



# Regulatorische Anforderungen an Lösungen der künstlichen Intelligenz im Gesundheitswesen

# 8

Ludwig Pechmann, Martin Mildner, Tim Suthau und Martin Leucker

## Inhaltsverzeichnis

8.1 Einleitung: Künstlichen Intelligenz im Gesundheitswesen .....	176
8.2 Grundlagen .....	178
8.3 Regulatorischer Umgang mit KI-gestützten Medizinprodukten .....	187
8.4 Schlussbetrachtung .....	195
Literatur .....	196

### Zusammenfassung

Diese Arbeit befasst sich mit dem Thema künstliche Intelligenz (KI) im Gesundheitswesen. Der Fokus liegt dabei auf dem aktuellen Stand der Normen und deren Anwendung hinsichtlich des Themas Zulassung von KI-gestützten Medizinprodukten. Dafür wird soweit in das Thema KI eingeführt, dass die Besonderheiten von KI als Software und die Unterschiede zwischen adaptiven, selbstlernenden und nicht adaptiven, nicht selbstlernenden Systemen ersichtlich werden. Zudem werden die

L. Pechmann (✉) · M. Mildner · T. Suthau  
UniTransferKlinik Lübeck GmbH, Lübeck, Deutschland  
E-Mail: [lpechmann@unitransferklinik.de](mailto:lpechmann@unitransferklinik.de)

M. Mildner  
E-Mail: [martin.mildner@unitransferklinik.de](mailto:martin.mildner@unitransferklinik.de)

T. Suthau  
E-Mail: [suthau@unitransferklinik.de](mailto:suthau@unitransferklinik.de)

M. Leucker  
Institut für Software Engineering und Programmiersprachen, Universität zu Lübeck, Lübeck,  
Deutschland  
E-Mail: [leucker@isp.uni-luebeck.de](mailto:leucker@isp.uni-luebeck.de)

verfügbaren (harmonisierten) Normen genannt und der Zulassungsprozess im Allgemeinen beschrieben. Dabei wird eine grobe Einführung in den Zulassungsprozess von Medizinprodukten gegeben, um die Problematik mit KI-gestützten Medizinprodukten und im Speziellen mit adaptiven KI-gestützten Medizinprodukten verstehen und nachvollziehen zu können. Anhand einiger Beispiele soll gezeigt werden, inwieweit die Zulassung von nicht adaptiven KI-gestützten Medizinprodukten unter Zuhilfenahme der verfügbaren Normen aussehen könnte. Ebenfalls soll ein Ausblick auf die bevorstehenden Aufgaben bei der Zulassung von adaptiven KI-gestützten Medizinprodukten erfolgen.

---

## 8.1 Einleitung: Künstlichen Intelligenz im Gesundheitswesen

Das Feld der Medizintechnik unterliegt einem starken Wandel. Dies wird zum Beispiel offensichtlich bei Umstellungen, wie z. B. von der Richtlinie 93/42/EWG über Medizinprodukte (MDD) zur Medizinprodukte-Verordnung 2017/745 (MDR), welche mit einem überarbeiteten und umfangreicheren Zulassungsprozess und Überwachung nach dem Inverkehrbringen von Medizinprodukten einhergeht (siehe Johner, 2019, o.S.). Dies fordert nicht nur die Hersteller und Benannten Stellen heraus, die sich an die neuen Gegebenheiten anpassen müssen, sondern auch andere verantwortliche Organe, wie z. B. die Europäische Kommission. Diese ist für die Umsetzung der Europäischen Datenbank für Medizinprodukte EUDAMED (siehe Europäischer Markt, o. D.), einer Datenbank, die zur Überwachung und Erreichung von Transparenz über die auf dem europäischen Markt zugelassenen Medizinprodukte etabliert werden soll, verantwortlich. Das Ziel der Umstellung auf die MDR und von Gesetzen und Normen im Allgemeinen ist die Steigerung der Patientensicherheit und natürlich auch die Sicherheit der Anwender. Es sollen alle Risiken bedacht und minimiert werden, die zu einem Schaden oder sogar zum Tode führen könnten. Zudem soll über Transparenz Vertrauen in die Produkte sowie den Hersteller sowohl bei den Ärzten als auch bei den Patienten geschaffen werden.

Aber auch in anderen Domänen der Medizin ist ein Wandel zu erkennen. Die Medizin kommt aus einer stark durch handwerkliches Vorgehen geprägten Domäne. Individuelle Erfahrungen eines Mediziners oder Chirurgen sowie ein Stück weit die Vorlieben und Tradition waren seit jeher der Grundstein für Diagnosen und Behandlungen. Der technologische Fortschritt erlaubt es nun, nicht nur schneller eine Diagnose zu stellen, sondern die Diagnosen werden aufgrund von gewonnenen Erkenntnissen und neuen Sichtweisen präziser. So kann ein Augenarzt mithilfe der optischen Kohärenztomografie (Optical Coherence Tomography, OCT) in die Retina eines Patienten „schauen“ und so den Fortschritt einer altersbedingten Makuladegeneration (AMD) befunden (vgl. Lenzen-Schulte, 2019, S. 146–149). Die Untersuchung dauert nur ein paar Minuten und der Patient muss dafür nur in das OCT-Gerät blicken.

Mit der Technologisierung hält die künstliche Intelligenz (KI) Einzug in die Medizin. Ärzte und Patienten profitieren gleichermaßen dadurch, dass das KI-gestützte Medizinprodukt Handlungsempfehlungen auf Grundlage einer systematischen Datenerfassung aus allen Domänen und Einflussgrößen vergleichbarer Prozeduren und Fälle ausspricht. Die Nutzung fallbezogener Daten aus allen verfügbaren relevanten Domänen erlaubt die kontextbezogene Unterstützung und die Prädiktion des Vorgehens. Dies beinhaltet die Vorhersage von Restlaufzeiten zur Erleichterung der Planung und des Ressourceneinsatzes genauso wie die patientenspezifische Simulation für den Einsatz von Roboter- und Assistenzsystemen. Naheliegend ist die Nutzung kontextbezogener Informationen zur Verbesserung der Benutzungsfreundlichkeit der Systeme und zur Verhinderung redundanter Handlungen. Somit können die Sicherheit, die Qualität und die Effizienz der Versorgung entscheidend verbessert werden.

Dies bedeutet für den MedizinproduktHersteller nicht nur den offensichtlichen Wandel, wie z. B. die Medizinprodukte-Verordnung, zu bewältigen, sondern ebenfalls den der Technologisierung. Für die Bewältigung der zukünftigen Herausforderungen sind Datenverfügbarkeit und Analyse von sehr heterogenen multimodalen Daten notwendig. Somit ist der Zugang zu qualitativ hochwertigen Daten in großem Umfang erforderlich, die sowohl den Prozess der Patientenversorgung als auch die Ergebnisse der Patienten dokumentieren. Erste Ansätze zum Aufbau und zur Nutzung solcher Plattformen finden sich bspw. bei:

- HighMED (siehe Konsortium HiGHmed, [2020](#)),
- openEHR (siehe openEHR User Group, [2018](#)).

Um den Übergang von der evidenzbasierten zur wissensbasierten datengesteuerten Medizin zu vollziehen, müssen o. g. Verfahrensdaten mit anderen heterogenen Patientendaten und Prozessdaten analysiert werden. Dies betrifft beispielsweise Daten der Genetik, Biomarker, Demografie und der prä- und intraoperativen Bildgebung. Weitere Themen in diesem Zusammenhang sind unter anderem Vernetzung und Interoperabilität inklusive Standardisierung, IoT, Cyber Security und Remote Service, um nur einige der Felder zu nennen. Die Umsetzung all dieser Themen zur zukünftigen Erfüllung des Bedarfs der Anwender ist (aber nicht ausschließlich) mithilfe der Methoden der künstlichen Intelligenz denkbar.

Dabei nimmt das Machine Learning (ML) als ein Teilbereich der KI eine besondere Rolle ein. Beim ML wird ausgehend von einer festen (nicht adaptiv) oder kontinuierlich wachsenden (adaptiv) Anzahl von Trainingsdaten eine Funktionalität einmalig bzw. kontinuierlich gelernt und als ggf. sich wandelnde Softwarekomponente in das Medizingerät eingebaut. Hierbei stellt sich die Frage, ob und wie dieses Vorgehen verträglich mit der Zulassung entsprechender Systeme ist.

Dieser Beitrag setzt sich mit der Erstellung und Zulassung von KI-gestützten Medizinprodukten auseinander. Im Folgenden werden dafür der nötige normative Rahmen sowie

die Grundlagen zu Themen wie künstliche Intelligenz und maschinelles Lernen beschrieben. Darauf folgt eine Auseinandersetzung der Probleme, die im Zusammenhang mit der Zulassung von-KI gestützten Medizinprodukten auftreten. Im Speziellen soll dabei zwischen adaptiven und nicht adaptiven KI-gestützten Medizinsystemen unterschieden werden. Schlussendlich folgt ein Ausblick auf zukünftige Tätigkeiten.

---

## **8.2 Grundlagen**

Die regulatorischen Anforderungen an künstliche Intelligenz im Gesundheitswesen entwickeln sich aus den Anforderungen an Medizinprodukte oder im Speziellen an medizinische Software. Dieser Abschnitt bietet einen Einblick in die Zulassungsvoraussetzungen für Medizinprodukte, um diese grundlegenden Anforderungen, die entsprechend auch für KI-Systeme gelten, zu verstehen, und nennt die wichtigsten zu beachtenden Normen. Besonderer Fokus wird dabei auf die Normen IEC 62304 und IEC 82304 gelegt.

### **8.2.1 Regulatorische Anforderungen an Medizinprodukte**

In Europa bildet die Medical Device Regulation (MDR) die Grundlage für die Zulassung von Medizinprodukten. Verschiedene Normen bieten genauere Vorgaben, wie die rechtlichen Forderungen der MDR umgesetzt werden sollen. Bei Normen handelt es sich um von nationalen oder internationalen Standardisierungskommissionen entworfene Dokumente, die den Stand der Technik dokumentieren. Sogenannte harmonisierte Normen wurden durch die EU ausgewählt und veröffentlicht. Sie bilden grundlegende Anforderungen für die gesetzlichen Forderungen. Die Kürzel ISO (International Organisation for Standardization) und IEC (International Electrotechnical Commission) bezeichnen internationale Normen. Die Präfixe EN und DIN kennzeichnen europäische bzw. nationale Normen. Es wird empfohlen, wenn möglich immer mit den europäischen bzw. nationalen Versionen zu arbeiten, da diese häufig Anhänge mit zusätzlichen relevanten Anforderungen enthalten (vgl. Johner, 2020a, o. S.). In dieser Arbeit werden einfachheitshalber aber nur die internationalen Kürzel ISO/IEC verwendet. Unterschieden wird dabei zwischen sogenannten Produktnormen und Prozessnormen. In diesem Beitrag stehen die Prozessnormen im Vordergrund, da diese maßgeblich bei der Zulassung von medizinischer Software Anwendung finden.

Damit ein Unternehmen ein Medizinprodukt in Verkehr bringen kann, muss dieses Produkt eine CE-Kennzeichnung erhalten. Dies erfolgt über ein Konformitätsbewertungsverfahren, welches der MedizinproduktHersteller selbst durchführt. In regelmäßigen Audits wird durch Benannte Stellen geprüft, ob die Entwicklung des Medizinprodukts entsprechend harmonisierten Normen und dem Stand der Technik durchgeführt wird. Als

Nachweis dient das vollständige Qualitätsmanagementsystem, welches der MedizinproduktHersteller anhand der ISO 13485 entwickelt hat. Kann der MedizinproduktHersteller dies in einem Audit glaubhaft belegen, liegt ein Vermutungscharakter vor und der Hersteller darf im Folgenden eine CE-Kennzeichnung auf sein Medizinprodukt anbringen. Die Medizinprodukte werden außerdem in einem aufwendigen Risikomanagementprozess, bei dem sich der MedizinproduktHersteller an den Vorgaben der ISO 14971 orientieren kann, entsprechend ihrem Risiko in verschiedene Klassen (I, IIa, IIb, III) eingeteilt. Das Risikomanagement findet über den gesamten Lebenszyklus des Produktes statt und wird schon parallel bei der Erstellung der Anforderungen angewendet. Auch nach dem Inverkehrbringen werden Fehler sowie Rückmeldungen aus dem Feld auf ihr Risiko bezüglich der Auftretenswahrscheinlichkeit und des Schweregrades des möglichen Schadens betrachtet und lenken so die Aktivitäten des MedizinproduktHerstellers. Dies ist eine vereinfachte und nicht vollständige Darstellung des Zulassungsprozesses, reicht jedoch für die Veranschaulichung der in den folgenden Abschnitten beschriebenen Probleme aus (vgl. Hastenteufel & Renaud, 2019, S. 18, 65).

Die wichtigsten Normen, die bei der Entwicklung von Software berücksichtigt werden müssen, sind in Tab. 8.1 beschrieben. Die Normen IEC 82304 und IEC 62304 wurden speziell für Software bzw. Software als Bestandteil eines Produkts (Embedded Software) entwickelt, wobei IEC 82304 nur bei eigenständiger Software anwendbar ist, und sollen im folgenden Abschnitt näher erläutert werden.

## 8.2.2 Besondere Anforderungen an Software

Bei einem Lebenszyklus eines Produktes handelt es sich um einen Prozess von der Produktidee bis zum Ausscheiden aus dem Markt. Eine Berücksichtigung wird in der MDR auch für medizinische Software verlangt. Wie bereits erwähnt finden die Normen IEC 62304 und IEC 82304 speziell bei der Zulassung von medizinischer Software Anwendung und bedürfen einer besonderen Betrachtung. Beide Normen ergänzen sich dabei und decken verschiedene Anforderungen an die Entwicklung ab. Die IEC 62304 deckt insbesondere die Anforderungen, Architektur und Implementierung von Medizinprodukten mit Software ab und fand bisher Anwendung bei allen Arten von Gesundheitssoftware. Die IEC 82304 beschreibt hingegen die Rahmenbedingungen der vorangestellten Produktanforderungen und der anschließenden Validierung und greift ausschließlich bei eigenständiger Medizinsoftware (Software as a Product). Bei in Medizingeräte eingebetteter Software ist diese Norm nicht anwendbar.

Die Grundlage für die Zulassung einer Gesundheitssoftware bildet, wie auch bei anderen Medizinprodukten, eine Zweckbestimmung, der Intended Use. Die Zweckbestimmung beschreibt eindeutig die Anwendergruppe sowie den bestimmungsgemäßen Gebrauch und gibt so auch die Grenzen des Einsatzgebietes des Medizinproduktes vor. Aus der Zweckbestimmung lassen sich User Stories und daraus Use Cases ableiten, auf die dann die IEC

**Tab. 8.1** Übersicht über Normen. (Quelle: eigene Zusammenstellung 2021)

Norm	Name	Inhalt
DIN EN ISO 13485	Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke	Anforderungen bezüglich Design, Herstellung, Datenschutz und Inverkehrbringen von Medizinprodukten
DIN EN ISO 14155	Klinische Prüfung von Medizinprodukten an Menschen – Gute klinische Praxis	Anforderungen an klinische Studien, basierend auf ethischen und wissenschaftlichen Gesichtspunkten
DIN EN ISO 14971	Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte	Management der Risiken durch den Hersteller; Verfahren, um Gefährdungen erkennen, bewerten und kontrollieren zu können; Anforderungen gelten während des gesamten Lebenszyklus des Medizinprodukts
DIN EN IEC 60601-1	Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale	Anforderungen an die Sicherheit und Ergonomie von medizinisch-elektrischen Geräten
DIN EN IEC 62304	Medizingeräte-Software – Software-Lebenszyklus-Prozesse	Anforderungen an Entwicklung, Wartung, Risikomanagement, Konfigurationsmanagement und Problemlösung speziell bei medizinischer Software
DIN EN IEC 62366-1	Medizinprodukte – Teil 1: Anwendung der Gebrauchstauglichkeit auf Medizinprodukte	Anforderungen an Beschreibung von Nutzungskontext, Nutzer, Patienten und Wirkungsprinzip; Verifizierung und Validierung der Gebrauchstauglichkeit (Usability)
IEC 82304	Health Software	Anforderungen an Stand-alone-Software – so genannte „Health Software“

Diese Tabelle beinhaltet eine Übersicht und kurze Beschreibung des Inhaltes der gültigen Normen auf die ein Medizinproduktehersteller zurückgreifen kann

62366 (Anwendung der Gebrauchstauglichkeit auf Medizinprodukte) angewendet werden kann. Die IEC 62366 fordert einen risikobasierten Ansatz zur Gestaltung von User Interfaces und Produkten mit Fokus auf die Minimierung von Use Errors. Parallel dazu bilden die User Stories sowie Use Cases Eingaben für die ISO 14971.

Aus der Zweckbestimmung sollen nach IEC 82304-1 ebenfalls die Produkthanforderungen abgeleitet werden. Diese Produkthanforderungen sollen unter anderem die Anforderungen an Schnittstellen, IT-Sicherheit, Installation und Dokumentation definieren. Folgende Systemanforderungen spezifizieren die Produkthanforderungen weiter und enthalten genauere Beschreibungen von technischen Schnittstellen, Bedieninterfaces und IT-Sicherheitsmaßnahmen. Diese Systemanforderungen sind mit den Softwareanforderungen von eingebetteten Softwareprodukten durch IEC 62304 vergleichbar. Ein weiterer Bestandteil der IEC 82304-1 ist die Produktvalidierung. Diese Validierung soll feststellen, ob die entwickelte Software die ursprünglichen Produkthanforderungen erfüllt. Auftretende Fehler werden mithilfe des später beschriebenen Problemlösungsprozesses unter IEC 62304 behandelt. Zusätzlich ist bei Änderungen der Software eine Revalidierung des Produkts durchzuführen. Die Norm fordert außerdem eine eindeutige Kennzeichnung der Version des Medizinproduktes, der Unique Device Identification. Mit dieser Kennzeichnung gehen auch entsprechende Dokumente wie Bedienungsanleitung und technische Beschreibung einher.

Die Regularien hinsichtlich der Umsetzung der Software werden durch IEC 62304 geregelt und decken dabei die fünf Kernprozesse des Softwarelebenszyklus ab. Bei den Prozessen handelt es sich unter anderem um Entwicklung, Wartung, Risikomanagement, Konfigurationsmanagement und Problemlösung.

Der Softwareentwicklungsprozess deckt verschiedene Tätigkeiten ab. Hierzu zählen unter anderem:

### **Anforderungsanalyse**

Hier müssen genaue Spezifikationen des späteren Produkts erläutert werden. Hierzu zählen unter anderem die Benutzerschnittstelle, technische Schnittstellen zu anderen Systemen, IT-Sicherheitsmaßnahmen und Risikobeherrschungsmaßnahmen.

### **Softwarearchitektur**

Die Softwarearchitektur muss klar bestimmt und dokumentiert sein. Sie beschreibt den inneren Aufbau eines Systems. Unter anderem müssen verwendete Komponenten der Software und einzelne Schnittstellen bestimmt und deren Zusammenspiel/Abhängigkeit beschrieben werden. Besondere Anforderungen werden dabei an SOUP-Komponenten, Software of Unknown Provenance, gestellt. Hierbei handelt es sich um allgemein verfügbare Software, die nicht speziell für die Integration in das medizinische Gerät entwickelt wurde (vgl. Hastenteufel & Renaud, 2019, S. 83 f.).

### **Implementierung und Verifizierung**

Alle Einheiten, die im Bereich Architektur identifiziert wurden, müssen implementiert und verifiziert werden. Ein bestimmtes Vorgehen bei der Verifizierung wird nicht vorgeschrieben. Möglich ist diese unter anderem mittels dynamischen Unit Testing oder statischer Codereviews.

### **Softwarefreigabe**

Bei einer Softwarefreigabe handelt es sich noch nicht um eine Marktfreigabe. Es handelt sich mehr um einen Abschluss der Entwicklungsarbeit. Bei dieser Freigabe müssen alle verbliebenen Fehler aufgelistet und bewertet werden, Softwareversion bestimmt und dokumentiert werden und alle Unterlagen hinsichtlich Anforderungen, Architektur und Verifizierungstests archiviert werden.

Neben dem Softwareentwicklungsprozess ist auch der Wartungsprozess Bestandteil der IEC 62304. Hier muss vor allem der Umgang mit Feedback geplant werden. Rückmeldungen werden in Form von Probleberichten verwertet. Daraus resultierende Änderungen müssen für die Implementierung den zuvor beschriebenen Softwareentwicklungsprozess durchlaufen.

Im Softwarerisikomanagementprozess wird eine Gefährdungsanalyse mit anschließender Betrachtung und Verifizierung von Maßnahmen zur Risikobeherrschung gefordert. Risikomanagement ist nach ISO 14971 von Anfang an ein Bestandteil der Produktentwicklung. IEC 62304 geht aber zusätzlich auf softwarespezifische Anforderungen an das Risikomanagement und die Überwachung der SOUP ein. Aus dem Risikomanagement leitet sich wieder eine Sicherheitsklasse (Klasse A, B, C) der jeweiligen Software ab, die einen Einfluss auf die Sicherheitsklasse des Medizinproduktes hat (vgl. Johner, 2017, o. S.).

Bei dem vierten Kernprozess handelt es sich um das Konfigurationsmanagement. Kern dieses Prozesses ist die Aufschlüsselung aller Identifikations-, Dokumentations- und Genehmigungsschritte. So soll sichergestellt werden, dass die Software optimal konfiguriert ist.

Abschließend regelt die Norm IEC 62304 auch den Problemlösungsprozess. Probleme, die nach der Freigabe in Zusammenhang mit der Nutzung der Software entstehen, müssen untersucht, dokumentiert und bewertet werden. Ein Problemlösungsprozess soll eine Änderungsanforderung für ein aufgetretenes Problem liefern oder begründen können, warum eine Änderung nicht notwendig ist. Der Fokus des Problemlösungsprozesses liegt somit auf der Einrichtung und dem Betrieb eines Kontrollsystems. Die eigentliche Lösung des Problems ist – anders als der Name vermuten lässt – nicht Gegenstand des Problemlösungsprozesses, sondern des Wartungsprozesses (vgl. Johner, 2020c, o. S.).

### **8.2.3 Einführung künstliche Intelligenz.**

Der Begriff „künstliche Intelligenz“ ist im alltäglichen Sprachgebrauch nicht eindeutig definiert. In der Informatik werden hierunter diverse Technologien und Konzepte zusammengefasst, bei denen Computersysteme menschenähnliches intelligentes Verhalten imitieren, das durch bestimmte Kernkompetenzen wie Wahrnehmung, Verstehen, Handeln und Lernen gekennzeichnet ist (vgl. Wirtz & Weyerer, 2019, S. 4–10.).



## 8.2.4 Was ist Intelligenz – natürlich oder künstlich?

Intelligenz wird oft als kognitive und geistige Leistungsfähigkeit des Menschen bezeichnet. Zu den kognitiven Eigenschaften des Menschen zählen beispielsweise:

- Wahrnehmung und Aufmerksamkeit,
- Erinnerung und Lernen,
- das Problemlösen, Kreativität und Vorstellungskraft,
- das Planen und die Orientierung,
- die Argumentation,
- die Selbstbeobachtung (Introspektion),
- der Wille
- und das Glauben (vgl. Wikipedia, [2020](#), o. S.).

Mindestens Vorstellungskraft, Wille, Glauben und vor allem Kreativität gehören nicht zu den Fähigkeiten einer künstlichen Intelligenz. Insofern ist KI nicht oder nur eingeschränkt intelligent.

Die vermeintliche Intelligenz wird durch Algorithmen (mathematische Zusammenhänge und Berechnungen) unterschiedlichster Herkunft geschaffen. Die Methodiken finden sich hinter solchen Begriffen, wie:

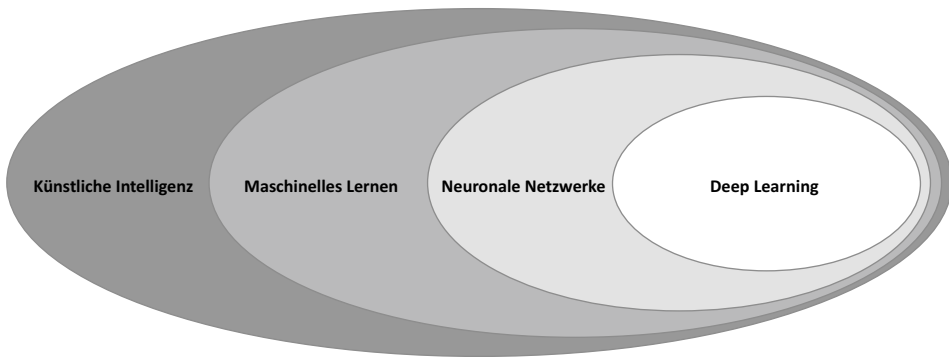
- Data Mining,
- Data Science,
- Statistik,
- maschinelles Lernen,
- neuronale Netze (mathematische Sequenzen).

Diese Methodiken (Berechnungen) werden nun zu künstlichen Intelligenzen, da entsprechende Rechenkapazitäten in Form von Hardware zur Verfügung stehen.

Somit ist die KI weniger in der Lage, den Menschen zu ersetzen, sondern erweitert den Handlungsspielraum des Menschen durch Rechenkapazitäten und Algorithmen um weitere Fähigkeiten.

## 8.2.5 Abgrenzungen innerhalb KI

Wie bereits beschrieben, geht es bei der KI darum, dass mithilfe von Computeralgorithmen bestimmte „kognitive“ Fähigkeiten des Menschen, wie das Lernen von (komplexen) Zusammenhängen, imitiert werden.



**Abb. 8.1** Zusammenhänge verschiedener Begriffe innerhalb von künstlicher Intelligenz. (Quelle: eigene Darstellung 2021)

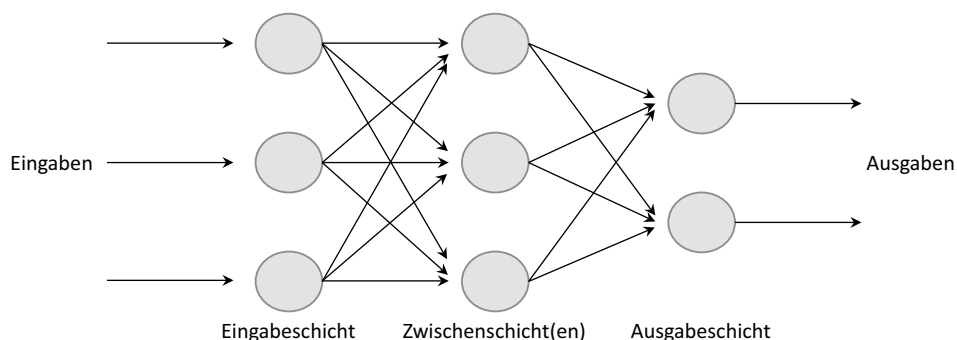
Der „KI-Verständige“ unterscheidet zwischen verschiedenen Methoden, die als Teilmenge immer genauer bezeichnen, welche Verfahren bzw. Techniken angewandt werden (siehe Abb. 8.1).

**Maschinelles Lernen (ML)** Mithilfe von statistischen Berechnungen können Maschinen auf der Grundlage gelernter Zusammenhänge spezifische Aufgaben ausführen. Durch die Erhebung und Sammlung von Daten werden Algorithmen von Computern selbstständig erlernt. Praktisch wird also ein entsprechender Algorithmus nicht von einem Spezialisten entworfen und programmiert, sondern anhand von Trainingsdaten automatisch generiert. Die hier derzeit eingesetzten Verfahren sind z. B.: neuronale Netze, Decision Trees, Bayesian Networks, Support Vector Machines, Logistic Regression und Random Forrest. Befinden sich die Daten in neuen situativen Zusammenhängen, muss dies erkannt und angepasst werden.

**Neuronale Netze (NN)** Neuronale Netze sind Computermodelle im Bereich des maschinellen Lernens, welche der Struktur und Funktionalität des Gehirns nachempfunden sind, diese jedoch nicht konkret nachbilden, sondern über Modellbildung abstrahieren.

Mehrere einfache Neurone (mit häufig sehr einfachen Berechnungen oder Klassifizierungen) verarbeiten Eingangssignale und geben ihr Ergebnis an weitere benachbarte Neurone weiter. Die Anordnung erfolgt in sogenannten Layern. Mithilfe von unterschiedlichen Architekturen der Anordnung dieser Neuronen lassen sich komplexe Sachverhalte lernen.

Die Neuronen befinden sich zwischen den Schichten (Layern) und sind untereinander verbunden, und zwar so, dass ein Neuron der einen Schicht eine Verbindung zu jedem anderen Neuron der nächsten Schicht aufbaut. Alle Informationen fließen dabei über eine

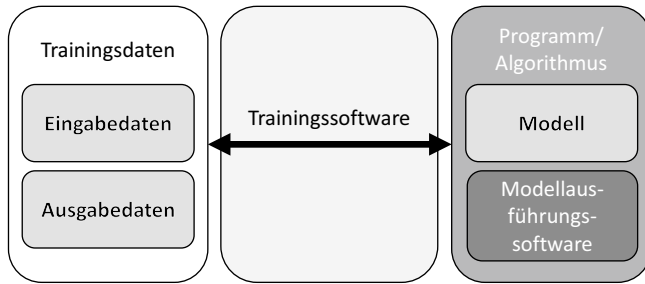


**Abb. 8.2** Netzarchitektur eines neuronalen Netzwerks. (Quelle: eigene Darstellung 2021)

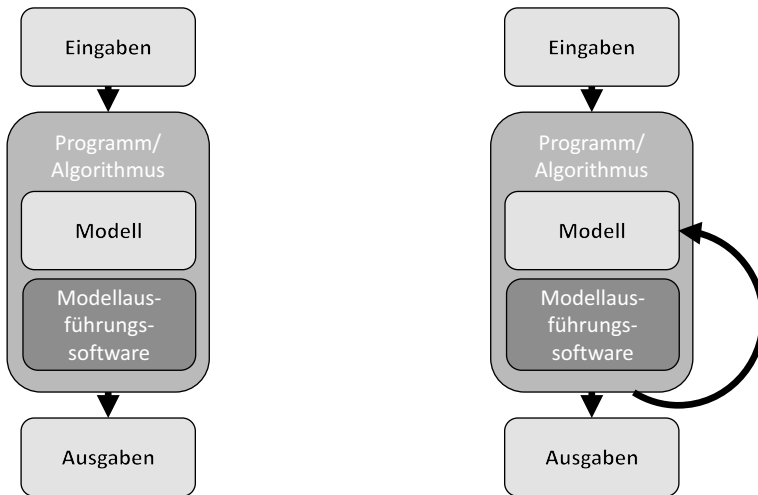
oder mehrere Zwischenschichten von der Eingabeschicht zur Ausgabeschicht (vgl. Moeser, 2018, o. S.; siehe Abb. 8.2).

**Deep Learning (DL)** Enthält eine Netzarchitektur mehr als eine Zwischenschicht, so wird von Deep Neural Networks oder Deep Learning gesprochen. Deep Learning ist eine Methode des maschinellen Lernens in künstlichen neuronalen Netzen. Diese umfassen mehrere Schichten, typischerweise eine Eingabe- und Ausgabeschicht sowie mehr als eine „versteckte“ dazwischenliegende Schicht. Die einzelnen Schichten bestehen aus einer Vielzahl künstlicher Neuronen, die miteinander verbunden sind und auf Eingaben von Neuronen aus der jeweils vorherigen Schicht reagieren. In der ersten Schicht wird etwa ein Muster erkannt, in der zweiten Schicht ein Muster von Mustern und so weiter. Je komplexer das Netz (gemessen an der Anzahl der Schichten von Neuronen, der Verbindungen zwischen Neuronen sowie der Neuronen pro Schicht), desto höher ist der mögliche Abstraktionsgrad und desto komplexere Sachverhalte können verarbeitet werden. Angewendet wird Deep Learning bei der Bild-, Sprach- und Objekterkennung sowie dem verstärkenden Lernen.

Beim maschinellen Lernen wird entsprechend ausgehend von Trainingsdaten mit entsprechenden Werkzeugen ein Modell gelernt (siehe Abb. 8.3). Nach einer Validierungsphase des Modells bildet dieses zusammen mit entsprechenden Modellausführungssystemen, oft vereinfacht KI Libraries genannt, eine Software, welche die gewünschte Funktionalität im Medizinprodukt darstellt. Bei adaptiver Software verändert jedoch die praktische Ausführung des Verfahrens das zugrunde liegende Modell. Diese Zusammenhänge sind in Abb. 8.4 dargestellt.



**Abb. 8.3** Trainingsphase. (Quelle: eigene Darstellung 2021)



**Abb. 8.4** Verwendungsphase des gelernten Systems, nicht adaptiv bzw. adaptiv. (Quelle: eigene Darstellung 2021)

### 8.2.6 Unterschied zwischen adaptiver und nicht adaptiver KI

Typischerweise ist das Modell, welches die KI verwendet, ein Algorithmus der seine Funktion durch Training mit Daten generiert. Dafür werden viele Daten benötigt, die mit einem Label versehen sind, z. B. in ein neuronales Netzwerk gegeben, damit sich die Neuronen anhand der Labels selber Gewichte zuweisen und auf der Ausgabenebene entsprechend eine Klassifizierung ausgeben. Es sei an dieser Stelle darauf hingewiesen, dass die KI bzw. das Modell, welches wiederum ein Stück Software entspricht, durch Software automatisiert entsteht und nicht durch einen Entwickler programmiert wird. Die Qualität und Zuverlässigkeit der KI hängen dabei stark von der Menge und Qualität der Trainingsdaten ab. Das Training wird verwendet, um ein Basismodell zu schaffen, welches in

der Lage ist, Daten korrekt zu labeln. Wie bereits beschrieben können Systeme sich mithilfe von verschiedenen Verfahren selbstständig weiterentwickeln. Durch den Zugang zu Trainingsdaten mit entsprechenden Labeln werden Algorithmen erlernt und die KI kann mit diesem Wissen Modelle lernen, die zur Erfüllung spezifischer Aufgaben verwendet werden können.

Sollte die Zufuhr an Trainingsdaten gestoppt werden, wird es keine weitere Entwicklung und keinen Lernfortschritt des Systems mehr geben. Es handelt sich in diesem Fall um ein geschlossenes Softwareprodukt. In diesem Fall wird auch von nicht adaptiver KI gesprochen.

Im Fall der adaptiven KI wird der Lernprozess hingegen nicht gestoppt. Eine adaptive KI lernt z. B. auch nach dem Inverkehrbringen und entwickelt sich weiter. Dies kann durch weitere Zuführung von Trainingsdaten neben dem praktischen Einsatz oder selbstständig direkt durch die praktische Erfahrung erfolgen. Eine solche stetige Weiterentwicklung macht das ursprünglich zugelassene Produkt von dem aktuellen Produkt unterscheidbar. Zusätzlich entwickeln sich die KI-Produkte je nach Standort und Nutzung unterschiedlich weiter und können Unterschiede in der Qualität der Ergebnisse aufweisen. Zu welchen regulatorischen Problemen dies führt, wird im nächsten Abschnitt näher erläutert.

---

## **8.3 Regulatorischer Umgang mit KI-gestützten Medizinprodukten**

In diesem Abschnitt wird betrachtet, inwieweit sich die regulatorischen Grundlagen auf KI-gestützte Medizinprodukte anwenden lassen. Dafür werden mithilfe von Beispielen Vorgehensweisen beschrieben und Limitierungen durch die Regularien aufgezeigt.

### **8.3.1 Regelungen bezüglich der Zulassung von KI-gestützten Medizinprodukten**

In den vorangegangenen Abschnitten wurde über die Zulassung von Medizinprodukten sowie harmonisierten Normen, die sich mit Software als Bestandteil eines Medizinproduktes oder auch als eigenständiges Medizinprodukt auseinandersetzen, gesprochen. Für die Zulassung von KI-gestützten Medizinprodukten existieren zum Zeitpunkt des Verfassens dieses Beitrags, abgesehen von einigen Initiativen und Drafts (vgl. Johnner, 2020b, o. S.), keine speziellen harmonisierten Normen, an denen sich der Medizinprodukthersteller orientieren könnte, um den Vermutungscharakter zu erlangen. Genau hier entsteht aber jetzt das Problem für den Medizinprodukthersteller. Aufgrund des Mangels an gesetzlichen Regelungen oder Normen, die Rahmenbedingungen für den Umgang mit KI-gestützten Medizinprodukten definieren, ist der Medizinprodukthersteller darauf angewiesen, selber Nachweise für die Konformität seiner Produkte zu belegen. Noch komplexer wird das

Problem für den Medizinprodukthersteller, sobald er vorhat sein KI-basiertes Medizinprodukt adaptiv, also selbstlernend, zu gestalten. Auf diese Problematik wird später noch einmal im Detail in Abschn. 8.3.3 eingegangen.

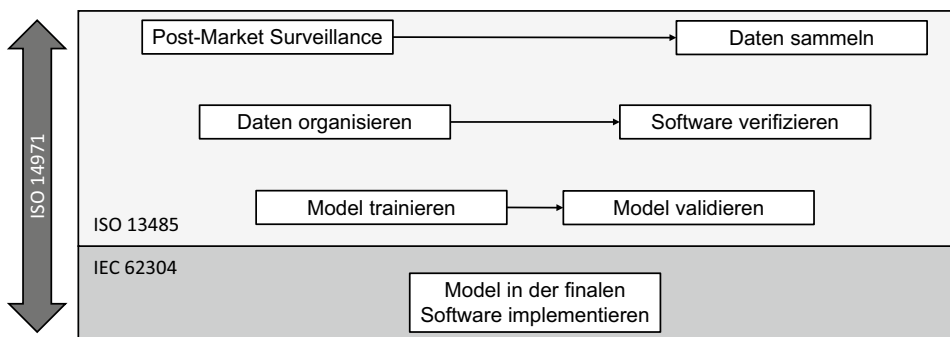
### **8.3.1.1 Umgang mit den vorhandenen Normen in der EU**

Der vorangegangene Abschn. 8.3 beschreibt, wie ein Hersteller durch die Verwendung von harmonisierten Normen ein Medizinprodukt entwickeln kann. Da es zum Thema KI explizit keine harmonisierten Normen gibt, entfällt diese offensichtliche Möglichkeit für den Hersteller. Wie aber im vorherigen Abschnitt erläutert, stellt KI oft ein Stück Software oder Hardware in einem komplexen Verbund aus anderen Software- und Hardwarekomponenten dar, der dann in einem komplexen Systemverbund erst zu ein Medizinprodukt wird. Der Vermutungscharakter kann somit auch über das Einhalten der verfügbaren und allgemein bekannten harmonisierten Normen aufgezeigt werden. Die wichtigsten zu berücksichtigenden Normen im europäischen Raum finden Sie in Tab. 8.1. Wie schon in Abschn. 8.2.1 erwähnt, bilden diese Normen die Basis zur Zulassung von Medizinprodukten im europäischen Raum, so wie es unter anderem die MDR fordert. Fast alle sind mindestens einmal revidiert worden und stammen somit aus einer Zeit, in der KI noch nicht im Fokus der jeweiligen Autoren stand. Vielmehr stellen diese Normen starke Anforderungen an die Sicherheit, um somit den Patientenschutz zu gewährleisten. Trotzdem können diese Normen sinnvoll auf die Entwicklung von nicht adaptiven KI-gestützten Medizinprodukten angewendet werden.

Wie einleitend schon erwähnt, ist eine KI ein Stück Software, welches sich auch im Rahmen der gegebenen Normen entwickeln lässt. So sollte schon bei der Definition der Zweckbestimmung (Intended Use) darauf geachtet werden, dass hier enge Grenzen gezogen werden, und die Verwendung des medizinischen Systems eindeutig beschrieben werden. Die Grenzen helfen anschließend die Validierung des medizinischen Systems im Rahmen zu halten. Trotzdem sollten diese Grenzen eine gewisse Toleranz bieten. Wird z. B. der Intended Use des KI-gestützten Medizinsystems beschrieben mit Bestimmung des Grades der Degeneration aufgrund einer KI-gestützten Auswertung von Bildinformationen und es zeigt sich im Nachhinein, dass eine aussagekräftige Bestimmung erst durch das Einbeziehen der Patientendaten wie Alter und Geschlecht möglich ist, so müsste der Intended Use geändert werden und das KI-gestützte Medizinsystem müsste sich erneut dem Prozess der Zulassung unterziehen. In der MDCG-2020-3- Guidance werden weitere Auslöser beschrieben, die zu einer Änderung eines Medizinprodukts führen können. (Anmerkung: Die „MDCG-Guidance zu wesentlichen Änderungen bei Medizinprodukten“ fokussiert sich auf Legacy-Produkte nach MDD und Änderungen die dazu führen, dass die Produkte nach MDR neu zugelassen werden müssten. Sie kann aber auch außerhalb dieses Kontextes angewendet werden und bietet einen guten Überblick über Änderungen, welche zu einer Neuzulassung führen.) So können beispielsweise Designänderungen oder Änderungen an der Software über einen Bug-fix hinweg zu einer erneuten Zulassung führen.

Ebenso ist es essenziell, dass von Beginn an das Risikomanagement berücksichtigt wird. Das Risikomanagement sollte sich kritisch mit der Daten- und Testbasis, der gewählten KI-Methode, dem trainierten Modell und der Validierung des Modells auseinandersetzen. Diese essenziellen Aspekte sind die Stützpfeiler einer soliden zuverlässigen KI und dürfen nicht vernachlässigt werden. So darf die Datenbasis nicht zu klein oder zu heterogen sein. Werden zu wenig Beispiele für das Training verwendet, ist das resultierende Modell evtl. nicht in der Lage, alle vorkommenden Modulationen einer Krankheit zu detektieren. Die Testbasis dient zur Validierung des trainierten Modells. Es sollte demzufolge keine Schnittmenge zwischen der Datenbasis für das Training und der Testbasis geben. Wird dasselbe Sample im Training sowie in der Validierung verwendet, wird wahrscheinlich ein hoher Score bei der Erkennung erreicht, da die Marker auf dem Bild im Test mit Bestandteil des trainierten Modells sind. In diesem Fall bedeutet ein hoher Score aber nicht zwangsläufig, dass das trainierte Modell tatsächlich gut im Detektieren ist, und könnte dazu führen, dass ein schlecht trainiertes Modell fälschlicherweise als gut empfunden wird. Ein Beispiel dafür wird in Abschn. 8.3.2.3 gezeigt. Wird das Risikomanagement richtig eingesetzt, kann es dabei helfen, die Wahl der Datenbasis ausgeglichen zu gestalten, um z. B. zu verhindern, dass ethnische Gruppenzugehörigkeit oder das Geschlecht bei der Erstellung der Diagnose eine Auswirkung hat, so wie es in dem Beitrag von Thoneick (2020, o. S.) gezeigt wird. Es gilt immer zu bedenken, dass das trainierte Modell ein Stück Software ist, welches wiederum durch Software entsteht. Schlussendlich muss das Produkt nach dem Inverkehrbringen beobachtet werden und Fehler bzw. Berichte über das Verhalten des Medizinproduktes, insbesondere über das Verhalten der KI, müssen risikotechnisch bewertet werden, um sicherzustellen, dass die Anwendung auch unter realen Bedingungen ihren bestimmungsgemäßen Gebrauch erfüllt.

Die vorhandenen Normen lassen sich auf diesem Weg auf das Thema KI anwenden. Ein vereinfachtes Vorgehen wird in Abb. 8.5 dargestellt.



**Abb. 8.5** Vereinfachtes Vorgehen ML. (Quelle: eigene Darstellung 2021)

### 8.3.1.2 Umgang mit den vorhandenen Normen in den USA

Außerhalb des europäischen Raumes ist die Food and Drug Administration (FDA) in den Vereinigten Staaten von Amerika (USA) zu erwähnen. Bei ihnen ist eine Registrierung von KI-gestützten Medizinprodukten bereits möglich. Dies gilt jedoch nur für nicht adaptive KI-Algorithmen. Sobald eine adaptive KI zum Einsatz kommt, würde sich durch die Verwendung und das Weiterlernen der KI der Zulassungsgegenstand ändern und müsste neu zugelassen werden. Allerdings hat die FDA hier erkannt, dass es eine Regulierungslücke beim Thema adaptive KI gibt. Um das Problem anzugehen, wurde von ihr ein Entwurf (vgl. Koll, 2019, o. S.) eines regulatorischen Rahmenwerkes aufgesetzt und offen zur Diskussion bereitgestellt.

Das „Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)“ (siehe Artificial Intelligence and Machine Learning in Software as a Medical Device, o. D.) definiert einen Prozess, der aus vier Komponenten besteht.

1. Quality Systems and Good Machine Learning Practices (GMLP):

Quality Systems and Good Machine Learning Practices (GMLP) steht für die Erweiterung des vorhandenen Qualitätsmanagementsystems mit Fokus auf das ML. Somit soll die Qualitätssicherung schon bei der Auswahl der Trainingsdaten ansetzen und sich beim Training und bei der Validierung des Modells fortsetzen. Dies macht die GMLP zum Leitbild des Medizinproduktherstellers und soll auf ganzer Ebene für durchweg hohe Qualitätsstandards Sorge tragen.

2. SaMD Pre-Specifications (SPS):

Durchführungen von Studien und Marktüberprüfungen für die KI-gestützten Medizinprodukte, welche unter Software as a Medical Device (SaMD) fallen. Dies dient der Sicherstellung der Sicherheit und Effektivität des Produktes und stellt zugleich die Basis für die Risikoüberwachung des Produktes über den gesamten Lebenszyklus dar.

3. Algorithm Change Protocol (ACP):

Überwachung der Modifikation an KI-Algorithmen durch das Lernen nach dem Inverkehrbringen zur Sicherstellung der Sicherheit und Effektivität der Algorithmen, inklusive Risikomanagementaktivitäten, unter Berücksichtigung der Vorgaben aus Software Changes. Also die Überwachung der adaptiven Algorithmen und Sicherstellung, dass die Änderungen keine Verschlechterung oder Änderung im Sinne eines Software Change darstellen.

4. Transparency

Transparenz für den Patienten und die FDA herstellen über die Änderungen an den KI-Algorithmen und der Aktivitäten zur Sicherstellung ihrer Sicherheit und Effektivität mit dem Ziel, Vertrauen aufzubauen.

Im Zentrum steht die Good Machine Learning Practice (GMLP), welche durch Risikomanagementaktivitäten und Transparenz gegenüber den Behörden und den Patienten



für Vertrauen sorgen soll. Zusätzlich muss der Hersteller umfangreich vor und nach dem Inverkehrbringen das Verhalten der KI-Algorithmen überwachen.

### **8.3.2 Anwendung der Normen bei der Erstellung von nicht adaptiven KI-gestützten Medizinprodukten**

Die beiden vorangegangenen Abschnitte zeigen, dass sich der Aufwand für KI-gestützte Medizinsysteme durch die Komplexität der KI-Komponente steigert. Die KI-Komponente besteht zuweilen aus einem Framework, welches Werkzeuge mitliefert, um aus den vorhandenen Daten ein Modell zu trainieren, und aus Bibliotheken, um das trainierte Modell zu implementieren. Dies führt dazu, dass die Werkzeuge nach ISO 13485 als Softwaretools im Entwicklungsprozess betrachtet werden sollten und damit der Toolvalidierung unterliegen. Das trainierte Modell sowie die Bibliotheken, die zur Implementierung notwendig sind, fallen wiederum unter IEC 62304 in den Bereich der SOUP, Software of Unknown Provenance, und müssen ebenfalls für ihren Aufgabenbereich in der finalen Anwendung validiert werden. Dies wird bereits in der Abb. 8.5 dargestellt.

#### **8.3.2.1 (Tool-)Validierung des KI-Baukastens und des Trainings**

Durch die stetig steigende Komplexität von Software und Hardware steigt auch die Fehlerrate in den Komponenten. Im Gegensatz zur Hardware unterliegt Software aber keinem Verschleiß. Das bedeutet, dass Fehler in der Software bereits während der Entwicklung entstehen. Ein Testen des Produkts nach der Fertigstellung allein reicht aber nicht mehr aus, um die fehlerfreie Funktion sicherzustellen. Die vorhandenen Kombinationen an Ein- und Ausgaben sind so komplex, dass es nicht mehr möglich ist, sie alle zu testen. Dies führt dazu, dass die Qualität und Sicherheit der Software schon während des Designs sichergestellt werden müssen, wie auch in Romo (2018, S. 3) ausgeführt wird, und so auch die Werkzeuge, die im Entwicklungsprozess zum Einsatz kommen. Die FDA fordert dafür schon länger eine risikobasierte Bewertung der Softwarewerkzeuge in der 21 CFR 820 und die ISO 13485 geht dieser Forderung in der 2016-Version nun in Abschn. 4.1.6 nach.

Für die Toolvalidierung nach ISO 13485 heißt dies im Detail, dass für die Referenzimplementierung des KI-Frameworks gezeigt werden muss, dass das Modell entsprechend den Eingaben seine Gewichte verteilt und so entsprechend lernt. Bevor überhaupt irgendwelche Daten zum Training verwendet werden und das trainierte Modell wieder mit Testdaten verifiziert werden kann, muss somit sichergestellt werden, dass das Modell entsprechend getroffener Annahmen seine Lernfähigkeit beweist und z. B. die Predict-Funktion auch in der Lage ist, das gewünschte Ergebnis zu liefern. Der Aufwand sollte der resultierenden Sicherheitsklasse des Produktes entsprechen und durch das Risikomanagement unterstützt werden.

### 8.3.2.2 Validierung der KI-Libraries und der Implementierung

Die Libraries, die notwendig sind, um das trainierte Modell in dem finalen Medizinprodukt zum Einsatz zu bringen, sowie das trainierte Modell an sich sind als SOUP zu betrachten und als solche ebenfalls zu validieren. Ein risikobasierter Ansatz wie bei der Toolvalidierung ist für SOUP nicht vorgesehen. Der Ablauf der SOUP-Validierung ist im Groben folgendermaßen (vgl. Johner, 2020d, 15:00–16:25):

1. Spezifikationen an die Softwarekomponenten definieren: Was ist die Aufgabe der Softwarekomponente und wie wird diese Aufgabe mit der Softwarekomponente gelöst? Gegebenenfalls sind sinnvolle Abgrenzungen, was mit der Softwarekomponente nicht gemacht wird, hilfreich.
2. Konzeption eines Testorakels: Festlegen definierter Testergebnisse, welche durch die Validierung erreicht werden sollen.
3. Bereitstellen von geeigneten Testdaten zur Validierung: Ermitteln und Festlegen geeigneter Testdaten mit denen Tests durchgeführt werden, damit glaubhaft und nachvollziehbar gezeigt werden kann, dass die Implementierung funktioniert. Diese Testdaten bestehen im besten Fall nicht aus den Daten, welche für die Verwendung im Endprodukt vorgesehen sind.

Folglich müssen Testszenarien erstellt werden, in denen die notwendigen Interfaces der Libraries, aber auch die Funktionalität des Modells überprüft werden können. Anforderungen an die notwendigen Interfaces sowie die Funktionalität des Modells lassen sich dafür aus dem Intended Use ableiten. Zudem muss in einem Testskript festgehalten sein, welche Schritte zu welchem Ergebnis führen. Anschließend kann mithilfe von einfachen, nachvollziehbaren Testdaten, die nicht dem Endprodukt entsprechen, die gewünschte Interaktion zwischen dem eigentlichen Programm bzw. dem Produktcode und dem Modell sichergestellt werden.

Für die SOUP-Validierung wird ein stark vereinfachtes KI-Modell ausreichen. Es soll nachgewiesen werden, dass das Modell entsprechend einer Eingabe in der Lage ist, eine adäquate Antwort zu liefern. Ein auf realen Daten trainiertes Modell ist viel komplexer und bedarf einer weitaus umfangreicheren Verifikation, welche im nächsten Abschnitt beschrieben wird.

### 8.3.2.3 Transparenz und Erklärbarkeit der KI

Da, wie schon in Abschn. 8.2.5 erklärt, das trainierte Modell von einer Software entwickelt ist, muss die KI zur Wahrung der korrekten Funktion umfangreich geprüft werden. Während die SOUP-Validierung aus dem vorgehenden Abschnitt sicherstellt, dass die Basisfunktionalität der einzelnen Komponenten, wie die Einbindung der Libraries und die korrekte Identifizierung von Markern auf einem Sample, durch das Modell gegeben ist, soll dieser Abschnitt die detaillierte Verifizierung des trainierten Modells beschreiben. Das Ziel ist es, den KI-Algorithmus, welcher sich hinter einem trainierten Modell verbirgt,

soweit es möglich ist, auf korrekte Funktion zu überprüfen und diese Funktion erklärbar darzustellen. Dies ist wichtig für den Medizinprodukthersteller, um sicherzustellen, dass sein Medizinprodukt nicht durch eine fehlerhafte oder ungenaue Erkennung einen Schaden verursacht. Zudem könnten zu solch einem Thema kritische Fragen innerhalb eines Audits gestellt werden, die es dann zu beantworten gilt.

Bei der Verifizierung der Software würde die Software in Komponenten zerlegt werden, um die einzelnen Komponenten gegen ihre Anforderungen zu testen. Dies kann dann in Regressionstests automatisiert oder durch einen Softwaretester erfolgen. Die KI bzw. das Modell ist dabei eine Komponente, die sich nicht in kleinere Komponenten zerlegen lässt. Die Anforderung der Erkennung von Markern in Sampeln führt zu einem Test, in dem das trainierte Modell mit vielen Testdaten auf die korrekte Erkennung von Labels überprüft wird. Da dieses Vorgehen sehr unpräzise ist und der Entscheidungsweg nicht ersichtlich ist, muss ein anderes Konzept angewendet werden. Es gibt einige Arbeiten zu diesem Thema, welche sich mit Kenntlichmachung der Entscheidungsgrundlage der KI auseinandersetzen, wie z. B. LIME oder Counterfactual Explanations. Eine Übersicht hierzu findet sich in Gilpin et al. (2019, o. S.). LIME z. B. versucht bei neuronalen Netzen, in denen Bilder klassifiziert werden, die Komponenten, auf deren Basis das trainierte Modell seine Entscheidung getroffen hat, zu visualisieren. Ribeiro et al. (2016, o. S.) konnten so zeigen, dass eine KI, die zwischen Huskys und Wölfen unterscheiden sollte, die zugrunde liegende Entscheidung anhand der falschen Klassifikatoren treffen kann. Dies wird für den Anwender aber nicht gleich über einen Score bzw. das Ergebnis verständlich. In ihrer Arbeit führen sie aus, dass die KI nicht das Tier an sich auf dem Bild klassifiziert, sondern den Schnee im Hintergrund dafür verwendet. So wurden alle Bilder mit Schnee als Wolf klassifiziert und alle Bilder ohne Schnee als Husky. Dies wäre in einem Medizinprodukt natürlich fatal.

Aber das Beispiel zeigt auch, dass das Maschine Learning Marker in einem Bild ausmachen kann, welche von einem Softwareentwickler vielleicht gar nicht berücksichtigt werden würden. So könnte es auch im positiven Sinne geschehen, dass die KI Marker in einem Bild erkennt, die noch gar nicht im Fokus der Anwender standen. Diese Marker sollten identifizierbar sein. Oder anders ausgedrückt sollte die Entscheidung der KI durch den Medizinprodukthersteller nachvollziehbar sein. Durch die Verbesserung der Nachweisbarkeit der Effizienz des Algorithmus wird der medizinische Nutzen des Medizinproduktes verstärkt werden.

Die Anwendung sollte zudem allgemein transparent sein. So könnte das KI-gestützte Medizinprodukt ein Ergebnis präsentieren und dem Anwender gleichzeitig den Score zu der getroffenen Entscheidung mitliefern. Dies kann in einer prozentualen Form erfolgen und zusätzlich über eine Ampel, welche mit roten, gelben und grünen Farbkategorien Ergebnisse schnell und verständlich visualisiert, vereinfacht dargestellt werden. Der behandelnde Arzt, der kein KI-Experte ist, aber die Diagnose stellt, kann sich dann ohne aufwendige Gegenprüfung schnell dafür entscheiden, ob er bei einem roten Ergebnis die Anwendung wiederholt oder Eingabeparameter (Lage- oder Lichtverhältnisse) verändert,

um ggf. ein besseres Ergebnis zu erhalten, oder bei einem grünen Ergebnis die Informationen bei der Befundung zu berücksichtigen. Bei welchem Score die Ampel entsprechend umschaltet, muss sinnvoll im Risikomanagement und mit Experten erarbeitet und zudem ausführlich begründet werden.

Eine Beobachtung des KI-gestützten Medizinsystems nach dem Inverkehrbringen ist nicht nur durch die MDR gefordert, sondern weiterhin ein wichtiger Bestandteil dessen, was mit zum Aufgabenbereich des Medizinproduktherstellers gehört. Ziel ist es, die korrekte Funktion der KI im Feld und damit außerhalb der bekannten Trainings- und Testdatensätze zu überwachen und ggf. Anomalien oder Fehlverhalten, das auf lokale Bedingungen oder auf Sonderfälle zurückzuführen ist, aufzudecken und aufzunehmen. Diese müssen dann risikobasiert bewertet werden und entweder in zukünftige Versionen der Software als Bug-fix oder Verbesserung mit einfließen. Im Zweifel müssen sie als Fehlverhalten der Behörden gemeldet und durch ein Update behoben werden.

### **8.3.3 Die Problemstellung bei adaptiven KI-gestützten Medizinprodukten**

Die vorangegangenen Abschnitte erklären, wie eine nicht adaptive KI in einem Medizinprodukt eingesetzt werden kann. Es ist also mit Einschränkungen möglich, KI-gestützte Medizinprodukte zu entwickeln. So sind Stand April 2019 bereits 26 (2018 waren es 18 und 2017 nur zwei; vgl. Prinz, 2020, o. S.)

Das Problem ist aber die Einschränkung, dass die KI ihr volles Potenzial durch die fehlende Adaption gar nicht entfalten kann. Wäre ein Medizinprodukt mit einer adaptiven, also selbstlernenden KI ausgestattet, würde dies dazu führen, dass sich das Medizinprodukt, welches in einem bestimmten Stand zugelassen wurde, durch die Verwendung im Feld verändern würde und so nicht mehr dem Zulassungsgegenstand entspricht, da sich das zugrunde liegende Modell der KI ebenfalls ändert. Dies wäre aus Softwaresicht eine Erneuerung oder Modifizierung des Algorithmus (vgl. auch MDCG 2020-3 Guidance) und müsste durch den Medizinprodukthersteller nach jeder Verwendung erneut validiert und freigegeben werden. Nun wird aber der Hersteller nicht nur ein Produkt verkaufen und nach jeder Anwendung mit einem Patienten das geänderte Modell wie unter Abschn. 8.3.1.1 beschrieben revalidieren oder neu zulassen wollen.

Wird dieses Szenario, dass das Medizinprodukt durch den Betrieb an unterschiedlichen Orten auch unterschiedlich lernt, weitergedacht, ergeben sich ganz neue Fragestellungen. So könnte Produkt A im Vergleich zu Produkt B mit einem Vielfachen an Patienten in Kontakt kommen, wodurch das Modell in Produkt A nicht nur schneller dazulernt, sondern Produkt B in der Genauigkeit der Diagnose übertrifft bzw. sogar eine andere Diagnose erstellt. Daraus resultiert die Frage, ob Patienten nach einem gewissen Lernzyklus darüber informiert werden, dass ihre Diagnose zum jetzigen Zeitpunkt überholt ist und ggf. anders ausfallen würde, evtl. besser oder gar schlechter?

Dies sind Fragen, die es durch zukünftige Arbeiten zu klären gilt. Schließlich ist der Intended Use des Medizinproduktes wahrscheinlich sogar so definiert, dass sich die KI durch die Diagnose von Patienten selbst verbessert. Kann außerdem gezeigt und gesichert werden, dass die KI sich auch wirklich durch z. B. bestärkendes Lernen verbessert und nicht verschlechtert? Ebenfalls müsste eine Lösung entwickelt werden, welche das neu trainierte Modell auch auf allen zugehörigen Medizinprodukten synchron hält.

---

## 8.4 Schlussbetrachtung

Für nicht adaptive KI-gestützte Medizinprodukte existieren Möglichkeiten, sie zur Zulassungsreife zu entwickeln, auch wenn der Aufwand dafür umfangreich ist. Hier empfiehlt es sich, bei der Wahl des KI-Frameworks auf Nischenprodukte zu verzichten und auf Projekte mit großer Akzeptanz sowie einer großen Community zu setzen. Da das Thema KI auch für die Medizin immer wichtiger wird und nicht vernachlässigt werden darf, wird es zukünftig KI-Frameworks geben, welche die Validierung in Teilen schon enthalten oder über eine Plattform, wie z. B. KI-SIGS (2020, o. S.), zur Verfügung gestellt werden, sodass nicht jeder Medizinprodukthersteller verpflichtet ist die Arbeit wieder und wieder zu durchlaufen. Dies würde Ressourcen für innovativen Wettbewerb freimachen und beispielsweise auch Start-ups befähigen, Medizinprodukte zu entwickeln, ohne an den regulatorischen Hürden zu scheitern.

Beim Thema adaptive KI-gestützte Medizinprodukte existiert noch ein hoher Bedarf an Vorgaben, Regelungen und Normen durch den Gesetzgeber. Die Initiative der FDA mit dem „Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback“ ist ein aktiver Schritt vorwärts für eine Diskussion zum Thema Regularien für KI. Auf der europäischen Seite war ein vergleichbarer Ansatz zum Zeitpunkt der Erstellung dieses Beitrags nicht ersichtlich. Hier muss aufseiten der Normen nachgebessert werden.

Es muss für alle Beteiligten eine eindeutige Regelung für folgende Fragestellungen geben. Sind Änderungen an dem trainierten Modell als Softwaremodifikation zu betrachten, obwohl dies gewünschtes Verhalten repräsentiert und dem bestimmungsgemäßen Gebrauch einer KI entspricht? Und wenn das zutrifft, müsste dann jede Änderung am trainierten Modell erneut durch den Medizinproduktehersteller freigegeben werden? Oder können die Änderungen an dem trainierten Modell außerhalb des Kontextes einer wesentlichen Änderung an einem Medizinprodukt betrachtet werden? Und welche Bedingungen müssen dafür geschaffen und umgesetzt werden?

## Literatur

- Artificial intelligence and machine learning in software as a medical device. (o. D.). U.S. Food and Drug Administration. <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device>. Zugegriffen: 23. Nov. 2020.
- Europäischer Markt. (o. D.). Europäischer Markt, BfArM, <https://www.dimdi.de/dynamic/de/medizinprodukte/europaeischer-markt/>. Zugegriffen: 23. Nov. 2020.
- Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2019). Explaining explanations: An overview of interpretability of machine learning. arXiv:1806.00069 [cs.AI], 1–10.
- Hastenteufel, M., & Renaud, S. (2019). *Software als Medizinprodukt – Entwicklung und Zulassung von Software in der Medizintechnik* (S. 18–65). Springer Vieweg.
- Johner, C. (2017). Sicherheitsklassen gemäß IEC 62304, Johner Institut (Hrsg.). <https://www.johner-institut.de/blog/iec-62304-medizinische-software/sicherheitsklassen-iec-62304/>. Zugegriffen: 6. Nov. 2020.
- Johner, C. (2019). Inverkehrbringung: Definition und regulatorische Anforderungen, Johner Institut (Hrsg.). <https://www.johner-institut.de/blog/regulatory-affairs/inverkehrbringung/>. Zugegriffen: 5. Nov. 2020.
- Johner, C. (2020a). Harmonisierte Normen: Beweisführung für Medizinproduktehersteller, Johner Institut (Hrsg.). <https://www.johner-institut.de/blog/regulatory-affairs/harmonisierte-normen/>. Zugegriffen: 6. Nov. 2020.
- Johner, C. (2020b). Künstliche Intelligenz in der Medizin, Johner Institut (Hrsg.). <https://www.johner-institut.de/blog/regulatory-affairs/kuenstliche-intelligenz-in-der-medizin/>. Zugegriffen: 29. Sept. 2020.
- Johner, C. (2020c). Problemlösungsprozess für Software, Johner Institut (Hrsg.). <https://www.johner-institut.de/blog/iec-62304-medizinische-software/problemloesungsprozess-software/>. Zugegriffen: 6. Nov. 2020.
- Johner C. (2020d) 2020-05: Validierung von ML-Libraries, [Audio-Podcast]. Medical Device Insights. [https://open.spotify.com/episode/3zIvmcmNRJvwaSjsMkRsVP?si=7XMP3KHtSkWm\\_MB2c7x3NA](https://open.spotify.com/episode/3zIvmcmNRJvwaSjsMkRsVP?si=7XMP3KHtSkWm_MB2c7x3NA).
- KI-SIGS. (2020). KI-SIGS Spaces für intelligente Gesundheitssysteme, UniTransferKlinik (Hrsg.). <https://ki-sigs.de>. Zugegriffen: 5. Nov. 2020.
- Koll, S. (2019). FDA hat Entwurf zu Künstlicher Intelligenz vorgelegt, Konradin-Verlag Robert Kohlhammer. <https://medizin-und-technik.industrie.de/digitalisierung/fda-hat-entwurf-zu-kuenstlicher-intelligenz-vorgelegt/>. Zugegriffen: 20. Okt. 2020.
- Konsortium HiGHmed. (2020). HiGHmed, Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF, Hrsg.). <https://www.medizininformatik-initiative.de/de/konsortien/highmed>. Zugegriffen: 6. Nov. 2020.
- Lenzen-Schulte, M. (2019). Künstliche Intelligenz: Algorithmen für den Augenarzt. *Deutsches Ärzteblatt*, 116(4), 146–149.
- Moeser, J. (2018). Künstliche Neuronale Netze, JUST ADD AI (Hrsg.). <https://jaai.de/kuenstliche-neuronale-netze-aufbau-funktion-291/>. Zugegriffen: 29. Okt. 2020.
- openEHR User Group. (2018). openEHR Haarbrandt B. (Hrsg.). <https://openehr.de/>. Zugegriffen: 6. Nov. 2020.
- Prinz, T. (2019). Künstliche Intelligenz und Medizinprodukte, Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE). <https://meso.vde.com/de/kuenstliche-intelligenz-medizinprodukte/>. Zugegriffen: 14. Okt. 2020.

- Prinz, T. (2020). Wie erfülle ich die regulatorischen Anforderungen für Künstliche Intelligenz-Anwendungen in der Medizin? Verband der Elektrotechnik Elektronik Informationstechnik e. V. (VDE, Hrsg.). <https://www.vde.com/topics-de/health/aktuelles/regulatorische-anforderungen-ki-medizin#:~:text=Die%20K%C3%BCnstliche%20Intelligenz%20in%20der,stark%20durch%20den%20Gesetzgeber%20reguliert>. Zugegriffen: 22. Okt. 2020.
- Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should i trust you?": Explaining the predictions of any classifier. arXiv:1602.04938 [cs.LG].
- Romo, S. (2018). Software tool validation for safety critical systems development, master's thesis, Aalto University (Hrsg.), Helsinki, S. 3.
- Thoneick, R. (2020). Diskriminiert dieser Automat Schwarze? Zeit (Hrsg.). <https://www.zeit.de/2020/32/kuenstliche-intelligenzdiskriminierung-hautfarbe-gesichtserkennung>. Zugegriffen: 29. Sept. 2020.
- Wikipedia. (2020). Kognition, Wikipedia (Hrsg.). <https://de.wikipedia.org/wiki/Kognition>. Zugegriffen: 29. Okt. 2020.
- Wirtz, B. W., & Weyerer, J. C. (2019). Künstliche Intelligenz: Erscheinungsformen, Nutzungspotenziale und Anwendungsbereiche. *WiSt*, 48(11), 4–10.

**Ludwig Pechmann, M. Sc.**, ist seit 2020 bei der UniTransferKlinik Lübeck GmbH als wissenschaftlicher Mitarbeiter maßgeblich an der Umsetzung des Verbundprojektes KI-SIGS beteiligt. Sein Schwerpunkt liegt dabei auf Untersuchung und Ausarbeitung der regulatorischen Grundlagen für die Zulassung von KI-gestützten Medizinprodukten. Ludwig Pechmann kann dafür auf eine langjährige Industrieerfahrung zurückgreifen. 2019 absolvierte Herr Pechmann erfolgreich eine nebenberufliche Ausbildung zum Manager Regulator Affairs. Seit 2016 war er für Haag Streit Möller Wedel, einem Hersteller für Operationsmikroskope, für die Qualitätssicherung der Softwareabteilung am Standort Lübeck verantwortlich und konnte den Softwarequalitätssicherungsprozess sowie das Produkt maßgeblich verbessern. 2016 absolvierte Herr Pechmann erfolgreich eine Ausbildung zum Qualitätsmanagementbeauftragten. Und davor konnte er als Softwareentwickler im Bereich eines Class-III-Medizinproduktes bei Philips Medical im Software-Tooling mitwirken und Erfahrungen sammeln. Herr Pechmann hat 2013 seinen Abschluss als Master of Science in Informationstechnologie an der Fachhochschule Kiel erworben.

**Martin Mildner** arbeitet als wissenschaftlicher Mitarbeiter mit dem Forschungsschwerpunkt auf regulatorischen Anforderungen und der Umsetzung KI-gestützter Medizinprodukte an der UniTransferKlinik Lübeck GmbH. Davor studierte er Volkswirtschaftslehre an der Georg-August-Universität Göttingen und schloss 2017 sein Masterstudium International Economics and Policy Consulting an der Otto-von-Guericke-Universität Magdeburg ab. Seitdem unterstützt er die UniTransferKlinik und das Institut für Softwaretechnik und Programmiersprachen der Universität zu Lübeck im Management und bei der Umsetzung verschiedener anwendungsorientierter Forschungsprojekte.

**Dr.-Ing. Tim Suthau** ist seit 2019 bei der UniTransferKlinik Lübeck GmbH maßgeblich an der Initiierung und Umsetzung von anwendungsorientierten Forschungsprojekten im Gesundheitswesen, bspw. der künstlichen Intelligenz (KI-SIGS), der Interoperabilität und Vernetzung (OR.NET) u. a. beteiligt. Sein Schwerpunkt liegt dabei bei den regulatorischen Anforderungen und möglichen Umsetzungen von Zukunftstechnologien. Tim Suthau kann dabei auf eine langjährige Industrieerfahrung zurückgreifen. Seit 2008 hat Herr Suthau für Haag Streit Möller Wedel, einem Hersteller für Operationsmikroskope, die Softwareabteilung am Standort Lübeck erfolgreich aufgebaut.

Danach war er bis 2018 als Director R&D lange Jahre für den gesamten Bereich Forschung und Entwicklung bei Möller Wedel verantwortlich und hat den digitalen Wandel im Unternehmen maßgeblich gestaltet und die Zulassung komplexer Medizinprodukte maßgeblich begleitet. Tim Suthau promovierte 2006 im Bereich Computer Vision der TU Berlin und am Krebsforschungszentrum Heidelberg im Bereich Augmented Reality zum Thema: „Positionsgenaue Einblendung räumlicher Informationen in einem See Through Head Mounted Display für die Medizin am Beispiel der Leberchirurgie“. Vor dem Hintergrund vielfältiger Erfahrungen der digitalen Transformation begeistert sich Herr Suthau für neue Technologien, Trends und Märkte.

**Martin Leucker** ist Professor für praktische Informatik, seit mehr als 10 Jahren Leiter des Instituts für Software Engineering und Programmiersprachen an der Universität zu Lübeck und Geschäftsführer der UniTransferKlinik GmbH, einer Technologietransfergesellschaft unter anderem des UKSH. Martin Leucker ist Autor von über 100 begutachteten Konferenz- und Zeitschriftenveröffentlichungen im Themenkomplex Software Engineering. Er ist stetiges Mitglied in Programmkomitees renommierter internationaler Konferenzen. In den letzten Jahren war Martin Leucker Projektleiter in verschiedenen öffentlichen und industriellen Projekten, insbesondere im Anwendungskontext Medizin/Medizintechnik. Prof. Leucker ist Konsortialführer des Projekts KI-SIGS, welches sich u. a. mit der Zulassung von KI-basierten Systemen im Gesundheitsbereich auseinandersetzt. Zuvor erforschte er im Projekt OR.NET Zulassungsfragestellungen von vernetzten Medizingeräten.