bestehen Herausforderungen in der **Workflow-Integration.** Neue Systeme müssen nahtlos in bestehende Abläufe passen, sonst entstehen zusätzliche Belastungen für das Personal. Fehlende Schulungszeit, unzureichendes Change-Management und mangelnde Usability führen dazu, dass digitale Tools trotz Verfügbarkeit nicht genutzt werden. Kliniker fordern zudem nachvollziehbare, klinisch validierte Systeme und klare Verantwortlichkeiten für KI-basierte Entscheidungen.

Regulatorisch erschweren Datenschutz, Cybersecurity-Anforderungen, zusätzliche Konformitätsverfahren der gematik und Haftungsfragen die Einführung ver-

netzter Systeme. Darüber hinaus müssen Krankenhäuser Risikoanalysen durchführen, Validierungsprozesse dokumentieren und Sicherheitsmaßnahmen nachweisen. Diese Anforderungen sind notwendig, aber ressourcenintensiv.

Wirtschaftlich stehen Krankenhäuser unter hohem Kostendruck. Investitionen in digitale Infrastruktur konkurrieren mit akuten Bedarfen wie Personal, Bettenkapazitäten und medizinischer Ausstattung. Ohne klare Finanzierungsmodelle für den Anschub der Digitalisierung und belastbare Business-Cases werden Digitalisierungsprojekte häufig zurückgestellt.

Zusammengefasst:

Krankenhäuser verfügen über die technische Basis, aber nicht über die strukturellen Voraussetzungen für eine flächendeckende Vernetzung. Sie sollten ihre Versorgungsprozesse so gestalten, dass sie dadurch Kosten reduzieren und gleichzeitig nachhaltig Erlöse und Effizienz erhöhen können. Ohne Governance, Ressourcen, Transformation der DIN EN-Standards und Qualifizierung bleibt Medizintechnik/IT isoliert – und ihr Potenzial entlang der gesamten Wertschöpfungskette ungenutzt.

4. Handlungsempfehlungen

Die Digitalisierung der klinischen Versorgung kann nur gelingen, wenn alle beteiligten Akteure – Hersteller, Krankenhäuser, Selbstverwaltung und Politik – koordiniert handeln. Die Herausforderungen sind komplex und betreffen technische, organisatorische, regulatorische und wirtschaftliche Dimensionen. Entsprechend müssen die Handlungsempfehlungen ganzheitlich gedacht werden. Ziel ist es, die Voraussetzungen für interoperable, sichere und klinisch wirksame digitale Versorgungsprozesse zu schaffen und gleichzeitig die wirtschaftliche Tragfähigkeit für die Selbstverwaltung, Krankenhäuser und Hersteller sicherzustellen.

Ein zentraler Erfolgsfaktor ist die konsequente Ausrichtung auf Interoperabilität. Ohne den Einsatz DIN EN standardisierter Schnittstellen, semantische Konsistenz und klare Datenmodelle bleibt Medizintechnik isoliert. Hersteller müssen DIN EN Standards implementieren, während Krankenhäuser Interoperabilität als Beschaffungsanforderung verankern müssen. Die Politik wiederum sollte verbindliche Rahmenbedingungen schaffen, die Anwendung der Standards fördern und proprietäre Insellösungen unattraktiv machen.

Ein zweiter Schwerpunkt liegt auf Governance und Organisation. Krankenhäuser benötigen interdisziplinäre Strukturen, die Medizintechnik, IT, Datenschutz, Recht und klinische Fachbereiche zusammenführen. Hersteller müssen ihre Support- und Integrationsmodelle professionalisieren und stärker auf gemeinsame Pilotprojekte setzen. Die Politik sollte Governance-Modelle fördern, die Verantwortlichkeiten klar definieren und Haftungsfragen adressieren.

Drittens ist Cybersecurity ein unverzichtbarer Bestandteil vernetzter Medizintechnik. Hersteller müssen Security-by-Design[7], Patch-Management und Telemetrie über den gesamten Produktlebenszyklus gewährleisten. Krankenhäuser benötigen robuste Netzwerke, Zero-Trust-Architekturen und klare Prozesse für Incident-Management. Die Politik sollte Mindeststandards definieren und deren Umsetzung fördern.

Viertens ist klinische Validierung entscheidend, insbesondere für KI-basierte Anwendungen. Hersteller müssen End-to-End-Workflows validieren, Erklärbarkeit sicherstellen und klinische Studien unterstützen. Krankenhäuser sollten Pilotprojekte durchführen, die klinische Endpunkte messen und Ergebnisse transparent kommunizieren. Die Politik kann durch Förderprogramme und regulatorische Klarheit unterstützen.

Schließlich ist Qualifizierung ein zentraler Erfolgsfaktor. Krankenhäuser benötigen Schulungen, Super-User[8]-Programme und kontinuierliche Weiterbildung. Hersteller sollten praxisnahe Trainings, Testumgebungen und Integrations-Kits bereitstellen. Die Politik sollte Qualifizierungsprogramme für Medizintechnik, IT und Pflege fördern.

4.1 Für Hersteller

Hersteller spielen eine zentrale Rolle bei der Digitalisierung der klinischen Versorgung. Ihre Produkte bilden die technische Grundlage für Datenflüsse, Entscheidungsunterstützung und adaptive Therapien. Um Medizintechnik als Treiber der Digitalisierung zu etablieren, müssen Hersteller ihre Entwicklungs-, Support- und Integrationsstrategien konsequent auf Interoperabilität, Sicherheit und klinische Wirksamkeit ausrichten.

Ein erster Schwerpunkt liegt auf offenen, standardkonformen Schnittstellen. Hersteller sollten HL7 FHIR für klinische Daten und Dokumente sowie DIN EN ISO/IEEE 11073 für bidirektionale Gerätekommunikation implementieren und Device Data Models unterstützen, um gerätespezifische Semantik zu standardisieren. Offene, dokumentierte APIs, Webhooks und Developer-Portale

7 Security-by-Design ist ein Cybersecurity und Systementwicklungsprinzip, bei dem Sicherheit von Anfang an fest in die Architektur eines Systems eingebaut wird – nicht erst nachträglich durch Patches oder Zusatzmaßnahmen.

8 Super-User wird in IT, Software Administration und auch in klinischen Anwendungen als Rolle verwendet, wenn bestimmte Personen mehr Befugnisse haben als normale Nutzer.

Abb. 4.1: Die Handlungsempfehlungen für Medizintechnik-Hersteller, Krankenhäuser und Politik auf einen Blick

mit Beispiel-Requests, SDKs[9] und Fehlercodes erleichtern die Integration erheblich.

Ein zweiter Schwerpunkt ist die semantische Interoperabilität. Hersteller sollten Messgrößen und Befunde auf LOINC und SNOMED-CT mappen und Mapping-Tabellen bereitstellen. Standardisierte FHIR-Ressourcen wie Observation, Device und DeviceMetric sollten vollständig implementiert und dokumentiert werden. Kontextinformationen wie Geräte-ID, Firmware-Version, Kalibrierungsstatus und Zeitstempel müssen konsistent übertragen werden.

Drittens müssen Hersteller Security-by-Design umsetzen. Dazu gehören Secure Boot, Verschlüsselung in Transit[10] und at Rest[11], Authentifizierung (z. B. Mutual TLS (mTLS[12]), O-Auth2[13]), rollenbasierte Zugriffskontrollen und Telemetrie für Health-Monitoring. Patch-Management-Prozesse müssen klar definiert sein, einschließlich Notfall-Patches und End-of-Life-Kommunikation.

Ein vierter Schwerpunkt ist die klinische Validierung. Hersteller sollten klinische Studien unterstützen, die den Nutzen vernetzter Funktionen belegen. Für KI-basierte Funktionen müssen Erklärbarkeits-Mechanismen bereitgestellt werden, etwa Konfidenzwerte, Entscheidungsgrenzen und Dokumentation der Trainingsdaten. Validierte End-to-End-Workflows erhöhen die Akzeptanz bei klinischen Anwendern.

Fünftens sollten Hersteller Integrations-Kits, Sandbox-Umgebungen und Referenzimplementierungen bereitstellen. Diese Werkzeuge reduzieren Integrationsaufwand, beschleunigen Projekte und erleichtern

9 Ein Software Development Kit (SDK) ist ein Werkzeugkasten für Entwickler, der meist Compiler, Debugger, Beispielcode und oft auch APIs enthält, um Anwendungen schneller und standardisiert zu entwickeln.

10 In-Transit-Verschlüsselung bezeichnet den Schutz von Daten während sie zwischen Geräten, Diensten oder Netzwerkknoten übertragen werden. Ziel ist es, Vertraulichkeit und Integrität sicherzustellen – also dass niemand mitlesen oder Daten verändern kann.

11 Die Verschlüsselung von Data-at-Rest schützt sie vor negativen Folgen wie Datenschutzverletzungen, unbefugtem Zugriff und physischem Diebstahl. Ohne den Schlüssel sind die Daten unbrauchbar.

12 Mutual TLS steht für mutual Transport Layer Security und beschreibt ein Verfahren, bei dem beide Kommunikationspartner – Client und Server – ihre Identität mittels digitaler Zertifikate nachweisen. Das Ergebnis ist eine gegenseitige Vertrauensprüfung.

13 OAuth2 – Open Authorization 2 ist ein internationaler Standard, der es Anwendungen ermöglicht, im Namen eines Nutzers sicher auf geschützte Ressourcen zuzugreifen – ohne dass Passwörter weitergegeben werden müssen.

die Zusammenarbeit mit Kliniken und Integratoren. Zertifizierte Interoperabilitätsmodule und veröffentlichte Testreports schaffen Vertrauen und Transparenz.

Schließlich sollten Hersteller gemeinsame Pilotprojekte mit Kliniken durchführen. Diese Piloten sollten klar abgegrenzte Use-Cases, definierte KPIs und transparente Evaluationsprozesse umfassen. Beispiele für KPIs sind Alarmreduzierung, Zeit bis zur Intervention, Integrationszeit oder klinische Endpunkte.

Hersteller, die frühzeitig in Interoperabilität, Security und klinische Validierung investieren, werden langfristig Wettbewerbsvorteile erzielen und die Digitalisierung der Versorgung maßgeblich vorantreiben.

4.2 Für Krankenhäuser

Krankenhäuser stehen im Zentrum der digitalen Transformation der Versorgung. Sie müssen vernetzte Medizintechnik nicht nur beschaffen, sondern auch sicher betreiben, in klinische Workflows integrieren und nachhaltig weiterentwickeln. Um dies zu erreichen, sind strategische, organisatorische und technische Maßnahmen erforderlich.

Ein erster Schritt ist die Entwicklung einer verbindlichen Digitalisierungsstrategie. Diese sollte klare Ziele, KPIs und einen mehrjährigen Investitionsplan umfassen. Beispiele für KPIs sind Reduktion von Notfallverlegungen, verkürzte Reaktionszeiten, geringere Dokumentationsaufwände oder ROI-Kennzahlen. Eine solche Strategie schafft Orientierung und Priorisierung.

Zweitens benötigen Krankenhäuser interdisziplinäre Governance-Strukturen. Ein Lenkungsgremium aus Medizin, Pflege, Medizintechnik, IT, Datenschutz und Recht sollte Prioritäten, Budgets und Verantwortlichkeiten steuern. Dies verhindert Insellösungen und fördert eine koordinierte Umsetzung.

Drittens sollten Krankenhäuser Interoperabilität als Beschaffungsstandard verankern. Ausschreibungen sollten verbindliche Anforderungen an HL7 FHIR, DIN EN ISO/IEEE 11073, semantische Modelle und Testnachweise enthalten. Geräte ohne standardkonforme Schnittstellen sollten nicht mehr beschafft werden.

Viertens ist eine modulare Integrationsarchitektur erforderlich. Eine robuste Middleware[14] sollte standardisierte DIN EN ISO/IEEE Geräte-Daten, pseudonymisieren und an klinische Systeme (HL7 FHIR, DICOM) verteilen. Dadurch entsteht eine durchgängige Interoperabilitätsschicht. Redundante Netzsegmente, Quality-of-Service-Mechanismen und Zero-Trust-Prinzipien erhöhen Sicherheit und Stabilität.

Fünftens müssen Krankenhäuser Schulungen und Change-Management priorisieren. Zeitlich gestaffelte Trainings, Super-User-Programme und kontinuierliche Feedback-Schleifen sind notwendig, um Akzeptanz und Nutzung sicherzustellen. Kliniker sollten frühzeitig in Anforderungsdefinition, Usability-Tests und Pilotphasen eingebunden werden.

Sechstens sollten Krankenhäuser Pilotprojekte mit messbaren klinischen Endpunkten durchführen. Diese Piloten sollten klar abgegrenzte Use-Cases umfassen, etwa digitale Einweisung-/Entlassprozesse, Telemonitoring oder KI-gestützte Frühwarnsysteme. Ergebnisse sollten transparent kommuniziert und in Skalierungsstrategien überführt werden.

Schließlich müssen Krankenhäuser Cybersecurity und Datenschutz systematisch adressieren. Dazu gehören Risikoanalysen, Dokumentation von Validierungs- und Testprozessen, sichere Einwilligungsmechanismen und Incident-Response-Prozesse.

Krankenhäuser, die diese Maßnahmen umsetzen, schaffen die Grundlage für eine ökonomische, skalierbare, sichere und klinisch wirksame digitale Infrastruktur.

4.3 Für Hersteller und Krankenhäuser gemeinsam

Die Digitalisierung der klinischen Versorgung kann nur gelingen, wenn Hersteller und Krankenhäuser eng zusammenarbeiten. Viele Herausforderungen – etwa Interoperabilität, Validierung, Workflow-Integration oder Security – lassen sich nur gemeinsam lösen. Daher sind kooperative Modelle, gemeinsame Pilotprojekte und abgestimmte Betriebsprozesse entscheidend.

Ein zentraler Ansatz sind gemeinsame Integrationspiloten. Hersteller, Klinik-IT und Medizintechnik sollten gemeinsam Tests in realen Umgebungen durchführen. Diese Piloten sollten definierte Use-Cases, klare KPIs und strukturierte Evaluationsprozesse umfassen. Beispiele für KPIs sind Alarmreduzierung, Zeit bis zur Intervention, Integrationszeit oder klinische Endpunkte.

Ein weiterer Schwerpunkt ist die vertragliche Klarheit. Verträge sollten Verantwortlichkeiten für Updates, Cybersecurity-Patches, Interoperabilitätstests und Haftungsfragen eindeutig regeln. Dies schafft Planungssicherheit und reduziert Risiken.

Hersteller sollten Integrations-Kits, Testumgebungen und zertifizierte Schnittstellen bereitstellen, während Krankenhäuser standardisierte Integrationsprozesse etablieren sollten. Gemeinsame Testumgebungen, Abnahmeprotokolle und Validierungsprozesse beschleunigen Integration und erhöhen Sicherheit.

Ein weiterer wichtiger Aspekt ist die gemeinsame Entwicklung von Datenmodellen, Alarmstrategien und Workflow-Designs. Kliniker sollten aktiv in die Gestaltung von Benutzeroberflächen, Alarmpriorisierung und Entscheidungsunterstützung eingebunden werden. Hersteller profitieren von praxisnahem Feedback, wäh-

14 Middleware ist eine Software-Schicht zwischen Betriebssystem und Anwendungen, die dafür sorgt, dass verschiedene Programme oder Dienste reibungslos miteinander kommunizieren können.

rend Krankenhäuser Systeme erhalten, die besser in den klinischen Alltag passen.

Schließlich sollten Hersteller und Krankenhäuser gemeinsame Schulungs- und Qualifizierungsprogramme entwickeln. Hersteller können praxisnahe Trainings, Super-User-Programme und technische Dokumentation bereitstellen, während Krankenhäuser interne Multiplikatoren ausbilden.

Diese kooperative Vorgehensweise schafft die Grundlage für nachhaltige, skalierbare und klinisch wirksame digitale Versorgungsprozesse.

4.4 Für die Politik

Die Politik spielt eine zentrale Rolle bei der Digitalisierung des Gesundheitswesens. Sie kann durch regulatorische Rahmenbedingungen, Förderprogramme und die Anwendung von Standards durch die gematik maßgeblich beeinflussen, wie schnell und wie erfolgreich vernetzte Medizintechnik in der Versorgung ankommt.

Ein erster Schwerpunkt liegt auf Interoperabilität als politischem Leitprinzip. Die Politik sollte verbindliche Standards fördern und proprietäre Insellösungen unattraktiv machen. FHIR, und DIN EN ISO/IEEE 11073 sollten als Mindestanforderungen für vernetzte Medizintechnik etabliert werden. Förderprogramme sollten Interoperabilität als Voraussetzung definieren.

Zweitens sollte die Politik Investitionen in digitale Infrastruktur fördern. Krankenhäuser benötigen Mittel für Netzwerke, Server, Middleware, Cybersecurity und Schulungen. Förderprogramme sollten langfristig angelegt sein und nicht nur punktuelle Projekte unterstützen.

Drittens ist regulatorische Klarheit für KI-basierte Medizinprodukte erforderlich. Die Politik sollte Leitlinien für Explainability, Validierung, Monitoring und Haftung entwickeln. Dies schafft Sicherheit für Hersteller und Anwender.

Viertens sollte die Politik die Umsetzung vorhandener Qualifizierungsprogramme fördern (z. B. Lernmanagementplattformen). Medizintechnik, IT, Pflege und klinisches Personal benötigen kontinuierliche Weiterbildung, um digitale Systeme sicher zu betreiben.

Schließlich sollte die Politik Anreizsysteme für digitale Transformation schaffen. Krankenhäuser, die Interoperabilität, Standardisierte und digitale Prozesse erfolgreich umsetzen, sollten finanziell profitieren.

Die Politik kann damit entscheidend dazu beitragen, dass vernetzte Medizintechnik ihr Potenzial entfaltet und die Versorgung nachhaltig verbessert.

5. Fazit

Die Digitalisierung des Gesundheitswesens steht an einem entscheidenden Punkt: Die technischen Möglichkeiten sind vorhanden, die klinischen Potenziale sind klar erkennbar, und der Bedarf an datengetriebenen Versorgungsmodellen steigt kontinuierlich. Gleichzeitig zeigt die Realität, dass vernetzte Medizintechnik in vielen Krankenhäusern noch nicht flächendeckend genutzt wird. Die Gründe dafür sind vielfältig – technische Heterogenität, organisatorische Trennlinien, fehlende Interoperabilität, unzureichende Ressourcen, regulatorische Unsicherheiten und wirtschaftliche Restriktionen. Dennoch ist das Potenzial so groß, dass ein entschlossenes, koordiniertes Vorgehen aller Akteure nicht nur sinnvoll, sondern zwingend notwendig ist.

Medizintechnik kann weit mehr sein als eine Komponente der Digitalisierung. Sie kann ihr **Treiber** sein. Moderne Geräte erfassen kontinuierlich hochwertige Daten, verarbeiten diese lokal vor und übernehmen zunehmend aktive Rollen in der Therapie. Mit eingebetteter KI entstehen neue Möglichkeiten der Frühwarnung, Entscheidungsunterstützung und adaptiven Therapie. Diese Entwicklungen können die Versorgung sicherer, effizienter und präziser machen – vorausgesetzt, die Daten sind interoperabel, sicher und klinisch validiert.

Damit dieses Potenzial gehoben werden kann, müssen mehrere Voraussetzungen erfüllt sein. **Erstens ist Interoperabilität der zentrale Schlüssel.** Ohne offene Schnittstellen, semantische Konsistenz und standardisierte Datenmodelle bleiben Geräte isoliert und ihr Nutzen begrenzt. Hersteller müssen konsequent auf Standards wie FHIR, und DIN EN ISO/IEEE 11073 setzen, während Krankenhäuser Interoperabilität als Beschaffungsanforderung verankern müssen. Die Politik wiederum sollte verbindliche Rahmenbedingungen schaffen, die proprietäre Insellösungen unattraktiv machen.

Zweitens ist Governance entscheidend. Krankenhäuser benötigen interdisziplinäre Strukturen, die Medizintechnik, IT, Datenschutz, Recht und klinische Fachbereiche zusammenführen. Hersteller müssen ihre Support- und Integrationsmodelle professionalisieren und stärker auf gemeinsame Pilotprojekte setzen. Die Politik sollte Governance-Modelle fördern, die Verantwortlichkeiten klar definieren und Haftungsfragen adressieren.

Drittens ist Cybersecurity ein unverzichtbarer Bestandteil vernetzter Medizintechnik. Hersteller müssen Security-by-Design, Patch-Management und Telemetrie über den gesamten Produktlebenszyklus gewährleisten. Krankenhäuser benötigen robuste Netzwerke, Zero-Trust-Architekturen und klare Prozesse für Incident-Management. Die Politik sollte Mindeststandards definieren und deren Umsetzung fördern.

Viertens ist klinische Validierung entscheidend, insbesondere für KI-basierte Anwendungen. Hersteller müssen End-to-End-Workflows validieren, Explainability sicherstellen und klinische Studien unterstützen. Krankenhäuser sollten Pilotprojekte durchführen, die klinische Endpunkte messen und Ergebnisse transparent kommunizieren. Die Politik kann durch Förderprogramme und regulatorische Klarheit unterstützen.

Fünftens ist Qualifizierung ein zentraler Erfolgsfaktor. Krankenhäuser benötigen Schulungen, Super-User-Programme und kontinuierliche Weiterbildung. Hersteller sollten praxisnahe Trainings, Testumgebungen und Integrations-Kits bereitstellen. Die Politik sollte Qualifizierungsprogramme für Medizintechnik, IT und Pflege fördern, siehe VDE Positionspapier Gestaltung der Digitalisierung im Gesundheitswesen.

Schließlich müssen **wirtschaftliche Rahmenbedingungen** geschaffen werden, die Investitionen in digitale Infrastruktur ermöglichen. Die Einführung der elektronischen Patientenakte (ePA) zeigt, dass Investitionen in Netzwerke, Schnittstellen, Geräteadapter, Cybersecurity und Schulungen notwendig sind, sich aber innerhalb von 6–36 Monaten amortisieren können – insbesondere wenn Pilotprojekte klar definierte KPIs verfolgen und Prozessoptimierungen konsequent umgesetzt werden.

Das übergeordnetes Fazit lautet:

Vernetzte und intelligente Medizintechnik ist ein zentraler Treiber eines modernen, datengetriebenen Gesundheitssystems. Sie kann die Versorgung sicherer, effizienter und patientenzentrierter machen. Sie kann Personal entlasten, Prozesse stabilisieren und klinische Ergebnisse verbessern. Doch dieses Potenzial entfaltet sich nur, wenn Interoperabilität, Sicherheit, klinische Evidenz und organisatorische Strukturen konsequent adressiert werden. Die Digitalisierung der Versorgung ist kein technisches Projekt, sondern ein struktureller Wandel – und Medizintechnik ist sein Motor.

6. Literatur

[DIN EN ISO/IEEE 11073] IEEE 11073 (DIN ISO 690) International Organization for Standardization; Institute of Electrical and Electronics Engineers. DIN EN ISO/IEEE 11073 10101:2020 – Health informatics — Point-of-care medical device communication — Part 10101: Nomenclature. Geneva: ISO; New York: IEEE, 2020. Verfügbar unter: www.iso.org/standard/70943.html (Zugriff am: 28. März 2026).

[HL7-FHIR] Health Level Seven International (HL7). FHIR Release 5: Fast Healthcare Interoperability Resources – Specification. Ann Arbor, MI: HL7 International, 2023. Verfügbar unter: https://hl7.org/fhir/ (Zugriff am: 28. März 2026).

[LOINC] Regenstrief Institute [Hrsg.] (2023): LOINC® Version 2.77: Logical Observation Identifiers Names and Codes. Indianapolis: Regenstrief Institute. Verfügbar unter: https://loinc.org (Zugriff am: 28. 03. 2026).

[mTLS] Rescorla, E. (2018): The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force (IETF). Verfügbar unter: https://www.rfc-editor.org/rfc/rfc8446 (Zugriff am: 28. 03. 2026).

[OAuth2] Hardt, D. (Hrsg.) (2012): The OAuth 2.0 Authorization Framework (RFC 6749). Internet Engineering Task Force (IETF). Verfügbar unter: https://www.rfc-editor.org/rfc/rfc6749 (Zugriff am: 28. 03. 2026).

[SDC] International Organization for Standardization; Institute of Electrical and Electronics Engineers. ISO/IEEE 11073 20702:2023 – Health informatics — Point-of-care medical device communication — Part 20702: Service-oriented Device Connectivity (SDC). Geneva: ISO; New York: IEEE, 2023. Verfügbar unter: https://www.iso.org/standard/80704.html (Zugriff am: 28. März 2026).

[SNOMED-CT] SNOMED International [Hrsg.] (2024): SNOMED CT® International Edition – January 2024 Release. London: SNOMED International. Verfügbar unter: https://www.snomed.org/snomed-ct (Zugriff am: 28. 03. 2026).

[VDE 2022] VDE Positionspapier Gestaltung Digitalisierung im Gesundheitswesen

7. Glossar

Aktuator Ein Aktuator ist ein technisches Bauteil, das Signale in mechanische Arbeit umsetzt. Er führt das aus, was ein Regler oder Algorithmus vorgibt – z. B. eine Bewegung, eine Druckänderung oder eine Dosierung.

API Application Programming Interface – eine standardisierte Programmierschnittstelle, über die Software-Systeme miteinander kommunizieren können. Sie definiert klar, welche Funktionen, Daten und Endpunkte ein System bereitstellt und wie andere Programme darauf zugreifen dürfen.

At-Rest Die Verschlüsselung von Data-at-Rest schützt sie vor negativen Folgen wie Datenschutzverletzungen, unbefugtem Zugriff und physischem Diebstahl. Ohne den Schlüssel sind die Daten unbrauchbar.

Closed Loop Ein Closed Loop System ist ein Regelkreis, der automatisch misst, entscheidet und eingreift, ohne dass ein Mensch jeden Schritt manuell steuern muss. Es ist also ein selbstregulierendes System, das kontinuierlich Rückmeldungen (Feedback) nutzt, um seine eigene Wirkung anzupassen.

Dicom Digital Imaging and Communications in Medicine ist ein internationaler Standard, der sowohl Dateiformate als auch Kommunikationsprotokolle definiert, sodass medizinische Bilder und zugehörige Metadaten zuverlässig, vollständig und herstellerübergreifend ausgetauscht werden können.

Edge Edge Analytics bedeutet, dass Daten direkt am Entstehungsort („am Edge“) analysiert werden, also auf dem Gerät selbst, in einem Sensor, einem Medizingerät, einem Gateway oder einem lokalen Edge Server – statt die Daten erst in eine zentrale Cloud zu übertragen.

ePA Elektronische Patientenakte

FES Functional Electrical Stimulation ist ein medizinisch-therapeutisches Verfahren, bei dem gezielte elektrische Impulse genutzt werden, um Muskeln künstlich zu aktivieren, die der Patient selbst nicht oder nicht ausreichend ansteuern kann.

FHIR FHIR Release 5 – Fast Healthcare Interoperability Resources

gematik Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH ist die zentrale Organisation, die in Deutschland die Telematikinfrastruktur (TI) verantwortet.

HL7 Health Level Seven International (HL7) – Organisation und gleichzeitig eine Familie internationaler Standards, die den Austausch medizinischer Informationen regeln

IEEE Institute of Electrical and Electronics Engineers ist eine weltweit agierende technische Fachorganisation, die Standards, Forschung, Fachpublikationen und technische Communities koordiniert und weiterentwickelt.

In-Transit In Transit Verschlüsselung bezeichnet den Schutz von Daten während sie zwischen Geräten, Diensten oder Netzwerkknoten übertragen werden. Ziel ist es, Vertraulichkeit und Integrität sicherzustellen – also dass niemand mitlesen oder Daten verändern kann.

ISO International Organization for Standardization

IT Informationstechnik

KI Künstliche Intelligenz

KPI Key Performance Indicator, auf Deutsch: Leistungskennzahl oder Schlüsselkennzahl

LAN Local Area Network – Ein LAN ist ein räumlich begrenztes Computernetzwerk, das Geräte innerhalb eines Gebäudes oder Campus miteinander verbindet – z. B. in einer Klinik, einem Labor, einer Station oder einem Büro.

Logging Bezeichnet die automatische Erstellung von Protokollen (Logs) über Systemereignisse, Fehlermeldungen, Status- und Prozessmeldungen und sicherheitsrelevante Vorgänge. Diese Informationen werden typischerweise chronologisch und mit Zeitstempeln gespeichert.

LOINC Logical Observation Identifiers Names and Codes ist ein internationaler Standard, der medizinische Laboruntersuchungen, klinische Messwerte und Beobachtungen eindeutig codiert.

Middleware Middleware ist eine Software-Schicht zwischen Betriebssystem und Anwendungen, die dafür sorgt, dass verschiedene Programme oder Dienste reibungslos miteinander kommunizieren können.

mTLS Mutual TLS steht für mutual Transport Layer Security und beschreibt ein Verfahren, bei dem beide Kommunikationspartner – Client und Server – ihre Identität mittels digitaler Zertifikate nachweisen. Das Ergebnis ist eine gegenseitige Vertrauensprüfung.

OAuth2 Open Authorization 2 ist ein internationaler Standard, der es Anwendungen ermöglicht, im Namen eines Nutzers sicher auf geschützte Ressourcen zuzugreifen – ohne dass Passwörter weitergegeben werden müssen.

QoS Quality-of-Service-Mechanismen stehen für technische Verfahren, die den Datenverkehr in Netzwerken priorisieren, steuern und absichern, damit wichtige Anwendungen zuverlässig funktionieren. Gerade in Kliniken und vernetzten Medizintechnik Umgebungen sind QoS Mechanismen essenziell, weil sie sicherstellen, dass kritische Datenströme (z. B. Alarme, Vitaldaten, SDC Kommunikation) immer Vorrang haben.

ROI Return of Invest, auf Deutsch: Kapitalrendite, Investitionsrendite oder Wirtschaftlichkeit einer Investition

SDK Ein Software Development Kit (SDK) ist ein Werkzeugkasten für Entwickler, der meist Compiler, Debugger, Beispielcode und oft auch APIs enthält, um Anwendungen schneller und standardisiert zu entwickeln.

SDC Service-oriented Device Connectivity ist ein internationaler Interoperabilitätsstandard aus der ISO/IEEE-11073-Familie und wurde speziell für die sichere, echtzeitfähige und bidirektionale Vernetzung von Medizingeräten am Point of Care entwickelt.

Security-by-Design Security by Design ist ein Cybersecurity- und Systementwicklungsprinzip, bei dem Sicherheit von Anfang an fest in die Architektur eines Systems eingebaut wird – nicht erst nachträglich durch Patches oder Zusatzmaßnahmen.

Semantisch „Semantisch“ bezieht sich auf die Bedeutung von Sprache, Daten oder Symbolen – also was etwas inhaltlich meint, nicht wie es aufgebaut ist.

SNOMED-CT Systematized Nomenclature of Medicine – Die heute relevante Version heißt SNOMED-CT (Clinical Terms) bezeichnet eine der weltweit umfassendsten klinischen Terminologien für Diagnosen, Befunde, Prozeduren und medizinische Konzepte.

Super-User Der Begriff wird in IT, Software Administration und auch in klinischen Anwendungen verwendet, wenn bestimmte Personen mehr Befugnisse haben als normale Nutzer.

Syntaktisch „Syntaktisch“ steht für die Ebene der Struktur, Anordnung und Form von Sprache oder Daten – also wie Elemente miteinander verknüpft sind, nicht was sie bedeuten.

VLAN Virtual Local Area Network – Ein ein logisch getrenntes Teilnetz innerhalb eines physischen Netzwerks. Mehrere Geräte können also im gleichen physischen LAN sein, aber virtuell in unterschiedlichen Netzwerken arbeiten.

WLAN Wireless Local Area Network – Ein WLAN ist ein lokal begrenztes Funknetz, das Geräte ohne Kabel miteinander verbindet – typischerweise über Wi Fi Technologie.

ZTA Zero-Trust-Architekturen stehen für ein IT Sicherheitsmodell, das auf dem Grundsatz basiert: „Never trust, always verify.“ Das bedeutet: Kein Gerät, keine Anwendung, kein Nutzer und kein Datenpaket wird automatisch als vertrauenswürdig eingestuft – auch nicht innerhalb des Krankenhaus LANs.

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e. V.
Merianstr. 28
63069 Offenbach am Main

Tel. +49 69 6308-0
Fax +49 69 6308-9865
info@vde.com
www.vde.com

VDE