Digitalisierung und Patientensicherheit

Eva Sellge und Ernst-Günther Hagenmeyer

J. Klauber et al. (Hrsg.), *Krankenhaus-Report 2019*
https://doi.org/10.1007/978-3-662-58225-1_10

Zusammenfassung

Um mögliche Zusammenhänge zwischen der zunehmenden Digitalisierung der Patientenversorgung und der Patientensicherheit zu identifizieren, haben die Autoren eine systematische Literaturrecherche in der PubMed-Datenbank des National Center for Biotechnology Information (USA) durchgeführt. Die Suche wurde auf den Bereich der Krankenhausversorgung eingegrenzt und durch eine Handsuche in einschlägigen deutschen Zeitschriften ergänzt. In den Funden zeigten sich deutliche Bezüge zwischen beiden Themen. Einerseits können bestimmte digitale Anwendungen zu einer deutlichen Verbesserung der Patientensicherheit führen. Andererseits ergeben sich aus technischen Mängeln in IT-Systemen oder durch ihre fehlerhafte Anwendung teils gravierende Risiken für die Sicherheit. Um tatsächlich die Potenziale der Digitalisierung für die Patientensicherheit zu realisieren, sind fortwährende gemeinsame Anstrengungen von Herstellern, Betreibern und Anwendern von IT-Systemen erforderlich.

In order to identify possible links between the growing use of health information technology in medical care and patient safety, the authors conducted a systematic literature search using the PubMed database (National Center for Biotechnology Information, USA). The search was limited to publications related to hospital care. A search in specific German language journals was added. The identified publications showed manifold relations between digitalisation of care and patient safety. On the one hand, health IT solutions may significantly improve patient safety. On the other hand, serious risks may result from technical flaws or improper use of health IT. In order to realise the potentials of health IT solutions for the improvement of patient safety, a continuous joint effort of producers, operators and users of such systems is necessary.

10.1 Einleitung und Fragestellung

Ein wesentliches Handlungsfeld für die Gesundheitspolitik und alle am System beteiligten Akteure ist die Überführung des Gesundheitswesens in das digitale Zeitalter. Nicht nur der internationale Vergleich, sondern auch die steigenden Anforderungen durch Fachkräftemangel und Demografie sowie die Verfügbarkeit einer Vielzahl von digitalen Produkt- und Prozessinnovationen zeigen deutlich, dass dem Thema auch in den Gesundheitsunternehmen selbst eine höhere strategische Bedeutung beigemessen werden muss. Aktuelle Befragungen belegen, dass die zunehmende Digitalisierung der Krankenversorgung von den Führungsverantwortlichen in den Krankenhäusern als starker Trend wahrgenommen wird, der sich positiv auf ihre wirtschaftliche Situation auswirkt und von dem zusätzliche Chancen erwartet werden (Roland Berger GmbH 2018).

Geht man nun davon aus, dass sowohl die leicht verbesserte wirtschaftliche Lage der Krankenhäuser

ebenso wie die in der 19. Legislaturperiode angekündigten Reformmaßnahmen zur Investitionsfinanzierung positiv auf den o. g. Trend wirken, dürfte es zukünftig kaum noch ein Krankenhaus geben, das nicht entsprechende Digitalisierungsprojekte angeht (Augurzky et al. 2018). Je nach Ausgangslage oder Reifegrad der Organisation könnte sich ein solches Projekt zunächst auf die Optimierung von Administration und internen Versorgungsprozessen fokussieren. Mit der Einführung einer standardisierten elektronischen Patientenakte könnten aber z. B. die Sektorengrenzen überschritten und damit neue Versorgungsmodelle ermöglicht werden.

Welche Rolle spielt in diesem Szenario nun die Patientensicherheit? Angesichts des breiten Spektrums der Digitalisierungsthemen ist sie vermutlich in vielfältiger Weise betroffen. Mit der vorliegenden Arbeit soll deshalb ein Beitrag zur Beantwortung der folgenden Fragen geleistet werden:

- Welche Möglichkeiten eröffnet die Digitalisierung bzw. der Einsatz von Health IT im Krankenhaus, um die Patientensicherheit zu stärken?
- Welche Risiken bringt die Digitalisierung bzw. der Einsatz von Health IT – insbesondere verstanden als Instrument zur Unterstützung und Optimierung von Versorgungsprozessen – für die Patientensicherheit mit sich?
- Gibt es Modelle, Empfehlungen oder Leitlinien, wie mit den Möglichkeiten und Risiken, welche die Digitalisierung für die Patientensicherheit mit sich bringt, umgegangen werden kann?

Nach einer Klärung der beiden zentralen Begriffe wird im Folgenden ein Bezugsrahmen für die Analyse der Zusammenhänge zwischen Patientensicherheit und Digitalisierung eingeführt. Darauf aufbauend wird das im Rahmen einer systematischen Literaturrecherche gefundene Material beschreibend ausgewertet. In allen Fällen werden internationale Erfahrungen mit einbezogen; nicht nur, weil die Digitalisierung in anderen Gesundheitssystemen bereits weiter fortgeschritten ist und somit mehr Erkenntnisse vorliegen. Ein weiterer Grund für die Einbeziehung einer breiten Informationsbasis ist, dass, wenn es um mögliche Risiken oder Fehler bei der Patientenversorgung geht, immer noch Barrieren und Vorbehalte gegenüber einer möglichst transparenten Berichterstattung und Diskussion bestehen.

10.2 Hintergrund und Methodik

10.2.1 Begriffsklärung

Allein die Vielfalt der Anwendungsbereiche von IT und die daraus resultierenden potenziellen Effekte für den Patienten und seine Sicherheit erfordern zunächst, die beiden Begriffe „Patientensicherheit" und „Digitalisierung" zu klären, sowie die Ebenen, auf denen sie im Folgenden betrachtet werden sollen, voneinander abzugrenzen.

Patientensicherheit

Patientensicherheit (patient safety) ist ein fundamentales Prinzip des Gesundheitswesens und wird als solches bereits seit dem Jahr 2002 auf globaler Ebene adressiert. In einer Resolution verpflichteten sich die Mitglieder der World Health Organisation (WHO), diesem Thema höchste Aufmerksamkeit zu widmen mit dem Ziel, wissenschaftsbasierte Systeme zu etablieren, die notwendig sind, um Patientensicherheit und Versorgungsqualität insgesamt zu verbessern (World Health Organization 2002). Die konkrete Arbeit einer eigens gegründeten Abteilung in der WHO besteht seitdem insbesondere darin, Evidenz über die Zusammenhänge zwischen Risiken und Patientenoutcomes zu erforschen, Rahmenbedingungen und Klassifikationen für die Messung von Risiken und ihren Effekten zu entwickeln sowie Instrumente und Beratung zur Verfügung zu stellen (World Health Organization 2017). Nationale Organisationen nutzen diese Angebote und übersetzen sie in jeweils eigene Strategien. Das soll insbesondere sicherstellen, dass Terminologien und Klassifikationen übergreifend genutzt werden, auch um auf diese Weise die Maßnahmen vergleichend evaluieren zu können.

In Deutschland ist ein wichtiger Akteur zum Thema Patientensicherheit das Aktionsbündnis Patientensicherheit (APS). Hier haben sich – unterstützt durch das Bundesministerium für Gesundheit – Vertreter der Gesundheitsberufe, Kranken-

kassen und ihrer Verbände, der Krankenhäuser und der Patientenorganisationen zusammengeschlossen und erarbeiten mit Experten in interdisziplinären Arbeitsgruppen Anleitungen zur Umsetzung von Sicherheitsstrategien. Das APS definiert Patientensicherheit abstrakt als einen Zustand, d. h. als *„Abwesenheit unerwünschter Ereignisse"*. Ein unerwünschtes Ereignis (adverse event) beschreibt in dem Zusammenhang *„ein schädliches Vorkommnis, das eher auf der Behandlung, denn auf der Erkrankung beruht. Es kann vermeidbar oder unvermeidbar sein."* (Aktionsbündnis Patientensicherheit e. V. 2018a)

Für den Einsatz im Kontext der Digitalisierung erscheint eine Definition in Anlehnung an Thomeczek jedoch eher geeignet, da diese weitergehende konkrete Elemente aus der Versorgungspraxis einbezieht: *„Patientensicherheit ist das Produkt aller Maßnahmen in Klinik und Praxis, die darauf gerichtet sind, Patienten vor unerwünschten Ereignissen in Zusammenhang mit der Heilbehandlung zu bewahren. Diese Ereignisse umfassen vermeidbare Patientenschädigung durch die Gesundheitsversorgung, kritische Ereignisse, Fehler und Beinahe-Schäden. Sicherheit entsteht durch Wechselwirkungen zwischen Systemkomponenten; sie ruht nicht in einer Person, einem Apparat oder einer Abteilung. Die Verbesserung der Sicherheit hängt ab von der Erkenntnis, wie Sicherheit aus dem Zusammenwirken der einzelnen Komponenten des Systems entsteht. Patientensicherheit ist ein essentieller Bestandteil der Qualität des Gesundheitswesens."* (Thomeczek et al. 2004)

Den explizit präventiven Charakter von Patientensicherheit betont die Definition des Institute of Medicine (IOM): *"the prevention of harm to patients"*. Der Schwerpunkt liegt dabei auf einem Versorgungssystem, das (1) Fehler vermeidet, (2) aus Fehlern lernt und (3) auf einer Sicherheitskultur basiert, die Leistungserbringer, Organisationen und Patienten einbezieht (Institute of Medicine (US) Committee on Data Standards for Patient Safety 2004).

Grundsätzlich lassen sich Ereignisse in unterschiedliche Schweregrade einteilen. Entscheidend ist dabei jeweils, ob überhaupt ein sicherheitsrelevantes Ereignis entsteht und wenn ja, ob und inwieweit ein individueller Patient davon betroffen ist. Insbesondere bei Medikationsfehlern wird – sobald ein Patient geschädigt wird – weiter differenziert. Die Bewertung reicht dabei von einer vorübergehenden Schädigung, die eine stationäre Behandlung erfordert, bis hin zum Tod eines Patienten. Eine solche Einordnung ist nicht nur für die Bewertung der Relevanz von kritischen Ereignissen oder Situationen von Bedeutung, sondern auch für die Meldung und Beurteilung von Fehlern.

Digitalisierung

Eine universelle Definition des Begriffs gibt es nicht. In Abhängigkeit von Perspektive oder Kontext wird der Begriff eher technisch dargestellt oder prozessbezogen verstanden. Inzwischen wird der Begriff häufig von dem der „digitalen Transformation" abgelöst, der verdeutlichen soll, dass das Thema eine neue, nicht mehr ausschließlich technisch prozessuale Ebene erreicht hat. Dabei geht es insbesondere darum, innovative Geschäftsmodelle zu ermöglichen, die neuen Kunden- bzw. Patientennutzen schaffen und dabei mittel- und unmittelbar auf Gesellschaft und Arbeitswelt durchwirken (Bröckerhoff 2018).

In Deutschland ist Digitalisierung im Krankenhaus ein stark technik- bzw. prozessbezogenes IT-Thema. Ausgangspunkt der Entwicklung bildete zunächst die Verwaltung. Daraus entwickelte sich dann in der Regel eine IT-Gesamtarchitektur, bestehend aus einer administrativen (z. B. Kosten- und Leistungsrechnung, Finanzbuchhaltung, Personal, Materialwirtschaft) und einer klinischen Ebene (z. B. pflegerisches und ärztliches Stationsmanagement, Qualitätssicherung, Ambulanzmanagement, Radiologie, Endoskopie, Apotheke). Dabei geht es darum, eine möglichst durchgängige IT-Unterstützung aller Arbeitsabläufe innerhalb des Krankenhauses und an den Schnittstellen zu den vor- und nachversorgenden Sektoren zu schaffen. Ein Grundgedanke dabei ist, bisher papiergebundene Prozesse und Schnittstellen zu den externen Partnern (niedergelassene Ärzte, andere Krankenhäuser, Reha-Kliniken, Pflegeeinrichtungen etc.) und zum Patienten selbst zu digitalisieren. Von diesen Veränderungen sind alle IT-Ebenen im Krankenhaus betroffen – am stärksten die klinischen Ebenen mit direkter Schnittstelle zum Patienten und einer großen Anzahl von Nutzern, d. h. Ärzten, Pflegepersonal und Funktionsdienst-Mitarbeitern.

Über diese substitutive Funktion von Digitalisierung hinaus verändern deren innovative Technologien und Prinzipien zunehmend die etablierten Prozesse von Pflege, Diagnostik und Therapie und damit auch bestehende Strukturen in Krankenhäusern. Telemedizinische Anwendungen und elektronische Patientenakten bilden hier einen Anfang. In Zukunft wird die konsequente digitale Vernetzung das individuelle Monitoring und die Etablierung von Frühwarnsystemen über Abteilungs- und Sektorengrenzen hinweg erlauben. Es wird erwartet, dass sich mit Big Data und künstlicher Intelligenz Diagnostik und Therapieentscheidungen optimieren lassen. Roboter sollen nicht nur bei einem breiten Spektrum von operativen Eingriffen unterstützen können, sondern auch in der Pflege Personal entlasten. Mit Hilfe von Virtual Reality lassen sich Verfahren simulieren und auf diese Weise ganz neue Wege der Ausbildung von medizinischem Fachpersonal beschreiten.

Nach dem Krankenhaus Rating Report 2018 (Augurzky et al. 2018) hat Deutschland im internationalen Vergleich jedoch einen großen Nachholbedarf, der sich nicht nur an den niedrigen IT-Investitionen zeigt, sondern auch am bisher erreichten Digitalisierungsgrad. Der lässt sich mit Hilfe eines internationalen Reifegradmodells – dem European Electronic Medical Adoption Model (EMRAM) der HIMSS Analytics – messen. Dieses Digitalisierungsmaß gibt anhand von acht Stufen den Fortschritt eines Krankenhauses bei der Einführung von papierlosen, elektronischen Patientenakten und Behandlungspfaden an. Stufe 0 bedeutet, dass die Kliniken noch ausschließlich mit Papier arbeiten, ein vollständig digitalisiertes Krankenhaus erreicht Stufe 7. Insgesamt liegt der EMRAM-Score für Deutschland bei 2,2, wobei die höchste Stufe noch von keinem Krankenhaus erreicht wird (Grätzel von Grätz 2017). Demgegenüber liegt der durchschnittliche Wert in anderen europäischen Gesundheitssystemen bei 5,3 (Dänemark) bzw. 3,2 (Spanien).

Angesichts des breiten Spektrums von Digitalisierungsaspekten und dem sehr heterogenen Umsetzungsgrad der IT in deutschen Krankenhäusern wird in diesem Beitrag ein generisches Verständnis von Digitalisierung im Sinne des Begriffs der „Health IT" zugrunde gelegt und der Definition des US-amerikanischen Office of the National Coordinator for Health Information Technology gefolgt: *„The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making."* (Office of the National Coordinator for Health Information Technology – ONC 2018)

Damit lassen sich die unterschiedlichen Digitalisierungsebenen einbeziehen, aus denen sich dann jeweils eine mittelbare oder unmittelbare Betroffenheit der Patienten ergibt.

10.2.2 Bezugsrahmen für die Analyse der Zusammenhänge zwischen Digitalisierung und Patientensicherheit

Klassische Systeme, mit denen Aspekte der Patientensicherheit im Krankenhaus adressiert werden, wie z. B. das klinische Risiko- oder das Qualitätsmanagement, enthalten bislang keine expliziten Verfahren zur Erfassung von bzw. zum Umgang mit IT-bezogenen Patientenrisiken. Mit seiner Handlungsempfehlung „Digitalisierung und Patientensicherheit" hat das Aktionsbündnis Patientensicherheit in diesem Jahr für den deutschen Sprachraum einen ersten Überblick und Empfehlungen für einen strukturierten Umgang mit dem Thema zusammengestellt (Aktionsbündnis Patientensicherheit e. V. 2018b). Bei der Einführung von neuen Technologien liegt der Fokus in der Regel mehr auf den Nutzeranforderungen oder den Fragen des Datenschutzes bzw. der Datensicherheit. Berücksichtigt man jedoch, dass Implementierungen von Health IT häufig über verschiedene Organisationseinheiten – zum Teil auch räumlich über größere Distanzen – verteilt sind und damit Sicherheitsprobleme nicht nur eine einzige Station, sondern auch ganze Abteilungen oder auch Kliniken und Klinikverbünde betreffen können, zeigt sich deutlich, dass es zur Identifikation und Bewertung von IT-bezogenen Patientenrisiken eines eigenen methodischen Bezugsrahmens bedarf. Dieser ist Voraussetzung für die Identifikation und Messung von Risiken für die Patientensicherheit ebenso wie für die Entwicklung und Einführung von geeigneten Maßnahmen zu deren Vermeidung bzw. Verminderung.

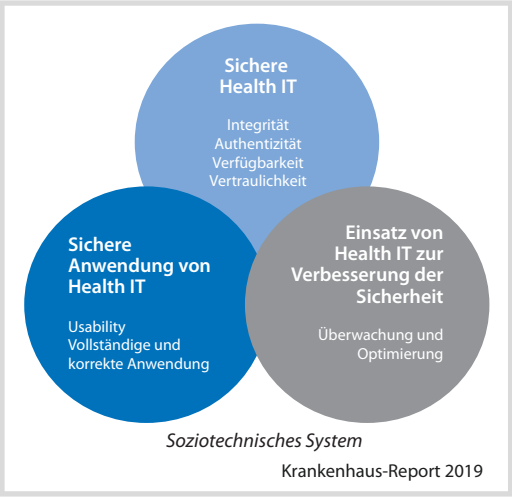

Abb. 10.1 Health-IT-Safety-Domänen (modifiziert nach Singh und Sittig 2016)

Mit dem Health Information Technology Safety Measurement Framework (HITS Framework) von Singh und Sittig liegt ein ganzheitliches Bezugssystem vor, das einen Ansatz verfolgt, der das komplette soziotechnische Arbeitssystem umfasst (Singh und Sittig 2016). Das heißt, es werden rein technikbezogene (z. B. Hardware, Software, Netzwerkinfrastruktur) von nicht-technischen Variablen (z. B. Nutzerverhalten, klinische Workflows, interne Standardprozeduren und externe Regulation) unterschieden, die allein oder durch Wechselwirkungen zwischen diesen Variablen die Patientensicherheit beeinflussen.

Das System gliedert sich in drei sich überlappende Domänen (Abb. 10.1):

1. „*Sichere Health IT*" – adressiert ausschließlich Sicherheitsbelange, die einzig und alleine mit der Technologie, also Hard- und Software zusammenhängen.
2. „*Sichere Anwendung von Health IT*" bezieht sich auf eine sichere und bestimmungsgemäße Nutzung von Health IT durch Ärzte, Pflegekräfte, jegliche weitere Art von Personal sowie den Patienten selbst.
3. „*Einsatz von Health IT* zur Verbesserung der Patientensicherheit" – umfasst Technologie und ihren Gebrauch zur Identifikation, zum Monitoring und zur Verminderung von Risiken für die Patientensicherheit.

Mit jeder Domäne lassen sich grundsätzliche Prinzipien verbinden, mit denen die Patientensicherheit gewährleistet und verbessert werden soll (Tab. 10.1).

Sinn des Bezugsrahmens ist es, mit seiner Hilfe die möglichen Risiken und Chancen, die mit Health IT in einem bestimmten Versorgungssetting ver-

Tab. 10.1 Health-IT-Domänen und ihre Kernprinzipien (modifiziert nach Singh und Sittig 2016)

Domäne	Prinzipien
1. Sichere Health IT	– *Datenverfügbarkeit*, d. h. Daten sind verfügbar und auf Anforderung für autorisierte Personen nutzbar. – *Datenintegrität,* d. h. Daten oder Informationen sind korrekt und in geeigneter Weise erfasst, sie werden nicht durch unautorisierte Prozesse verändert oder zerstört. – *Vertraulichkeit*, d. h. Daten und Informationen sind nur für autorisierte Personen oder Prozesse verfügbar oder abrufbar.
2. Sichere Anwendung von Health IT	– *Vollständige und korrekte IT-Anwendung,* d. h. Health-IT-Features und Funktionalitäten sind wie intendiert implementiert und werden ebenso genutzt. – *Health-IT-System-Usability,* d. h. Health-IT-Features und Funktionalitäten sind so gestaltet und implementiert, dass sie effektiv, effizient und zur Zufriedenheit der Nutzer angewendet werden können, um das mit ihnen verbundene Schadenspotenzial zu minimieren.
3. Einsatz von Health IT zur Verbesserung der Patientensicherheit	– *Überwachung und Verbesserung*, d. h. als Teil eines kontinuierlichen Qualitätssicherungs- und Performance-Optimierungsprozesses sind Mechanismen umgesetzt, mit denen grundsätzliche sicherheitsrelevante Aspekte ebenso wie die sichere Anwendung von Health IT überwacht werden können. Kritische Ereignisse werden frühzeitig entdeckt und berichtet, d. h. Health IT wird aktiv genutzt, um Schäden zu vermeiden und die Sicherheit zu erhöhen.

Krankenhaus-Report 2019

bunden sind, umfassend und systematisch zu beschreiben. Auf diese Weise lassen sie sich aus vorhandenen Dokumentationen retrospektiv erfassen – was auch in der hier durchgeführten systematischen Literaturrecherche praktiziert wird. Darüber hinaus können Risiken in dieser Struktur auch prospektiv identifiziert und entsprechende Präventionsmaßnahmen implementiert werden.

10.2.3 Methodik des Reviews

Zur möglichst umfassenden Beantwortung der in der Einleitung entwickelten Fragestellung – welche Möglichkeiten eröffnen sich einerseits durch die Digitalisierung im Krankenhaus, um die Patientensicherheit zu stärken, und welche Risiken für die Patientensicherheit bringt sie andererseits mit sich – wurde zunächst eine systematische Literaturrecherche in PubMed[1] durchgeführt. Dabei wurden die Themenfelder „Digitalisierung", „Patientensicherheit" und „Krankenhausbehandlung" jeweils mit den zugehörigen englischen Begriffen aus dem Medical-Subject-Headings-Verzeichnis (MeSH) operationalisiert. Die Suche wurde dann anhand einer UND-Verknüpfung der Themenfelder durchgeführt. Der gewählte Recherchezeitraum umfasst die letzten zehn Jahre, einbezogen wurden Publikationen in englischer oder deutscher Sprache.

Die Treffer wurden nach dem HITS-Framework (Singh und Sittig 2016) den drei Domänen zugeordnet:

1. Publikationen zur Patientensicherheit im Zusammenhang mit der Technik (Health Information Technology, HIT) bzw. zu technischen Aspekten der Digitalisierung im Krankenhaus
2. Publikation zur Patientensicherheit im Zusammenhang mit der Anwendung der HIT
3. Publikationen zum Einsatz von Health IT mit dem Zweck der Verbesserung der Patientensicherheit.

Zusätzlich wurden alle Treffer noch danach beurteilt, ob sie sektorenübergreifende Aspekte behandeln.

Anschließend wurden die thematischen Schwerpunkte für jede Domäne herausgearbeitet. Der Evidenzstatus von einbezogenen Studien wurde im Rahmen dieses Artikels nicht berücksichtigt.

Darüber hinaus wurden für den Blick auf die Besonderheiten der deutschen Krankenhauslandschaft und aktuelle Management-Themen weitere Quellen mit direktem Bezug zum deutschen Gesundheitswesen hinzugezogen und ergänzend ausgewertet:

1. Handrecherche über die Jahrgänge 2016 bis Juni 2018 in ausgewählten deutschen Fachzeitschriften mit Krankenhausbezug: das Krankenhaus (Deutsche Krankenhaus Verlagsgesellschaft mbH, Düsseldorf); kma – Krankenhausmanagement aktuell (Georg Thieme Verlag KG, Stuttgart); ehealthcom (HEALTHCARE-COM GmbH, Offenbach); Deutsches Ärzteblatt (Deutscher Ärzteverlag GmbH, Berlin) sowie Open-Access-Publikationen der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e. V.
2. Stichprobenhafte Abfragen im Krankenhaus-CIRS-Netz Deutschland 2.0, ein Berichts- und Lernsystem (Critical Incident Reporting-System – (CIRS)[2]), das von der Deutschen Krankenhausgesellschaft (DKG), dem Deutschen Pflegerat (DPR) und dem Ärztlichen Zentrum für Qualität (ÄZQ) getragen wird
3. Tagungsbeiträge der APS-Jahrestagung „Digitalisierung und Patientensicherheit" vom 3./4. Mai 2018 in Berlin

10.3 Ergebnisse

10.3.1 Gruppierung der einbezogenen Publikationen

Von den insgesamt 1.132 Treffern aus der PubMed-Recherche (06.07.2018) wurden 821 ausgeschlossen; die verbliebenen 311 wurden in die verschiedenen Domänen-Kategorien gruppiert. Dabei bestätigen die Artikelfunde auch die Darstellung von Singh und Sittig, wonach die Domänen nicht immer scharf zu trennen sind und sich überlappen können. Das heißt, es kommt zu Ereignissen, die

1 https://www.ncbi.nlm.nih.gov/pubmed

2 https://www.kh-cirs.de/

Tab. 10.2 Übersicht Anzahl der Publikationen in den Domänen nach Singh und Sittig (2016)

Domäne	Publikationen	Anzahl
1	… zu Patientenrisiken, die ausschließlich auf die eingesetzten Informations-Technologien zurückzuführen sind	18
2	… zu Patientenrisiken, die durch die fehlerhafte Anwendung von digitalen Anwendungen entstehen	30
2	…, in denen digitale Anwendungen beschrieben werden, die spezielle Patientenrisiken verringern oder verhindern	144
1 und 2	… zu Patientenrisiken, die auf die verwendeten Technologien und nicht sachgerechtes Anwenderverhalten zurückzuführen sind	19
2 und 3	… zu Patientenrisiken, die durch nicht sachgerechtes Anwenderverhalten in digitalen Anwendungen zur Reduzierung von Sicherheitsrisiken entstehen	95
1 und 3	… zu Patientenrisiken, die durch technische Fehlfunktionen in Anwendungen zur Reduzierung von Sicherheitsrisiken entstehen	5

Krankenhaus-Report 2019

aus einer Kombination von technischen mit anwenderbezogenen Problemen zurückzuführen sind. Aus diesem Grunde wurden die drei Domänen um die möglichen Mischformen ergänzt und diesen die entsprechenden Artikel zugeordnet (Tab. 10.2).

Bei einer großen Anzahl der gefundenen Publikationen handelt es sich um Fallstudien. Es finden sich aber auch Analysen von Fehlerberichtssystemen, sekundäre Auswertungen anderer Datenquellen, Auswertungen von Interviews mit Anwendern sowie konzeptionelle Arbeiten.

Von den 311 Publikationen befassten sich 13 explizit mit sektorenübergreifenden Aspekten.

Bei den ausgeschlossenen Treffern (821) handelt es sich vor allem um Publikationen, die klinische Studien oder deren Methodik beschreiben. Häufig kommen dabei digitale Tools bzw. elektronische Patientenakten zur Datensammlung zum Einsatz. Zugleich berichten klinische Studien notwendigerweise über Aspekte der Patientensicherheit. Eine Teilmenge von 43 Treffern konnte wegen mangelnder Informationen bei fehlendem Abstract keiner Domäne zugeordnet werden.

Auch relevante Artikel aus den in ▶ Abschn. 10.2.3 genannten deutschen Fachzeitschriften sowie beispielhafte Fallbeschreibungen aus dem Krankenhaus-CIRS-Netz Deutschland wurden den einzelnen Domänen zugeordnet.

10.3.2 Beschreibende Auswertung der Domänen nach Themenschwerpunkten

Domäne 1: Publikationen zu Patientenrisiken, die ausschließlich auf die eingesetzten Informations-Technologien (Health IT) zurückzuführen sind

- **Schwerpunktmäßig untersuchte Health-IT-Produktkategorien**
  - IT-Netzwerk einer Versorgungseinrichtung, insgesamt oder Teile davon
  - Datenbanksysteme
  - Systeme zur Entscheidungsunterstützung (Decision Support Systeme)
  - Telekommunikationssysteme

- **Beschriebene Fehlfunktionen**

In jedem IT-System spielen Daten eine wesentliche Rolle. Ihre Verfügbarkeit und Verlässlichkeit sind zentral für den Einsatz im Rahmen der Patientenversorgung – unabhängig von der jeweiligen „Produktkategorie". Kommt es beispielsweise zu einem Stromausfall, kann nicht nur auf Dokumentationssysteme nicht zugegriffen werden – auch Überwachungs- und Alarmsysteme fallen aus (Samy et al. 2010). Eine ggf. notwendig gewordene Wiederherstellung von Daten nach einem Stromausfall oder auch einem Virusangriff kann unvollständige oder auch fehlerhafte Daten zur Folge haben (Sax et al. 2016).

Grundsätzlich kann das Vertrauen auf Daten in den Systemen (z. B. Laborwerte oder Arzneimittelverordnungen), von denen nicht durch geeignete Maßnahmen sichergestellt ist, dass sie unverfälscht und dem richtigen Patienten zugeordnet sind, zu kritischen Ereignissen führen. Dies zeigen z. B. auch Fallbeschreibungen aus dem KH-CIRS: Die automatische Übernahme von Patientendaten aus Voraufenthalten bei Übereinstimmung von Vor- und Nachnamen sowie Geburtsdatum führte zu einer Patientenverwechslung, da es sich um eine häufiger vorkommende Kombination der personenbezogenen Daten handelt. Es fehlte die systemseitige Zuordnung eines eindeutigen Patientenkennzeichens und ein automatischer Warnhinweis an den Anwender, der ihn zur erneuten Überprüfung der Patientenidentität auffordert (KH-CIRS-Netz Fall-Nr. 37.779).

Auch durch Fehl- oder Nichtauslösung von Alarmen entstehen Risiken. Gründe für diese Art von Fehlfunktionen bleiben dem Anwender in der Regel verborgen. Dabei handelt es sich beispielsweise um nicht intendierte Deaktivierungen von Regeln oder Änderungen im Softwarecode, die durch Upgrades entstehen. Häufig liegen Fehlfunktionen auch in einer nicht oder nur begrenzt beeinflussbaren Wechselwirkung mit Web-basierten Systemen, die nicht direkt im Zugriff der Anwender sind. Aktuelle Ansätze zur Prävention und Aufdeckung derartiger technischer Fehler werden als nicht ausreichend beschrieben (Wright et al. 2016).

Direkter sichtbar werden die Effekte technischer Störungen im Telekommunikationssystem, durch die beispielsweise in einer Notfallsituation der diensthabende Arzt erst mit zeitlicher Verzögerung angerufen werden konnte (KH-CIRS-Netz Fall-Nr. 173.609).

Domäne 2: Publikationen zu Patientenrisiken, die durch die fehlerhafte Anwendung von digitalen Anwendungen entstehen

Schwerpunktmäßig untersuchte Health-IT-Produktkategorien

- Elektronische Erfassung und Verarbeitung von therapeutischen Anweisungen eines Arztes (Computerized Physician Order Entry – CPOE)/Elektronische Arzneimittelbestellung/-verordnung
- Elektronische Gesundheitsakte (Electronic Health Record – EHR)

Dargestellte Anwenderprobleme

Die Ursachen von nicht sachgerechter Anwendung von Health IT liegen häufig in fehlender oder inadäquater Schulung der Mitarbeiter oder einem nicht anwenderorientierten Design (Clarke et al. 2016). Gelegentlich treffen diese Umstände auch zusammen. Eine nicht-intuitive Nutzerführung erhöht den Schulungsbedarf und führt bei Problemen schnell zu einem Akzeptanzverlust bei den Anwendern (Simon 2017). Ein häufig zu beobachtender Effekt sind sogenannte „Workarounds". Dabei lassen sich informelle von formalen Workarounds unterscheiden. Die Erstgenannten entstehen, wenn Mitarbeiter ohne formale Genehmigung durch ihr Management Änderungen am technisch vorgegebenen Workflow vornehmen. Gründe hierfür sind Probleme mit der Anwendung des Systems, mangelhafte Performance oder Verfügbarkeit der Anwendungen. Formale Workarounds entstehen auf Anweisung des Managements insbesondere dann, wenn tatsächliche oder vermeintliche Patientenrisiken abgewendet werden sollen. Bei beiden Typen werden zusätzlich papierbasierte Workflows oder andere Software-Anwendungen genutzt (Cresswell et al. 2017), die zu Inkonsistenzen oder unvollständigen Datensätzen im System führen können. Durch den so entstehenden Medienbruch wird außerdem eine neue Fehlerquelle eröffnet. (KH-CIRS-Netz Fall-Nr. 167.939).

Ein anderes anwenderbezogenes Problem entsteht, wenn einzelne Computer durch unterschiedliche Berufsgruppen genutzt werden. Erfolgt keine korrekte Abmeldung beim Verlassen des Arbeitsplatzes, kann eine andere Person im Nutzerprofil eines Kollegen oder einer Kollegin Daten eingeben oder verändern. Dies erfolgt häufig unbemerkt und kann dann zu nicht gewollten Datenänderungen am Datensatz eines Patienten führen (KH-CIRS-Netz Fall-Nr. 153.015).

Unabhängig davon kann es in allen patientenbezogenen IT-Systemen zu Falscheingaben, zur Verwechslung klinischer Parameter in der Eingabemaske, zum nicht intendierten Überschreiben von

Informationen, zur unbemerkten falschen Zuordnung von Daten oder Doppelanordnung von Medikamenten kommen. Diese werden besonders häufig in prozessunterstützenden Anwendungen wie dem CPOE beobachtet (Vélez-Díaz-Pallarés et al. 2017).

Anwenderbezogene Gründe für derartige Fehler in der Nutzung von IT-Systemen ergeben sich häufig auch durch ungünstige Rahmenbedingungen wie eine hohe Arbeitsbelastung der Mitarbeiter durch Fachkräftemangel bzw. eine starke Arbeitsverdichtung in den Krankenhäusern. Auch können besondere Stresssituationen durch unklare Verantwortlichkeitsstrukturen oder fehlendes Training entstehen (Hampel 2016a, 2016b).

Domäne 3: Publikationen, in denen digitale Anwendungen beschrieben werden, die spezielle Patientenrisiken verringern oder verhindern

- **Schwerpunktmäßig untersuchte Health-IT-Produktkategorien bzw. Funktionalitäten**
  - Elektronische Patientenakten (EHR)
  - Systeme zur Entscheidungsunterstützung (Decision-Support-Systeme)
  - Systeme zur Risikobewertung
  - Systeme zur Kalkulation von Dosierungen
  - Warn- und Erinnerungssysteme
  - Teleradiologische Anwendungen
  - Robotik
  - Fehlermeldesysteme (CIRS)

In dieser Domäne wird deutlich, dass intendierte positive Effekte von Health IT auf die Patientensicherheit durch technische Mängel oder fehlerhafte Anwendung zugleich konterkariert werden können. Deshalb erfolgt hier zusätzlich die Darstellung der Thematiken von Publikationen, die der Domäne 3, zugleich aber auch Domäne 1 oder 2 zugeordnet werden konnten.

- **Untersuchte Funktionen zur Minimierung von Patientenrisiken**

IT-Systeme zur Entscheidungsunterstützung und Risikobewertung greifen in der Regel auf die Daten des Krankenhausinformationssystems oder die Inhalte von elektronischen Patientenakten zurück. Häufig werden auch web-basierte Datenquellen und spezielle Wissensdatenbanken (z. B. Zulassungsinformationen zu Arzneimitteln) angebunden. Hierunter fallen auch Anwendungen, die bestimmte Risiken ermitteln, über Scores darstellen und diese mit entsprechenden Handlungsanweisungen zur Minimierung oder Vermeidung dieser Risiken verknüpfen. Untersucht wurden insbesondere Algorithmen zur Vermeidung von Stürzen (Townsend et al. 2016; Yokota et al. 2017), tiefen Venenthrombosen (Spirk et al. 2017), Wiederaufnahmen (Colavecchia et al. 2017) sowie grundsätzliche Ansätze zur Senkung der Krankenhausmortalität (Nakas et al. 2016).

Integrale Bestandteile von entscheidungsunterstützenden IT-Systemen sind oft auch Dosiskalkulationssysteme, die in der Radiologie (Jurado-Román et al. 2016) oder im Zusammenhang mit der Verabreichung von Arzneimitteln (Czock et al. 2015) zum Einsatz kommen. Häufig sind diese mit entsprechenden Warn- und Erinnerungssystemen kombiniert. Die dort verwendeten Regeln greifen zumeist auf weitere interne Datenquellen wie z. B. die Stammdaten für Alters- und Größenangaben zurück, können aber auch externe Informationen einbeziehen.

Ein direkter Zugriff auf Vitalparameter von gefährdeten Patienten erfolgt durch Frühwarnsysteme, die speziell für den Einsatz auf Allgemeinstationen entwickelt wurden. Durch ein kontinuierliches Monitoring von Werten, die einer kritischen klinischen Situation vorausgehen, und automatischer Alarmauslösung bei der Überschreitung definierter Schwellenwerte können auch dort medizinische Zwischenfälle verhindert werden.

Mittelbar auf die Patientensicherheit wirkt die Teleradiologie als Instrument zur Einholung einer Zweitmeinung. Sie erhöht die Qualität der Diagnostik und hilft ggf. Mehrfachuntersuchungen und damit verbundene Strahlenbelastung zu vermeiden (Swanson et al. 2012).

Ebenfalls nur mittelbar auf die Patientensicherheit kann sich der Einsatz von Robotern bei minimalinvasiven Operationen auswirken. In den gefundenen Studien geht es dabei primär um den Vergleich der minimalinvasiven mit der offenchirurgischen Technik. Das eigentliche Thema ist jedoch die Bewertung von roboter-assistierten Operationsmethoden (Trinh et al. 2012; Yu et al. 2012); sie soll als solches hier nicht weiter vertieft werden.

Ein weiterer Anwendungsbereich für den Einsatz von Robotersystemen ist die Krankenhausapotheke. Dort können insbesondere im Rahmen der Herstellung von patientenindividuellen Arzneimittelzubereitungen wie z. B. intravenösen Chemotherapien Fehler bzw. Risiken bei der Zubereitung (z. B. substanz-, dosierungs-, oder hygienebezogene Aspekte) reduziert werden (Hagebeucker et al. 2018).

Die Etablierung von Fehlermeldesystemen dient explizit der Verbesserung der Patientensicherheit und gewinnt als Instrument im Rahmen des klinischen Risikomanagements in Krankenhäusern zunehmend an Bedeutung (Aktionsbündnis Patientensicherheit e. V. 2016). Diese Systeme bieten die sanktionsfreie Möglichkeit zur Meldung von Ereignissen, die potenziell oder tatsächlich zu Patientenschäden geführt haben. Ziel ist es, aus diesen zu lernen, indem sie strukturiert aufbereitet, bewertet und veröffentlicht werden. Der damit verbundene Melde-, Bewertungs- und Publikationsprozess erfolgt im Wesentlichen internetbasiert. Melder sowie ggf. betroffene Patienten und Einrichtungen bleiben anonym.

▪ Dargestellte Fehlfunktionen und Anwenderprobleme

IT-Anwendungen, die eigentlich die Patientensicherheit erhöhen sollen, können ihrerseits wieder Ursache für neue Risiken sein, so zum Beispiel im Zusammenhang mit der Verwendung von Dosiskalkulationssystemen. Hier kann es durch Inkompatibilitäten zwischen den verknüpften Systemen zu technik- oder anwenderbezogenen Fehlern kommen. Das heißt, bei der Übertragung von Dosiseinheiten oder Parametern zur Dosisberechnung können beispielsweise verschiedene Einheiten verwendet, übertragen und ohne Rückfrage durch das System falsch interpretiert werden (Kirkendall et al. 2014).

Ein weiteres Risiko entsteht durch das Phänomen der „Alarm Fatigue". Diese beschreibt eine abnehmende oder auch Nicht-mehr-Reaktion auf Alarme durch Ärzte oder Pflegepersonal aufgrund der hohen Rate von Fehlalarmen (Stultz und Nahata 2014). Studien zeigen, dass von den 150 bis 350 Alarmen der Monitoring-Systeme in der Intensivmedizin pro Patient und Tag rund 80 bis 95 Prozent Fehlalarme oder sogenannte Artefakte sind und damit tatsächlich auch keine unmittelbare Handlung notwendig wird. Wird aber auf einen tatsächlichen Alarm zu spät reagiert, kann dies für den betroffenen Patienten auch tödlich enden (Wilken et al. 2017). So kam es zwischen 2005 und 2010 in der durch die U. S. Food & Drug Administration (FDA) geführten Datenbank mit 566 gemeldeten „Alarm-bezogenen Todesfällen" zu schwerwiegenden Zwischenfällen im Zusammenhang mit der Anwendung von Medizinprodukten (MAUDE 2018).

Auswertung nach sektorenübergreifenden Aspekten: Publikationen, die sich im Schwerpunkt mit den Patientenrisiken aus explizit sektorenübergreifenden digitalen Anwendungen befassen

▪ Schwerpunktmäßig untersuchte Health-IT-Produktkategorien bzw. Funktionalitäten

- Elektronische Patientenakten (EHR)
- Systeme zur Unterstützung des Entlassmanagements
- Systeme zur Unterstützung von Übergaben im Krankenhaus (Hand-over)

▪ Untersuchte Funktionen zur Minimierung von Patientenrisiken

Ein zentrales Einsatzfeld von Health IT ist die Unterstützung des „Versorgungskontinuums" (continuity of care), nicht nur zwischen den unterschiedlichen Funktionseinheiten eines Krankenhauses, sondern insbesondere auch als Verbindung zwischen den Sektoren. Beim Übergang vom Krankenhaus in die ambulante Versorgung ermöglichen es digitale Anwendungen wie die elektronische Patientenakte, patientenbezogene Daten und Informationen für alle Akteure, vollständig, nachvollziehbar und aktuell bereitzustellen. Der Vorteil bzw. Nutzen, den dies gegenüber reinen papierbasierten Informationsübermittlungen entfaltet, wird in den hier eingruppierten Publikationen untersucht und grundsätzlich bestätigt (Okoniewska et al. 2012).

Dabei wird jedoch auch offensichtlich, dass ein elektronisch unterstütztes Entlassmanagement einschließlich der Ausstellung eines digitalen Medikationsplans oder Rezepts nur so gut sein kann wie die Dokumentation der Daten in den vorausgegangenen Prozessschritten. Die dort möglichen Fehler,

z. B. im Rahmen der Ermittlung einer korrekten Dosierung, können so auch nach Entlassung eines Patienten noch zu kritischen Ereignissen führen (Caruso et al. 2015).

10.3.3 Einschränkungen

Aufgrund der Operationalisierung von „Digitalisierung" über einzelne Suchbegriffe können Einschränkungen bei der PubMed-Literaturrecherche bestehen. Es fehlt eine allgemein akzeptierte und übergreifend verwendete Definition der „Digitalisierung" (▶ Abschn. 10.2.1). Da es sich um eine sehr allgemeine und weitreichende Begrifflichkeit handelt, besteht die Möglichkeit, dass anhand der Suchbegriffe möglicherweise nicht alle relevanten Aspekte des Themas erfasst wurden.

Ferner erforderte der Such-Algorithmus zwingend einen Bezug zur stationären Versorgung (UND-Verknüpfung). Somit konnten Publikationen, die sich grundsätzlich zu Zusammenhängen zwischen Digitalisierung und Patientensicherheit äußern und möglicherweise für die Arbeit von Interesse gewesen wären, nicht gefunden werden.

10.4 Diskussion

In der Gesamtschau der Ergebnisse lässt sich grundsätzlich feststellen, dass die Anzahl der Artikelfunde in den drei definierten Domänen sehr heterogen verteilt ist. So sind rein technisch begründete Patientenrisiken mit 18 von 311 Treffern (5,8 Prozent) nur in begrenztem Umfang Gegenstand von Publikationen bzw. Studien. Patientenrisiken allein aufgrund von fehlerhaftem Gebrauch von Health IT werden in 29 Treffern (9,3 Prozent) thematisiert. Darstellungen zu Kombinationen von fehlerhafter Technik und nicht intendierter Anwendung finden sich in ähnlicher Größenordnung: 19 Treffer (6,1 Prozent). Inwiefern man angesichts dieser Zahlen von einer angemessenen oder zu geringen Repräsentation der Thematik in der Literatur sprechen kann, muss, da geeignete Vergleichsmaßstäbe fehlen, dem subjektiven Empfinden des Lesers überlassen werden. Inhaltlich sprechen die gefundenen Publikationen hinsichtlich der ermittelten Risiken für die Patienten durch fehlerhafte Health IT oder fehlerhafte Anwendung derselben jedenfalls eine deutliche Sprache.

Der Schwerpunkt der Treffer liegt eindeutig in Untersuchungen zu den Anwendungen, die explizit zur Verbesserung der Patientensicherheit beitragen sollen (144 von 311, Domäne 3). Dies ist insofern plausibel, als dass diese Health-IT-Anwendungen nicht nur mit Blick auf die Patientensicherheit, sondern auch in Hinblick auf ihre Überlegenheit in Bezug auf den ursprünglichen, häufig papierbasierten Prozess analysiert werden. Die Kombination mit den anwenderinduzierten Problemen wird in weiteren 95 Treffern (Domäne 2 und 3) thematisiert, was wiederum deutlich zeigt, dass die Nachteile solcher Systeme sehr häufig mit der Interaktion zwischen Menschen und Maschinen zusammenhängen. Durch die nicht bestimmungsgerechte Anwendung von Health IT – unabhängig davon, ob durch unzureichende Schulung oder wenig intuitive Workflows und Nutzerführung – entstehen nicht intendierte Effekte bis hin zu kritischen Ereignissen mit Todesfolge, wie sie beispielsweise im Zusammenhang mit der Alarm Fatigue dokumentiert sind (MAUDE 2018).

- **Prozessunterstützende Anwendungen zeigen großes Potenzial – entscheidend dabei ist die Mensch-Computer-Interaktion**

Vielversprechende digitale Anwendungen zur Stärkung der Patientensicherheit (Domäne 3) sind CPOE-Systeme – dort häufig bezogen auf den Anwendungsfall „Verbesserung der Arzneimitteltherapiesicherheit" und in Verbindung mit Health-IT-Komponenten wie der elektronischen Verordnung, dem Medikationsplan oder spezieller Dosiskalkulations- und Warnsysteme. Der Nutzen solcher Systeme erschließt sich unmittelbar, geht man davon aus, dass rund die Hälfte der Medikationsfehler als vermeidbar gilt und jährlich mehr als 50.000 Patienten aufgrund von Fehlern in der Arzneimitteltherapie sterben. Fehler und damit Patientenrisiken können im gesamten Medikationsprozess entstehen, beginnend mit Doppelverordnungen, Nicht-Berücksichtigung von Dosisanpassungen, Übersehen von Gegenanzeigen oder Wechselwirkungen bzw. einfachen Lesefehlern. Oder sie geschehen später im Rahmen der Zubereitung bzw. Anwendung von

Arzneimitteln. Der gesamte Ablauf kann durch integrierte digitale Anwendungen unterstützt werden, durch die sich die genannten Risiken reduzieren lassen. Allerdings zeigen einzelne Studien ebenfalls sehr klar, dass dabei technologie- und anwenderinduzierte Probleme auftreten können, die wiederum dem Nutzen gegenübergestellt werden müssen. Aus diesem Grunde fällt die Bilanz mit Blick auf potenzielle Sicherheits-, Effizienz- und Effektivitätsgewinne nicht immer eindeutig aus (Stürzlinger et al. 2009).

Zur Erhöhung der Arzneimitteltherapiesicherheit erfolgt häufig der Einsatz von unterschiedlich komplexen, wissensbasierten Systemen zur Entscheidungsunterstützung. Dabei erhält der Anwender automatisiert fallbezogene Hinweise oder zusätzliche Informationen zur Entscheidungsfindung. In aufwändigen Systemen liegen diesen Empfehlungen komplexe Algorithmen zugrunde. Schleichen sich hier Fehler ein, kann das zu kritischen Ereignissen führen. Daraus resultieren auf der einen Seite hohe Anforderungen an die Vollständigkeit und Konsistenz der Daten, die zur Berechnung der Algorithmen verwendet werden. Auf der anderen Seite bedarf es konsequenter Validierungs- und Testmaßnahmen, um das Vertrauen in die gelieferten Informationen zu rechtfertigen (Huckvale et al. 2010).

Ein weiteres großes Thema ist die elektronische Patientenakte (EHR), verstanden als patientenbezogene, sektoren- und fächerübergreifend angelegte Akte, in der Gesundheitsinformationen strukturiert abgelegt und definierten Adressaten zugänglich gemacht werden. Im Rahmen dieses Artikels wird auf die in Deutschland aktuell diskutierten Ausdifferenzierungen verzichtet – zumal die gefundenen Studien dazu nicht aus dem deutschsprachigen Raum stammen. Hier geht es im Wesentlichen um die Digitalisierung von relevanten medizinischen Informationen, die über den Versorgungsprozess hinweg allen daran Beteiligten zur Verfügung gestellt werden. Der Nutzen liegt in der daraus entstehenden Transparenz und der Möglichkeit des schnellen Zugriffs auf z. B. notfallrelevante Informationen. Doppeluntersuchungen und -verordnungen lassen sich vermeiden, der Patient hat selbst einen Überblick über seine Anamnese und laufenden Therapien. Darüber hinaus können mit Inhalten der digitalen Akten Risiko-Scores ermittelt und verbundene Warnsysteme getriggert werden. Auch hier ist der Effekt auf die Patientensicherheit offensichtlich – aber die technologie- und anwenderinduzierten Probleme ähneln denen bereits unter CPOE genannten. Letztgenannte können zu kritischen Ereignissen und damit zu substanziellen Patientenschäden führen und relativieren damit den erwarteten Nutzen für die Patientensicherheit. Chancen und Risiken von Health IT bleiben darüber hinaus in diesem Anwendungsbereich (EHR) nicht immer auf einen Sektor beschränkt.

Prüft man die in der Einleitung geweckten Erwartungen an den Einsatz von künstlicher Intelligenz (KI) zur Entscheidungsunterstützung und Verbesserung der Patientensicherheit, so war in der Literaturrecherche wenig dazu zu finden. Yokota et al. (2017) erprobten einen Algorithmus, um mit Hilfe von im Krankenhaus verfügbaren Daten Patienten mit erhöhtem Sturzrisiko zu identifizieren, allerdings mit verbesserungsbedürftigen Werten für die Sensitivität und Spezifität. Nakas et al. (2016) nutzten KI-Algorithmen, um die Krankenhaus-Sterblichkeit vorherzusagen. Erwähnenswert ist die Arbeit von Shimabukuro et al. (2017), da hier der seltene Fall einer randomisierten kontrollierten Studie vorliegt, bei der der KI-basierte Ansatz mit einem herkömmlichen Sepsis-Scoring verglichen wurde. Die nachfolgende Behandlung der identifizierten Fälle war in KI- und Kontrollgruppe gleich. Im Ergebnis waren Krankenhaussterblichkeit und Verweildauer in der KI-Gruppe geringer als in der Vergleichsgruppe. In allen hier erwähnten Publikationen wurde die KI als prognostisches Instrument eingesetzt. Die Qualität von konkreten Handlungsempfehlungen durch KI scheint aktuell für einen Routineeinsatz nicht ausreichend zu sein, wie auch an den wieder abgebrochenen Versuchen mit IBMs Watson-System zu sehen ist (Nelson 2018).

Ansätze zum Umgang mit den Risiken – Transparenz ist der Schlüssel

Insgesamt erfährt der Zusammenhang zwischen Digitalisierung und Patientensicherheit eine zunehmende Aufmerksamkeit. Aus diesem Grunde erhält die systematische und übergreifende Befassung mit den intendierten und nicht intendierten Effekten von Health IT eine immer größere Bedeutung. Ent-

sprechende Initiativen und Forschungsaktivitäten von zumeist international besetzten Teams finden zunehmend Niederschlag in Konzepten und Publikationen der Bio- und Medizininformatik. Dort werden die Themen wie sicheres HIT-Design, sichere HI-Implementierung, Berichtssysteme für technologieinduzierte Fehler, Fehleranalysesysteme und HIT-Risikomanagement diskutiert und weiterentwickelt (Borycki et al. 2016).

Bereits 2012 führte das ECRI Institute einen sogenannten „Deep Dive" durch, in dem auf Basis von 171 von Krankenhäusern gemeldeten Health-IT-bezogenen Ereignissen zunächst eine Klassifikation dieser Ereignisse mit Blick auf ihre Sicherheitsrelevanz vorgenommen wurde. Danach wurden risiko-reduzierende Strategien entwickelt und strukturiert dargestellt. Grundlage dafür bildete der Health-IT-Lebenszyklus: Planung/Vorbereitung, Implementierung und kontinuierliche Verbesserung sowie durchgehendes Monitoring. Abschließend erfolgte eine Bewertung der Wirkung (impact) der eingesetzten Maßnahmen (ECRI 2013).

Von besonderem Interesse für den deutschsprachigen Raum sind die Handlungsempfehlungen, die das APS gemeinsam mit Patientensicherheitsorganisationen aus Österreich und der Schweiz zu diesem Thema erarbeitet hat (Aktionsbündnis Patientensicherheit e. V. 2018b). Dabei haben sie sich auf ausgewählte Risikobereiche konzentriert. Zusätzlich zum hier bereits beschriebenen Risiko für die Patientensicherheit durch Ausfall oder Störung der IT-Infrastruktur oder durch mangelnde digitale Kompetenz der Anwender werden Gefahren durch Cyberangriffe, durch Verletzung des Datenschutzes, durch fehlerhafte Einbindung aktiver Medizinprodukte und durch die Überlassung von Patientendaten an Cloud-Dienste analysiert. Der besondere Wert der genannten Veröffentlichung liegt in den jeweils dazugehörigen Empfehlungen zur Risikominderung.

Für die Krankenhäuser, die nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik als „kritische Infrastruktur" gelten, erarbeitet die Deutsche Krankenhausgesellschaft derzeit einen branchenspezifischen Sicherheitsstandard, der diese Krankenhäuser in die Lage versetzen soll, kritische Systeme, Prozesse und Komponenten zu identifizieren und angemessene technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT zu treffen (Holzbrecher-Morys 2018). Dieser Standard soll perspektivisch auch als Leitfaden zur Erhöhung der IT-Sicherheit in allen Krankenhäusern genutzt werden. Dabei geht es nicht nur um die Vermeidung externer Hackerangriffe wie dem im Lukaskrankenhaus in Neuss, sondern auch um die grundsätzliche Sensibilisierung für das Thema und eine Professionalisierung des Umgangs damit (Krüger-Brand 2017).

Patientensicherheit und Digitalisierung ist jedoch kein reines Technikthema, das ausschließlich von IT-Experten zu lösen ist. Die identifizierten Chancen und Risiken auszubalancieren ist vielmehr eine mehrdimensionale und multiprofessionelle Herausforderung:

- Für die Hersteller: Health IT muss nutzerorientiert gestaltet und intuitiv bedienbar sein sowie sicher implementiert und betrieben werden können. Dazu gehört der Einsatz von Standards, die Sicherstellung der Interoperabilität von Systemen ebenso wie eine rigorose Testung und kontinuierliche Pflege.
- Für die Anwender: Health IT kann nur sicher und bestimmungsgerecht angewendet werden, wenn neben den digitalen Produkten auch die damit verbundenen (neuen) Workflows regelmäßig geschult und trainiert werden. Dazu gehört auch die Motivation zur Übernahme einer aktiven Rolle im Rahmen des Digitalisierungsprozesses im Krankenhaus zu fördern (Savage et al. 2010; Menon et al. 2017).
- Für die Verantwortlichen im Krankenhaus: Health IT ist ein strategisches Thema mit einem starken Bezug zum übergreifenden Risikomanagement. Auswahl und Einführung von neuen Systemen sollten auch mit Blick auf die Patientensicherheit erfolgen, d. h. es sind gleichzeitig Mechanismen zur Identifikation und Vermeidung von Fehlern zu etablieren. Eine gelebte „Fehlerkultur" hilft alle Mitarbeiter aktiv einzubinden und eine hohe Akzeptanz für die Health IT zu erreichen (Feldman et al. 2018).
- Für die Wissenschaft: Health IT ist ein aktives Element in einem komplexen Umfeld, das in der Versorgungs- und IT-Forschung als „sozio-

technisches System“ beschrieben wird (Schrappe 2018). Daraus ergibt sich für die weitergehende wissenschaftliche Befassung mit dem Thema – neben der Schaffung von Transparenz über kritische Ereignisse – die Notwendigkeit von interdisziplinären Ansätzen, mit denen die häufig noch ausstehende Evidenz für den Nutzen des Einsatzes digitaler Anwendungen geschaffen werden kann.

10.5 Fazit

Der auf einer systematischen Literaturrecherche basierende Review mit Schwerpunkt auf der Krankenhausversorgung macht deutliche Zusammenhänge zwischen Digitalisierung und Patientensicherheit sichtbar.

Dabei zeigt die Digitalisierung hinsichtlich ihrer Bedeutung für die Patientensicherheit zwei Gesichter: Einerseits kann sie mit bestimmten Anwendungen zu einer Verbesserung der Patientensicherheit führen, andererseits ergeben sich aus technischen Mängeln in IT-Systemen oder ihre fehlerhafte Anwendung teils gravierende Risiken für den Patienten. Dieses gemeinsame Auftreten von Chancen und Risiken für die Patientensicherheit findet sich deutlich auch bei Anwendungen, denen eine zentrale Rolle bei der Digitalisierung der gesundheitlichen Versorgung zugeschrieben wird: der elektronischen Patientenakte, den Systemen zur Entscheidungsunterstützung und der computergestützten Medikamentenverordnung (CPOE).

Um solche Risiken zu vermeiden und die Potenziale der Digitalisierung zur Verbesserung der Patientensicherheit zu realisieren, sind – begleitet durch interdisziplinäre Forschung – fortwährende gemeinsame Anstrengungen von Herstellern, Anwendern, System-Planern und Betreibern erforderlich. Eine wesentliche Voraussetzung dafür ist die Schaffung von Transparenz: sicherheitsrelevante Vorkommnisse, die im Zusammenhang mit der Verwendung von Health IT entstehen, sollten strukturiert dokumentiert und veröffentlicht werden, damit alle Akteure von diesem Wissen profitieren und entsprechende Vorkehrungen treffen können. Inwieweit hierzu zusätzliche gesetzliche und regulatorische Maßnahmen notwendig sind, beispielsweise zur Festlegung einheitlicher Standards, muss im Zusammenhang mit den weiteren Entwicklungen auf dem Gebiet der Digitalisierung diskutiert werden.

Literatur

Aktionsbündnis Patientensicherheit e. V. (2016) Einrichtung und erfolgreicher Betrieb eines Berichts- und Lernsystems (CIRS). Berlin

Aktionsbündnis Patientensicherheit e. V. (2018a) Glossar Patientensicherheit. http://www.aps-ev.de/glossar/. Zugegriffen: 15 August 2018

Aktionsbündnis Patientensicherheit e. V. (2018b) Digitalisierung und Patientensicherheit – HE 1. Handlungsempfehlung für das Risikomanagement in der Patientenversorgung. Berlin

Augurzky B, Krolop S, Mensen A et al (2018) Krankenhaus Rating Report 2018, 1. Aufl. medhochzwei, Heidelberg

Borycki E, Dexheimer JW, Hullin Lucay Cossio C et al (2016) Methods for Addressing Technology-induced Errors: The Current State. Yearb Med Inform 1:30–40

Bröckerhoff H-P (2018) E-HEALTH-COM: Trend-Guide Gesundheits-IT. https://e-health-com.de/compendien/trend-guide/. Zugegriffen: 21 August 2018

Caruso MC, Gittelman MA, Widecan ML, Luria JW (2015) Pediatric emergency department discharge prescriptions requiring pharmacy clarification. Pediatr Emerg Care 31:403–408

Clarke A, Adamson J, Watt I et al (2016) The impact of electronic records on patient safety: a qualitative study. BMC Med Inform Decis Mak 16:62

Colavecchia AC, Putney DR, Johnson ML, Aparasu RR (2017) Discharge medication complexity and 30-day heart failure readmissions. Res Soc Adm Pharm RSAP 13:857–863

Cresswell KM, Mozaffar H, Lee L et al (2017) Workarounds to hospital electronic prescribing systems: a qualitative study in English hospitals. BMJ Qual Saf 26:542–551

Czock D, Konias M, Seidling HM et al (2015) Tailoring of alerts substantially reduces the alert burden in computerized clinical decision support for drugs that should be avoided in patients with renal disease. J Am Med Inform Assoc JAMIA 22:881–887

ECRI (2013) Deep Dive: Health Information Technology. ECRI Institute, Plymouth Meeting

Feldman SS, Buchalter S, Hayes LW (2018) Health Information Technology in Healthcare Quality and Patient Safety: Literature Review. JMIR Med Inform 6:e10264

Grätzel von Grätz P (2017) Neuer Digital-Champion im Krankenhaussektor. E-Health-Com. https://e-health-com.de/details-news/neuer-digital-champion-im-krankenhaussektor/37e05326654e61cdedb2bd5860f6ded5/. Zugegriffen: 15 August 2018

Hagebeucker M, Hölscher N, Klass C, Roeder N (2018) Auf dem Weg zur Apotheke 4.0. Das Krankenhaus 4:302–311

Hampel E (2016a) Patientensicherheit im Krankenhaus 2025. Delphi-Studie mit Experten in der Gesundheitsversorgung (Teil 1). das Krankenhaus 4:286–290
Hampel E (2016b) Patientensicherheit im Krankenhaus 2025. Delphi-Studie mit Experten in der Gesundheitsversorgung (Teil 2). das Krankenhaus 5:387–392
Holzbrecher-Morys M (2018) IT-Sicherheit ist Patientenschutz. Klinikmanagement Aktuell Mai 2018:50–53
Huckvale C, Car J, Akiyama M et al (2010) Information technology for patient safety. BMJ Qual Saf 19:i25–i33
Institute of Medicine (US) Committee on Data Standards for Patient Safety (2004) Patient Safety: Achieving a New Standard for Care. National Academies Press (US), Washington, DC
Jurado-Román A, Sánchez-Pérez I, Lozano Ruíz-Poveda F et al (2016) Effectiveness of the implementation of a simple radiation reduction protocol in the catheterization laboratory. Cardiovasc Revascularization Med Mol Interv 17:328–332
KH-CIRS-Netz (2018) Fall-Nr. 37.779 „Patientenidentifikation in großen Krankenhaus-Datenbanken". Krankenhaus-CIRS-Netz Dtschl. https://www.kh-cirs.de/. Zugegriffen: 15 August 2018
KH-CIRS-Netz (2018) Fall-Nr. 153.015 „Medikamentenverordnung im noch aktiven Account von einer Pflegeperson durchgeführt". Krankenhaus-CIRS-Netz Dtschl. https://www.kh-cirs.de. Zugegriffen: 15 August 2018
KH-CIRS-Netz (2018) Fall-Nr. 167.939 „Medikamentenfehlanordnung durch Doppelanordnung". Krankenhaus-CIRS-Netz Dtschl. https://www.kh-cirs.de. Zugegriffen: 15 August 2018
KH-CIRS-Netz (2018) Fall-Nr. 173.609 „Erreichbarkeit des Bereitschaftsdienstes". Krankenhaus-CIRS-Netz Dtschl. https://www.kh-cirs.de. Zugegriffen: 15 August 2018
Kirkendall ES, Spooner SA, Logan JR (2014) Evaluating the accuracy of electronic pediatric drug dosing rules. J Am Med Inform Assoc JAMIA 21:e43–49
Krüger-Brand HE (2017) IT-Sicherheit im Krankenhaus: Cyberrisiken als Herausforderung. Dtsch Arztbl 114(42):A-1910/B1620/C-1586
MAUDE (2018) FDA Manufacturer and User Facility Device Experience Database. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm. Zugegriffen: 15 August 2018
Menon S, Singh H, Giardina TD et al (2017) Safety huddles to proactively identify and address electronic health record safety. J Am Med Inform Assoc JAMIA 24:261–267
Nakas CT, Schütz N, Werners M, Leichtle AB (2016) Accuracy and Calibration of Computational Approaches for Inpatient Mortality Predictive Modeling. PloS One 11:e0159046
Nelson R (2018) IBM Watson Oncology: Not Living Up to Expectations. Medscape Family Medicine. http://www.medscape.com/viewarticle/900746. Zugegriffen: 10 Oktober 2018
Office of the National Coordinator for Health Information Technology (ONC) (2018) Glossary of Selected Terms Related to Health IT. Gloss Sel Terms Relat Health IT. https://www.healthit.gov/topic/health-it-basics/glossary. Zugegriffen: 15 August 2018
Okoniewska BM, Santana MJ, Holroyd-Leduc J et al (2012) The Seamless Transfer-of-Care Protocol: a randomized controlled trial assessing the efficacy of an electronic transfer-of-care communication tool. BMC Health Serv Res 12:414
Roland Berger GmbH (2018) Roland Berger Krankenhausstudie 2018. München
Samy GN, Ahmad R, Ismail Z (2010) Security threats categories in healthcare information systems. Health Informatics J 16:201–209
Savage I, Cornford T, Klecun E et al (2010) Medication errors with electronic prescribing (eP): Two views of the same picture. BMC Health Serv Res 10:135
Sax U, Lipprandt M, Röhrig R (2016) The Rising Frequency of IT Blackouts Indicates the Increasing Relevance of IT Emergency Concepts to Ensure Patient Safety. Yearb Med Inform 130–137
Schrappe M (2018) APS-Weißbuch Patientensicherheit. Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin
Shimabukuro DW, Barton CW, Feldman MD et al (2017) Effect of a machine learning-based severe sepsis prediction algorithm on patient survival and hospital length of stay: a randomised clinical trial. BMJ Open Respir Res 4
Simon A (2017) Wie zufrieden sind Anwender mit der IT-Unterstützung im Krankenhaus? Pilotstudie zur empirischen Erhebung und Validierung der allgemeinen Zufriedenheit von IT-Anwendern im Krankenhaus. GMS Med Inf Biom Epidemiol 13(1):Doc04 (20171004)
Singh H, Sittig DF (2016) Measuring and improving patient safety through health information technology: The Health IT Safety Framework. BMJ Qual Saf 25:226–232
Spirk D, Stuck AK, Hager A et al (2017) Electronic alert system for improving appropriate thromboprophylaxis in hospitalized medical patients: a randomized controlled trial. J Thromb Haemost JTH 15:2138–2146
Stultz JS, Nahata MC (2014) Appropriateness of commercially available and partially customized medication dosing alerts among pediatric patients. J Am Med Inform Assoc JAMIA 21:e35–42
Stürzlinger H, Hiebinger C, Pertl D, Traurig P (2009) Computerized Physician Order Entry – effectiveness and efficiency of electronic medication ordering with decision support systems. GMS Health Technol Assess 5:Doc07
Swanson JO, Thapa MM, Iyer RS et al (2012) Optimizing peer review: A year of experience after instituting a real-time comment-enhanced program at a children's hospital. AJR Am J Roentgenol 198:1121–1125
Thomeczek C, Bock W, Conen D et al (2004) Das Glossar Patientensicherheit – Ein Beitrag zur Definitionsbestimmung und zum Verständnis der Thematik „Patientensicherheit" und „Fehler in der Medizin". Gesundheitswesen 66:833–840
Townsend AB, Valle-Ortiz M, Sansweet T (2016) A Successful ED Fall Risk Program Using the KINDER 1 Fall Risk Assessment Tool. J Emerg Nurs JEN Off Publ Emerg Dep Nurses Assoc 42:492–497

Trinh Q-D, Sammon J, Sun M et al (2012) Perioperative outcomes of robot-assisted radical prostatectomy compared with open radical prostatectomy: results from the nationwide inpatient sample. Eur Urol 61:679–685

Vélez-Díaz-Pallarés M, Álvarez Díaz AM, Gramage Caro T et al (2017) Technology-induced errors associated with computerized provider order entry software for older patients. Int J Clin Pharm 39:729–742. doi: 10.1007/s11096-017-0474-y

Wilken M, Hüske-Kraus D, Klausen A et al (2017) Alarm Fatigue: Causes and Effects. Stud Health Technol Inform 243:107–111

World Health Organization (2002) Quality of care: patient safety. Resolution WHA 55.18. 55th World Health Assembly, Geneva

World Health Organization (2017) Patient Safety: Making health care safer. Geneva

Wright A, Hickman TT, McEvoy D et al (2016) Analysis of clinical decision support system malfunctions: a case series and survey. J Am Med Inform Assoc JAMIA 23:1068–1076

Yokota S, Endo M, Ohe K (2017) Establishing a Classification System for High Fall-Risk Among Inpatients Using Support Vector Machines. Comput Inform Nurs CIN 35:408–416

Yu H, Hevelone ND, Lipsitz SR et al (2012) Comparative analysis of outcomes and costs following open radical cystectomy versus robot-assisted laparoscopic radical cystectomy: results from the US Nationwide Inpatient Sample. Eur Urol 61:1239–1244