universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

Digitalisierung in der Pflege Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag

verfasst von / submitted by

Florian Kunze, B.Sc.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 242
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Risikoprävention und Katastrophenmanagement
Betreut von / Supervisor:	Prof. Dr. rer. Medic Inge Eberl MScN, BScN

Danksagung

An dieser Stelle möchte ich Frau Prof. Dr. Eberl danken, dass Sie sich bereiterklärt hat mich auch bei meiner Masterarbeit weiter zu unterstützen und zu betreuen.

Des Weiteren möchte ich mich bei Herrn Frey für die Betreuung der Masterarbeit seitens des Klinikum Ingolstadts bedanken.

Ein herzliches Dankeschön geht ebenfalls an die Experten, die mich bei meinem Vorhaben unterstützt haben.

Der größte Dank geht an meine Familie und meinen Partner, die mich in allen Höhen und Tiefen während meines Masterstudiengangs in Wien begleitet und unterstützt haben.

Kurzfassung

Die Digitalisierung in der Pflege bringt eine Vielzahl von Vorteilen mit sich. Es müssen aber auch eine Reihe von Herausforderungen bewältigt werden. Dies wird vor allem im Bereich der elektronischen Patientenakte in Krankenhäusern deutlich.

Das Ziel dieser Masterthesis besteht darin, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert erarbeiten und Handlungsempfehlungen daraus ableiten zu können.

Um dieses Ziel zu erreichen, wurden sechs Forschungsfragen festgelegt:

- Was sind die Vorteile von digitalen Dokumentationssystemen gegenüber papiergestützter Dokumentation im akutstationären Setting?
- Welche Patientendaten müssen im Falle eines Ausfalls der IT-Struktur im akutstationären Setting den am Patienten tätigen Personen zur Verfügung stehen, wenn der Zugriff auf die elektronische Patientenakte nicht mehr möglich ist oder Datensätze verloren gegangen sind?
- Sind elektronische Patientenakten im Klinikalltag vulnerabler gegen Cyberangriffe als papiergebundene Patientenakten?
- Welche Anforderungen muss eine elektronische Patientenakte im akutstationären Setting in Hinblick an die Datenverfügbarkeit, den Datenschutz und die Sicherheit erfüllen?
- Welche Rahmenbedingungen müssen erfüllt sein, damit die elektronische Patientenakte im Klinikalltag implementiert werden kann?
- Welche Akteure im Krankenhaus müssen bei der Implementierung der elektronischen Patientenakte miteinbezogen werden, um eine gelungene Einführung der elektronischen Patientenakte zu erreichen?

Zur Beantwortung der Forschungsfragen wurden im Rahmen eines qualitativen Forschungsdesigns 15 Experteninterviews geführt und anschließend inhaltsanalytisch ausgewertet.

Die Ergebnisse zeigen, dass die Implementierung und der Betrieb einer digitalen Patientenakte im Krankenhaus komplex sind. Neben der Sicherheit der Systeme, spielen gesetzliche, operative und wirtschaftliche Aspekte eine entscheidende Rolle.

Die Digitalisierung in der Pflege bietet Raum für weitere Forschungsvorhaben, beispielsweise die Entwicklung von Schulungskonzepten.

Abstract

Digitization in nursing care brings with it a host of benefits. However, a number of challenges must also be overcome. This is particularly evident in the area of electronic patient records in hospitals.

The aim of this master's thesis is to develop requirements for nursing documentation in the IT-supported patient file in a scientifically sound manner and to be able to derive recommendations for action.

To achieve this goal, six research questions were defined:

- What are the advantages of digital documentation systems over paper-based documentation in the acute inpatient setting?
- In the event of a failure of the IT structure in the acute inpatient setting, what patient data must be available to those working on the patient if access to the electronic patient record is no longer possible or data records have been lost?
- Are electronic patient records in the hospital setting more vulnerable to cyberattacks than paper-based patient records?
- What requirements must an electronic patient record meet in the acute inpatient setting with regard to data availability, data protection and security?
- What framework conditions must be met for the electronic patient record to be implemented in the hospital setting?
- Which hospital stakeholders need to be involved in the implementation of the electronic health record in order to achieve a successful introduction of the electronic health record?

To answer the research questions, 15 expert interviews were conducted as part of a qualitative research design and then evaluated using content analysis.

The results show that the implementation and operation of a digital patient record in hospitals is complex. In addition to the security of the systems, legal, operational and economic aspects play a decisive role.

Digitization in nursing care offers scope for further research projects, such as the development of training concepts.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

b.B.	bei Bedarf
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfJ	Bundesamt für Justiz
BKA	Bundeskriminalamt
BLÄK	Bayerische Landesärztekammer
BMG	Bundesgesundheitsministerium
BMI	Bundesministerium des Innern
BMJV	Bundesministerium für Justiz und für Verbraucherschutz
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStK	Bayerische Staatskanzlei
ComSec	Commonwealth Secretariat
CTO	Commonwealth Telecommunications Organisation
DIN	Deutsches Institut für Normung
DKI	Deutsches Krankenhausinstitut
DRG	Diagnosis Related Groups
DSGVO	Datenschutz-Grundverordnung
EC	European Commission
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EN	Europäische Norm
EU	Europäische Union
EUR-OP	Amt für Veröffentlichungen der Europäischen Union
FAQ	Frequently Asked Questions
GmbH	Gesellschaft mit beschränkter Haftung
IEC	International Electrotechnical Commission
iOK	induktive Oberkategorie
IoT	Internet-of-Things
ISO	International Organization for Standardization
IT	Informationstechnologie

ITU	International Telecommunication Union
iUK	induktive Unterkategorie
KI	Künstliche Intelligenz
KIS	Krankenhausinformationssystem
KRITIS	Kritische Infrastruktur
kV	Kilovolt
MS Teams	Microsoft Teams
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
o.J.	ohne Jahresangabe
o.S.	ohne Seitenangabe
OK	Oberkategorie
PC	Personal Computer
PDF	Portable Document Format
PIN	Persönliche Identifikationsnummer
QDA	Qualitative Datenanalyse
QR-Code	Quick Response Code
SGB	Sozialgesetzbuch
SGD	Studiengemeinschaft Werner Kamprath Darmstadt GmbH
SPSS	Sammeln, Prüfen, Sortieren, Subsumieren
StMGP	Bayerisches Staatsministerium für Gesundheit und Pflege
UK	Unterkategorie
UKD	Universitätsklinikum Düsseldorf
UNDRR	United Nations Office for Disaster Risk Reduction
UNISDR	United Nations International Strategy for Disaster Reduction
UP KRITIS	früher: Umsetzungsplan Kritische Infrastrukturen; jetzt: Eigennamen des Gremiums KRITIS
VR	Virtual-Reality
WLAN	Wireless Local Area Network
z.B.	zum Beispiel

1. Einleitung, Relevanz und Problemstellung

Auch im Gesundheitswesen (z.B. Krankenhäuser) spielt das Thema Digitalisierung eine wichtige Rolle. Krankenhäuser versprechen sich durch die Digitalisierung eine qualitative, effiziente und hochwertige Patientenversorgung. Jedoch hinken deutsche Krankenhäuser in Sachen Digitalisierung hinter her (Dörries, Gensorowsky & Greiner, 2017).

In einer vom Bundesministerium für Wirtschaft und Energie in Auftrag gegebenen Studie wurde deutlich, dass das deutsche Gesundheitswesen in Sachen Digitalisierung auf einem niedrigen Level ist und im Vergleich von unterschiedlichen Branchen an letzter Stelle steht (Bundesministerium für Wirtschaft und Energie [BMWi], 2017).

Dabei bringt die Digitalisierung im Gesundheitswesen viel Potenzial mit sich. Nutzenpotenzial lässt sich bei allen drei Akteuren im Gesundheitswesen erkennen. Den ersten Akteur stellt der Leistungserbringer dar. Für ihn kann Digitalisierung bedeuten, dass sich Prozesse beschleunigen und der Einsatz von Ressourcen effizienter gestalten lassen. Aber auch die transsektorale Vernetzung mit anderen Akteuren im Gesundheitswesen kann dadurch gefördert und gestärkt werden. Ein weiterer wichtiger Faktor für den Leistungserbringer kann die verbesserte Information und transparentere Kommunikation aller Beteiligter durch individualisierte Zugriffsrechte sein. Dies kann zu einer Verbesserung der Versorgungsqualität führen (Dörries et al., 2017).

Als weiterer Akteur im Gesundheitswesen ist der Patient selbst und seine Angehörigen anzuführen. Hier kann die Digitalisierung u.a. zu einer Verbesserung und Erhöhung des Patienten Empowerments beitragen (Dörries et al., 2017). Dies kann durch die Bereitstellung von digitalen Chroniker-Tagebüchern, Apps, und digitalen Gesundheitsportalen geschehen, welche die Position des Patienten durch Informationen, Mitwirkungsmöglichkeiten und Mitentscheidung verbessern (Reichardt & Gastmeier, 2013; Thranberend, Knöppler & Neisecke, 2016). Durch den einfachen Zugriff auf Gesundheits-Apps und die Nutzung von zielgruppenspezifischen Informationsangeboten (z.B. Gesundheits-Apps für Jugendliche) wird die Patientenadhärenz unterstützt. Durch die Einführung von Videosprechstunden und elektronischen Rezepten kann die Patientenversorgung und die Lebensqualität des Patienten durch beispielsweise verkürzte Wege- und Wartezeiten verbessert werden (Bundesgesundheitsministerium [BMG], 2019b; Dörries et al., 2017). Ein letztes und wichtiges Potenzial stellt die Verbesserung des Patientenoutcomes dar (Dörries et al., 2017). Diabetes-Apps können dazu beitragen, den Therapieerfolg signifikant zu erhöhen. So zeigt eine Studie von Kebede und Pischke (2019), dass das Selbstpflegeverhalten vor allem in den Bereichen ‚Blutzuckermessung', ‚Aktivität' und ‚allgemeine Ernährung' von App-Benutzern signifikant höher ist als das der Nicht-App-Benutzer (Kebede & Pischke, 2019).

Die übrigen Akteure stellen die Gesellschaft und die Kostenträger dar. Hier kann die Digitalisierung dazu beitragen, dass die angebotenen Gesundheitsdienstleistungen

transparent und nachvollziehbar werden (z.B. gesundheits- und krankheitsbezogene Statistiken für jedermann abrufbar). Des Weiteren werden unnötige Doppelbehandlungen vermieden, was wiederum wichtige Ressourcen einspart. Auch die Kosten-Nutzen-Relation kann durch zielgerichtete Digitalisierung verbessert werden (Dörries et al., 2017).

Die Digitalisierung im Gesundheitswesen bringt aber auch eine Vielzahl von Herausforderungen mit sich. So kommt es z.B. immer wieder zu Cyberangriffen auf Krankenhäuser. Eines der aktuellsten Beispiele ist das Universitätsklinikum Düsseldorf (UKD). Am 10.09.2020 gegen 03:00 wurde das UKD Opfer eines Hackerangriffes. Der Täter verschlüsselte das IT-System des Klinikums, was dazu führte, das große Teile der IT-gestützten Systeme ausfielen. Das Krankenhaus wurde von der Notfallversorgung abgemeldet, die Notaufnahme geschlossen und das OP-Programm auf Notfälle beschränkt. Ein Patient verlor durch die verzögerte Behandlung und die Verlegung in ein anderes Krankenhaus sein Leben (Kucera, 2020).

Aber auch andere Krankenhäuser waren bereits Opfer von Hackerangriffen:

- 12/2019: Hackerangriff auf das Klinikum in Fürth/Bayern (Kucera, 2020)
- 10/2019: Hackerangriff auf elf Krankenhäuser in Rheinlandpfalz und Saarland (Kucera, 2020)
- Januar/Februar 2016: Hackerangriff auf 28 Krankenhäuser in Nordrhein-Westfalen. Unter anderem das Lukaskrankenhaus in Neuss mit einem Schaden von etwa 1.000.000 € (Kucera, 2020; Ludwig, 2016)

Ein weiteres großes Problem welches die Digitalisierung mit sich bringt, besteht bei der Software. Die aktuell verwendete Software bei IT-Systemen wie z.B. PC, Smartphone, Notebook, beinhaltet viele Schwachstellen. Die Qualität der aktuellen Betriebssoftware ist für die derzeit herrschende Bedrohungslage nicht mehr ausreichend (Pohlmann, 2019). Pohlmann (2019) erläutert die Fehlerdichte von Softwaresystemen:

„Die Fehlerdichte – die Anzahl der Softwarefehler pro 1 000 Zeilen Code – liegt bei qualitativ hochwertiger Software heute im Schnitt bei 0,3. Da gängige Betriebssysteme und größere Anwendungen mehr als zehn Millionen Zeilen Code haben, sind hier im Schnitt 3 000 Software-Fehler zu finden“ (Pohlmann, 2019, : 56).

Bei der Digitalisierung muss zudem eine Reihe von gesetzlichen Rahmenbedingungen berücksichtigt und erfüllt werden. Diese Gesetze regeln u.a. die datenschutzrechtlichen Bestimmungen und die zu treffenden Sicherheits- und Schutzmaßnahmen bei der Einführung und beim Betrieb digitaler Infrastrukturen sowie die gesetzlichen Rahmenbedingungen für den Auf- und Ausbau digitaler Versorgungsstrukturen im Gesundheitswesen. Ziele dieser Gesetze sind, neben der Sicherung der Datenschutzanforderungen, die Verbesserung der Patientenversorgung sowie die Verbesserung der digitalen Infrastrukturen im Gesundheitswesen:

- Digitale-Versorgung-Gesetz (Bundesgesundheitsministerium [BMG], 2020a)
- Das zukünftige Krankenhauszukunftsgesetz (Bundesgesundheitsministerium [BMG], 2020b)

- Patientendaten-Schutzgesetz (Bundesgesundheitsministerium [BMG], 2020c)
- Gesetz für mehr Sicherheit in der Arzneimittelversorgung (Bundesgesundheitsministerium [BMG], 2019a)
- Terminservice- und Versorgungsgesetz (BMG, 2019b)
- EU-Datenschutzgrundverordnung (Engel jun., 2018; Erwig, 2019)
- Bundesdatenschutzgesetz (Engel jun., 2018)
- Sozialgesetzbuch SGB V (Gesellschaft für Telematikanwendungender Gesundheitskarte mbH [gematik], 2019)
- Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) (Deutscher Bundestag, 2015)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (Bundesministerium der Justiz und für Verbraucherschutz [BMJV] & Bundesamt für Justiz [BfJ], 2009)
- IT-Sicherheitsgesetz (Bundesamt für Sicherheit in der Informationstechnik [BSI], o.J.a)
- RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2013; Europäische Union [EU], 2008)

Eine weitere Herausforderung welche die Digitalisierung mit sich bringt zeigt sich im Krankenhaussektor. Die im Rahmen der Digitalisierung eingeführten elektronischen Patientenakten im Krankenhaus sind vulnerabel gegenüber Stromausfällen, Hackerangriffen, IT-Ausfällen und Schnittstellenproblemen bzw. Softwareproblemen.

So können längere Stromausfälle Auswirkungen auf den Zugriff zu den Daten von elektronischen Patientenakten haben. Wie weitreichend ein solcher langfristiger Stromausfall ist, zeigt ein Vorkommnis in Berlin im Jahr 2019. So kam es zwischen 19.02.2019 und 20.02.2020 in Berlin-Köpenick zu einem 31-Stündigem Stromausfall, nachdem im Rahmen von Baggerarbeiten zwei 110-kV-Hochspannungskabel zerstört wurden. Im betroffenen Berlin Stadtteil Köpenick befindet sich auch ein Krankenhaus des Deutschen Roten Kreuzes. Die in der Klinik vorhandenen Notstromaggregate sprangen kurz nach dem Stromausfall ohne Probleme an. Da sich der Stromausfall über längere Zeit hinzog, begannen die Notstromaggregate instabil zu Laufen. Wenig später fielen die Notstromaggregate vollständig aus. Ein weiteres Problem stellten die Rechner, welche zum großen Teil nicht am Notstromaggregat angeschlossen waren, dar. Der Zugriff auf wichtige Telefonnummern war nicht möglich (Höhne & Lenz, 2019).

Daraus lässt sich ableiten, dass auch der Zugriff auf elektronische Patientenakten bei einem Ausfall der Rechner, die nicht am Notstrom angeschlossen sind, zu diesem Zeitpunkt nicht möglich war. Somit ist auch der Zugriff auf wichtige Laborparameter, Medikamentenanordnungen und Befunden nicht möglich, was zu einer inadäquaten Versorgung der Patienten führen kann. Zudem ist es für den Laien auf den ersten Blick nicht möglich herauszufinden, welche weiteren Konsequenzen (z.B. fehlende,

veränderte oder falsch zugeordnete Patientendaten) der Ausfall der IT-Struktur mit sich gebracht hat.

Aber auch die Gefahr eines IT-Ausfalls spielt eine wichtige Rolle, wenn es um das Thema Digitalisierung geht. Sax, Lipprandt und Röhrig (2016) stellen drei IT-Probleme dar, die für den Anwender von großer Bedeutung sind. Zum einen spielt die mangelnde Systemverfügbarkeit eine Rolle. Wenn Benutzer das benötigte System nicht benutzen bzw. nicht darauf zugreifen können, kommt es für den Anwender zu einer Handlungsunfähigkeit. Diese Handlungsunfähigkeit ist wiederum mit einer erhöhten Gefahr für die Patientensicherheit verbunden (z.B. durch fehlende Labor- oder Medikamenteninformationen des Patienten). Als zweite Gefahr sehen Sax et al. (2016) die Gefahr des Datenverlustes. Nach einem Systemausfall kann es passieren, dass Daten nicht wiederhergestellt werden können und damit verloren sind. Dies führt im ungünstigsten Fall dazu, dass Medikamente doppelt verabreicht werden oder der Patient durch den Verlust radiologischer Daten einer erneuten Strahlendosis für eine Neuaufnahme ausgesetzt wird. Das dritte Problem für den Anwender und zugleich der am schwersten zu entdeckende Systemfehler, ist der Verlust der Datenintegrität. So kann es beispielsweise zur Fehlzuweisungen bei der Patientenidentifikation kommen, bestimmte Daten können durch eine fehlende Identifikation verloren gehen oder es kann auf Grund von Datenintegritätsmängel zu Fehlentscheidungen kommen (Sax et al., 2016).

Zusammenfassend bleibt zu sagen, dass die Digitalisierung im Gesundheitswesen nicht nur Potenziale mit sich bringen, sondern auch eine Reihe von Herausforderungen. Gerade in Gesundheitseinrichtungen, welche in Deutschland zu den Kritische Infrastruktur gezählt werden, gilt es die Herausforderungen stets im Blick haben zu können und diese auch bewältigen zu können. Dies ist Notwendig, da Gesundheitseinrichtungen als Kritische Infrastruktur einen besonders hohen Schutz benötigen, um weiterhin funktionsfähig bleiben und ihren Dienstleistungsauftrag erfüllen zu können (Cwojdzinski et al., 2012).

2. Zielsetzung und Forschungsfrage

Das Ziel dieser Masterthesis besteht darin, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert erarbeiten und Handlungsempfehlungen daraus ableiten zu können.

Dieses IT-gestützte Dokumentationssystem soll dazu dienen, die Bearbeitung elektronischer Patientenakten im Pflegealltag unter Beachtung gesetzlicher, operativer, wirtschaftlicher Aspekte zu ermöglichen. Die Erwartung an solch ein System besteht darin, sowohl die Verfügbarkeit als auch die Anfälligkeit gegenüber natürlichen und menschlichen Ereignissen zu verbessern.

Um dieses Ziel zu erreichen wurden sechs Forschungsfragen gewählt, die im Rahmen dieser Arbeit beantwortet werden sollen:

Forschungsfrage 1:

Was sind die Vorteile von digitalen Dokumentationssystemen gegenüber papiergestützter Dokumentation im akutstationären Setting?

Forschungsfrage 2:

Welche Patientendaten müssen im Falle eines Ausfalls der IT-Struktur im akutstationären Setting den am Patienten tätigen Personen zur Verfügung stehen, wenn der Zugriff auf die elektronische Patientenakte nicht mehr möglich ist oder Datensätze verloren gegangen sind?

Forschungsfrage 3:

Sind elektronische Patientenakten im Klinikalltag vulnerabler gegen Cyberangriffe als papiergebundene Patientenakten?

Forschungsfrage 4:

Welche Anforderungen muss eine elektronische Patientenakte im akutstationären Setting in Hinblick an die Datenverfügbarkeit, den Datenschutz und die Sicherheit erfüllen?

Forschungsfrage 5:

Welche Rahmenbedingungen müssen erfüllt sein, damit die elektronische Patientenakte im Klinikalltag implementiert werden kann?

Forschungsfrage 6:

Welche Akteure im Krankenhaus müssen bei der Implementierung der elektronischen Patientenakte miteinbezogen werden, um eine gelungene Einführung der elektronischen Patientenakte zu erreichen?

3. Theoretischer Hintergrund

In diesem Kapitel werden nachfolgend die wichtigsten Begrifflichkeiten und Konzepte für dieses Studienvorhaben dargestellt.

3.1. Vulnerabilität

Der Begriff der Vulnerabilität oder auch Verwundbarkeit/Verletzlichkeit ist in der Wissenschaft nicht mehr wegzudenken (Duden, o.J.; Weichselgartner, 2016).

Eine Vielzahl von wissenschaftlichen Disziplinen arbeitet mit Vulnerabilitätskonzepten. Dies bedeutet aber auch, dass der Vulnerabilitätsbegriff nicht universell einsetzbar ist und jede Disziplin eine eigene Auffassung von Vulnerabilität besitzt.

Zwischen den Disziplinen herrscht jedoch ein Konsens bezüglich der Parameter, die die Vulnerabilität beeinflussen. Zum einen ist hier die Empfindlichkeit zu nennen, die den Grad der Einwirkung einer möglichen Störung kennzeichnet. Ein weiterer Parameter stellen die Bewältigungspotenziale dar. Bewältigungspotenziale sind Ressourcen und Fähigkeit, mit deren Hilfe auf Schadenspotenziale eingewirkt werden kann. Die Exposition als dritter Parameter spiegelt den Grad wider, in welchem Ausmaß man der Schädigung ausgesetzt war. Die Vulnerabilität ist hierbei abhängig von einer spezifischen Störung, hat aber keinerlei Abhängigkeit zu einer spezifischen Exposition (Weichselgartner, 2016).

In der englischsprachigen Literatur findet man eine Vielzahl von Vulnerabilitätsbegriffen. So definiert das United Nations Office for Disaster Risk Reduction (UNDRR) Vulnerabilität wie folgt:

> *„The conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards" (United Nations Office for Disaster Risk Reduction [UNDRR], o.J.b, : o.S.).*

Des Weiteren definierte die United Nations International Strategy for Disaster Reduction (UNISDR) in einer Publikation von 2009 den Begriff der Vulnerabilität als:

> *„The characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard" (United Nations International Strategy for Disaster Reduction [UNISDR], 2009, : 30).*

Die Europäische Kommission verwendet in ihrer Publikation 'Risk Assessment and Mapping Guidelines for Disaster Management' neben der Begrifflichkeit der UNISDR eine weitere Definition aus dem Bereich Risikomanagement:

> *„In probabilistic/quantitative risk assessments the term vulnerability expresses the part or percentage of Exposure that is likely to be lost due to a certain hazard" (European Commission [EC], 2010, : 10).*

Für den deutschsprachigen Raum definierte Rudolf-Miklau (2009) den Begriff Vulnerabilität - auch Schadensempfindlichkeit genannt - wie folgt:

> *„Die Schadensempfindlichkeit oder Vulnerabilität ist [...] die Anfälligkeit eines Subjekts/Objekts für Schäden aufgrund seiner Eigenschaften und des einwirkenden Prozesses“ (Rudolf-Miklau, 2009, : 13).*

Auch Suda et al. (2012) prägte den Begriff der Schadensempfindlichkeit:

> *„Die Schadensempfindlichkeit ist der Erwartungswert eines Schadens an einem Objekt als Folge eines bestimmten Ereignisses“ (Suda et al., 2012, : 72).*

3.2. Resilienz

Das Konzept der Resilienz spielt in verschiedenen wissenschaftlichen Disziplinen und Fachbereichen (z.B. Psychologie, Sozioökonomie, Maschinenbau) eine Rolle. Auch im Bereich des Katastrophenrisikomanagements hat dieses Konzept Einzug gehalten (Fekete, Hufschmidt & Kruse, 2014). Allgemein wird unter dem Begriff Resilienz:

> *„[…] die Eigenschaft eines Objekts, eines Akteurs oder einer Gruppe von Akteuren verstanden, welche die Widerstandskraft gegenüber schleichenden, abrupten oder auch radikalen Veränderungen bzw. äußeren, negativen Einwirkungen bestimmt“ (Schneiderbauer, Kruse, Kuhlicke & Abeling, 2016, : 22).*

Dabei beschreibt dieses Konzept, inwieweit durch die negativen Einflüsse, Störungen in der Aufrechterhaltung der Funktionsfähigkeit von Systemen ausgelöst oder verhindert werden können (Schneiderbauer et al., 2016).

Je nach wissenschaftlicher Disziplin stehen verschiedene Subjekte/Objekte im Mittelpunkt. In den psychologischen Disziplinen steht das einzelne Individuum im Vordergrund. Im Zusammenhang mit Resilienz und Gemeinschaften liegt der Fokus auf Gemeinschaften bzw. Gruppen. Im Kontext der Sozioökonomie betrachtet man im Rahmen der Resilienz die wechselseitige Beziehung von Prozessen im Bereich Sozioökonomie und Biophysik. Im Bereich der Resilienz von Kritischen Infrastrukturen stehen Einrichtungen sowie Systemen welche in der Gesellschaft eine Sonderfunktion einnehmen (z.B. Kommunikation, Einrichtungen mit Schutzfunktion und Versorgungsfunktion) (Schneiderbauer et al., 2016).

Im wissenschaftlichen Bereich kann man zwei Strömungsrichtungen des Resilienzkonzepts unterscheiden. Das „konservative technisch-physikalische Verständnis“ (Schneiderbauer et al., 2016, : 22) zielt darauf ab, dass Systeme nach einem negativen Ereignis ihren Ausgangszustand erhalten bzw. diesen wiedererlangen. Holling (1973) definierte im Zusammenhang mit dem Resilienzkonzept nicht nur den Begriff Resilienz an sich, sondern auch den Begriff Stabilität:

> *„Resilience determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist. In this definition resilience is the property of the system and persistence or probability of extinction is the result. Stability, on the other hand, is the ability of a system to return to an equilibrium state after a temporary disturbance. The more rapidly it returns, and with the least fluctuation, the more stable it is. In this definition stability is the property of the system and the degree of fluctuation around specific states the result" (Holling, 1973, : 17).*

Die zweite Strömungsrichtung hat die Wurzeln ihres Verständnisses in der Sozialökonomie. Dieser Ansatz wiederum schreibt Bevölkerungsgruppen oder Systemen die Fähigkeit zu, nach einem negativen Ereignis eine Analyse durchzuführen. Diese Analyse dient dazu, das eigene Reaktionsverhalten auf das Ereignis kritisch zu hinterfragen sowie der Entwicklung von Anpassungsmaßnahmen, um für zukünftige negative Ereignisse besser vorbereitet zu sein (Schneiderbauer et al., 2016).

Grundsätzlich stellt eine Erhöhung der Resilienz gleichzeitig eine Verringerung der Vulnerabilität dar und umgekehrt. Jedoch muss berücksichtigt werden, dass der Begriff Resilienz weiter gefasst ist als der Begriff Vulnerabilität. So beinhaltet der Resilienzbegriff auch die Punkte Lernbereitschaft, Reflektion, Adaption und Reorganisation. Aus diesem Grund sollte der Begriff Resilienz und Vulnerabilität nicht ausschließlich unter denselben Aspekt betrachtet werden, sondern jeder Begriff einzeln betrachtet und dann in Abhängigkeit gesetzt werden (Schneiderbauer et al., 2016).

Wie das Resilienzkonzept in der Praxis aussehen kann zeigt das europäische Forschungsvorhaben 'emBRACE'. Hierbei wird der Begriff gesellschaftliche Resilienz definiert als:

> *„[…] ein Ergebnis von vorhandenen Ressourcen und Kapazitäten (z.B. physische, humane, soziale), von konkreten Handlungen (z.B. ziviler Katastrophenschutz, soziale Dienstleistungen) sowie von Lernprozessen (z.B. durch kritische Reflektion, Experimentieren)" (Schneiderbauer et al., 2016, : 22).*

Diese drei Komponenten sind wiederum eingebettet im Umfeld von Veränderungen sowie Störungen als auch im Umfeld der Disaster Risk Governance (inklusive Gesetze, Verantwortlichkeiten, Politiken). Abbildung 3.1 zeigt die Abhängigkeit der drei Komponenten und die Einbettung dieser in ihre verschiedenen Kontexte.

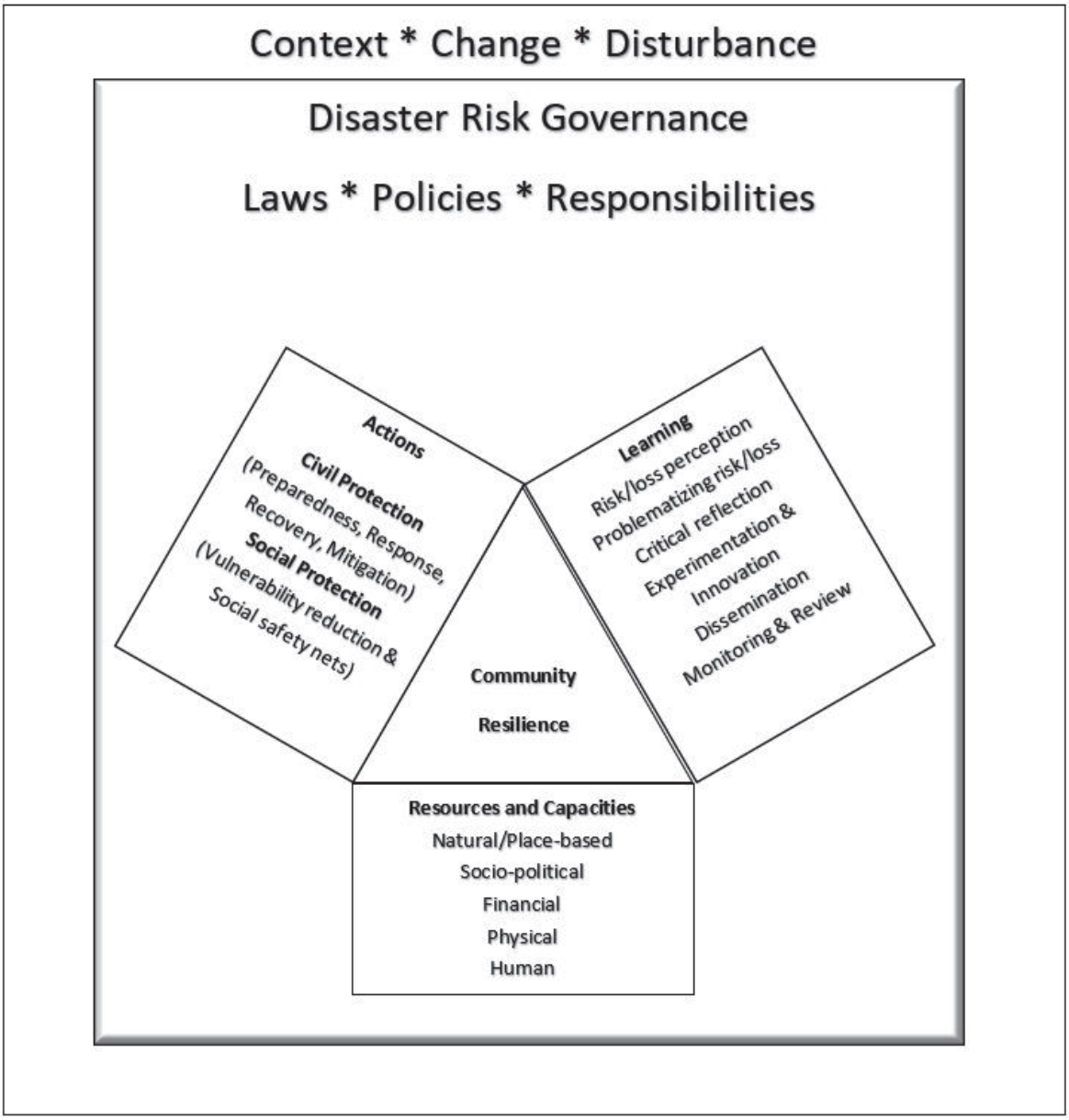


Abbildung 3.1: Resilienz im Kontext des Forschungsvorhabens emBRACE (Angelehnt an: Kruse et al., 2019)

Im Kontext des Katastrophenmanagements definierte das United Nation Office for Disaster Risk Reduction Resilienz als:

> *„The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management" (United Nations Office for Disaster Risk Reduction [UNDRR], o.J.a, : o.S.).*

3.3. Elektronische Patientenakte

Die elektronische Patientenakte spielt im Gesundheitswesen eine wichtige Rolle. Als elektronische Patientenakte im Sinne dieses Forschungsvorhaben, wird die Definition von Dolle et al. (2004) verwendet:

> *„Die elektronische Patientenakte wird [...] als eine IT-gestützte, strukturierte Dokumentation verstanden, in der die zeitlich und räumlich verteilt erhobenen Gesundheitsdaten eines Menschen zusammengefasst werden“ (Dolle et al., 2004, : 9).*

Die elektronische Patientenakte enthält die Gesamtheit aller medizinische, präventiven und administrativen Daten die im Laufe der Behandlung zusammengetragen wurden und den Patienten und den Erbringer der Leistung betreffen. Diese Datensätze werden mit Hilfe eines konsistenten Ortungssystems elektronisch erfasst und gespeichert. Die klinikübergreifenden elektronischen Patientenakte bringt für den Behandlungsalltag einen Vorteil mit sich. So kann die Krankengeschichte des Patienten transparent und problemorientiert allumfassend dargestellt werden. Dies ist Notwendig, um die Versorgungsqualität und damit das Patientenoutcome zu verbessern. Ein weiterer Vorteil durch die Transparenz ist die Verringerung bzw. Vermeidung von Ressourcenverschwendung (z.B. doppelte Untersuchungsleistungen) und die Verhinderung von unnötigen Verzögerungen (Dolle et al., 2004).

3.4. Kritische Infrastruktur

In der Literatur findet man Vielzahl von Definitionen des Begriffes 'Kritischen Infrastruktur'. So definiert Artikel 2 Abschnitt a) der RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern den Begriff der Kritischen Infrastruktur wie folgt:

> *„[…] ‚kritische Infrastruktur‘ die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten“ (EU, 2008, : 77).*

Eine weitere Definition findet sich in der Publikation von Cwojdzinski et al. (2012). In der Veröffentlichung ‚Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus' werden ‚kritische Infrastrukturen‘ beschrieben als:

> *„Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" (Cwojdzinski et al., 2012, : 12).*

Seit 2009 werden die 'Kritischen Infrastrukturen' in neun unterschiedliche Sektoren unterteilt. Diese Sektoren werden wiederum in 29 Branchen kategorisiert. Die Sektoren und Branchen können in Tabelle 3.1 entnommen werden (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [BBK] & Bundesamt für Sicherheit in der Informationstechnik [BSI], 2009):

Tabelle 3.1: Sektoren- und Brancheneinteilung 'Kritischer Infrastrukturen' (Angelehnt an: BBK & BSI, 2009)

Sektoren	Branchen
Energie	Elektrizität, Mineralöl, Gas
Gesundheit	Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
Staat und Verwaltung	Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen inklusive Katastrophenschutz
Ernährung	Ernährungswirtschaft, Lebensmittelhandel
Transport und Verkehr	Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
Finanz- und Versicherungswesen	Banken, Börsen, Versicherungen, Finanzdienstleister
Informationstechnik und Telekommunikation	Telekommunikation, Informationstechnik
Medien und Kultur	Rundfunk, Presse, Kulturgut, symbolträchtige Bauwerke
Wasser	Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung

Ein Blick auf die Sektoren ‚Staat und Verwaltung' und ‚Gesundheit' zeigt, dass Krankenhäuser als Dienstleistungsbetriebe im Bereich Gesundheit sowohl in der täglichen Routinepraxis als auch im Falle von Katastrophen zu den Kritischen Infrastrukturen Deutschlands zählen. Dies bedingt die Notwendigkeit, dass Krankenhäuser geschützt und auf Schadenslagen (z.B. IT-Ausfall) vorbereitet werden müssen. Dies ist das oberste Ziel, damit Krankenhäuser im Realfall funktionstüchtig bleiben können (Cwojdzinski et al., 2012).

3.5. Key-User

Der Begriff Key-User wird in dieser Forschungsvorhaben gleichbedeutend mit dem Begriff Power-User verwendet. Im Kontext der Informationstechnologie wird der Begriff des Power-Users definiert als:

> *„Benutzer mit erweiterten Kenntnissen in bestimmten Anwendungen und verfügen über spezielle Berechtigungen oder Rollen. Sie arbeiten in den Fachabteilungen und stehen den anderen Benutzern als Ansprechpartner zur Verfügung“ (SAP SE, o.J., : o.S.).*

Im Pflegebereich von Krankenhäusern sind Key-User bzw. Power-User Mitarbeitende aus dem Pflegebereich, die eine erweiterte Einweisung auf und eine erweiterte Berechtigung für Softwareprodukte (z.B. elektronische Pflegedokumentationssysteme) haben. Mit ihrem erweiterten Fachwissen, stehen Key-User den Mitarbeitenden auf den Pflegestationen bei Fragen und Problemen mit der Software direkt vor Ort zur Verfügung.

3.6. Cybersicherheit

Die Begriffe Cybersicherheit, Informationssicherheit und IT-Sicherheit werden im Alltag oftmals gleichbedeutend verwendet. Dabei ist der Terminus 'Cybersecurity' derjenige der die Thematik umfassend erfasst (Solms & van Niekerk, 2013).

Die International Telecommunication Union [ITU], the World Bank, Commonwealth Secretariat [ComSec], the Commonwealth Telecommunications Organisation [CTO] und NATO Cooperative Cyber Defence Centre of Excellence [NATO CCD COE] (2018) definierte in den Begriff 'Cybersecurity' wie folgt:

> *„[…] the term 'cybersecurity' is meant to describe the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organisations and citizens; these assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data in the cyber-environment“ (ITU et al., 2018, : 13).*

Alle Begrifflichkeiten haben die Ziele 'Vertraulichkeit', 'Integrität' und 'Verfügbarkeit' gemeinsam und richten ihre Maßnahmen darauf aus. Die drei Ziele sind nach der DIN EN ISO/IEC 27000 wie folgt definiert:

- Vertraulichkeit (eng.: confidentiality):

  „Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird“ (Deutsches Instiut für Normung [DIN], 2020, : 8).

- Integrität (eng.: integrity):

  „Eigenschaft der Richtigkeit und Vollständigkeit“ (DIN, 2020, : 12).

- Verfügbarkeit (eng.: availability):

  „Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat“ (DIN, 2020, : 8).

Bei der Informationssicherheit geht es darum, die Vertraulichkeit, die Integrität sowie die Verfügbarkeit von Informationen zu erhalten (DIN, 2020). Hierbei muss erwähnt werden, dass in diesem Zusammenhang alle Informationen in verschiedenen Formen vorliegen können (z.B. analog auf Papier, digital auf Speichermedium) und sich hier nicht nur um digitale Informationen handelt (Brockhaus, 2019).

Solms und van Niekerk (2013) unterschied die IT-Sicherheit nochmals von der bereits oben erwähnten Informationssicherheit. Nach Solms und van Niekerk (2013) werden im Zusammenhang von IT-Sicherheit die vorliegenden Informationen unter Zuhilfenahme von IT-Technologie sowohl übertragen als auch gespeichert (Solms & van Niekerk, 2013). Hierbei ist zu erwähnen, dass sich die IT-Sicherheit auf die Erhaltung der Vertraulichkeit, der Integrität und der Verfügbarkeit von informationstechnischen Anlagen und deren darin enthaltenen Informationen bezieht (Bundesministerium des Innern [BMI], 2016).

Cybersicherheit geht noch einen Schritt weiter und erweitert die IT-Sicherheit um den virtuellen Raum (Cyberraum) und der daran angeschlossenen IT-Systemen auf der ganzen Welt (BMI, 2016).

4. Aktueller Stand der Forschung

Bursig (2019) stellte in seinem Artikel ‚Cybersicherheit vernetzter Medizinprodukte: Neue Herausforderungen' fest, dass Krankenhäuser zunehmend digitalisiert sind. Damit stellt dies Krankenhäuser vor eine besondere Herausforderung im Bereich der Cybersicherheit. So definiert Bursig (2019) fünf Grundprinzipien, um den Anforderungen an die Cybersicherheit gerecht zu werden:

- Die Cybersicherheit baut auf die integralen Rahmenbedingungen an die Medizintechnik auf
- Während des kompletten Produktlebenszyklus muss die Cybersicherheit gepflegt werden
- Cybersicherheit ist eine systemübergreifende Aufgabe im Krankenhaus
- Informationstransfer und das Vermitteln von Wissen müssen von allen Anwendern unterstütz und gelebt werden
- Risiken die unvermeidbar sind werden zur Kenntnis genommen

Auch für Pohlmann (2019) stellt die Digitalisierung für Krankenhäuser ein großes Problem dar. So beschreibt Pohlmann folgende Cybersicherheitsrisiken die auf die Krankenhäuser im Rahmen der Digitalisierung zukommen können (Pohlmann, 2019):

- Eine hohe Anzahl von Softwareschwachstellen
- Mangelnder Schutz vor Schadprogrammen (z.B. Computerviren/-würmer)
- Fehlende internationale Lösungen im Bereich der Identifikation sowie die Authentifizierung im Internet (z.B. kurze, leichte Passwörter, welche schnell entschlüsselt werden)
- Mangelnde Sicherheit von Internet-of-Things-Geräten (IoT-Geräten) wie beispielsweise Internet-Videokameras

Des Weiteren führt Pohlmann (2019) verschiedene Cybersicherheitsbedürfnisse von Krankenhäusern an. Dazu zählen die Vertraulichkeitsgewährleistung, die Authentifikationsgewährleistung, die Authentizität, die Verbindlichkeits- und Verfügbarkeitsgewährleistung sowie die Anonymisierungsgewährleistung. Zudem stellt Pohlmann die möglichen Cybersicherheitsmechanismen (personelle, organisatorische und technische Maßnahmen) vor. Zum Schluss legt er ein Augenmerk auf die Vorteile für den Einsatz von künstlicher Intelligenz (KI) zur Verbesserung der Cybersicherheit. Durch den Einsatz von KI-Technologie können Angriffe auf Netzwerke und Hardware besser detektiert werden. Ein weiterer Vorteil welche die KI-Technologie mit sich bringt ist die Unterstützung der IT-Experten. Große Datenmengen können mit künstlicher Intelligenz verarbeitet werden und solche Vorfälle rausfiltern, welche von menschlichen Analysten bearbeitet werden müssen.

Lux und Breil (2017) sprechen ebenfalls Gefahren an, die eine Digitalisierung mit sich bringt. Die Autoren geben an,

> *„[…], dass (patientenbezogene oder -beziehbare) Gesundheitsdaten als besondere Art personenbezogener Daten im Sinne des Datenschutzes gelten und daher entsprechend schützenswert sind (§3 Abs. 9 Bundesdatenschutzgesetz)“ (Lux & Breil, 2017, : 691).*

Die Anforderungen an die Datenverarbeitung und den IT-System-Betrieb ist hochkomplex. Die Einhaltung dieser Regelungen kann dazu führen, dass sich die Nutzbarkeit derartiger IT-Systeme äußerst schwierig erweisen. Aber auch diverse andere gesetzliche Regelungen wie das Medizinproduktegesetz können die Entwicklung von Innovationsprodukten in diesem Bereich behindern (Lux & Breil, 2017). Lux und Breil (2017) sind jedoch der Meinung, dass die Erfüllung der datenschutzrechtlichen Rahmenbedingungen aus IT-technischer Sicht durchaus machbar ist (Lux & Breil, 2017).

5. Methodischer Teil

5.1. Design

Für dieses Studienvorhaben wurde als Studiendesign ein qualitativer Forschungsansatz gewählt. Die Wahl für ein qualitatives Design lässt sich damit begründen, dass im Gegensatz zum quantitativen Design, in welchem messbare Daten erhoben und statistisch ausgewertet werden, bei diesem Design subjektive Erfahrungen von Menschen erhoben werden sollen. Das Ziel dieser Arbeit besteht darin, ein Konzept zu entwickeln, welches in die Praxis und auf andere Kontextsituationen übertragbar ist (Brandenburg et al., 2013).

Im Rahmen dessen werden leitfadengestützte Experteninterviews (Lamnek & Krell, 2016) geführt. Unter leitfadengestützten Experteninterviews versteht man:

> *„[…] stärker strukturierte Formen der Befragung mit den Ziel der Gewinnung harter Fakten, die sich aus anderen Quellen nicht oder nur eingeschränkt ermitteln lassen. Mittels des Interviewleitfadens erfolgt die Befragung mit dem klaren Ziel der Abfrage spezifischen Wissens, das zur Beantwortung einer bereits präzisen (und theoretisch eingebetteten) Forschungsfrage notwendig ist“ (Kaiser, 2014, : 35).*

5.2. Literaturrecherche

Am Anfang dieses Forschungsvorhabens wurde eine orientierende Literaturrecherche durchgeführt. Diese dient dazu, relevante wissenschaftliche Literatur zu identifizieren und eine erste Orientierung zu geben.

Nach der orientierenden Literaturrecherche wurde in eine systematische Literaturrecherche übergegangen. Das Ziel der systematischen Literaturrecherche besteht darin, die Punkte Nachvollziehbarkeit und Reproduzierbarkeit transparent darzustellen. Dies erfordert von Seiten des Recherchierenden eine umfangreiche Vorbereitung und Durchführung sowie die lückenlose und nachvollziehbare Dokumentation des gesamten Rechercheprozesses (Simon, 2013).

Bei der orientierenden als auch bei der systematischen Literaturrecherche wurden folgende Datenbanken und Bibliotheken durchsucht:

- u:search der Universität Wien
- Google Scholar
- Google
- Gesetze im Internet
- Bibliothek Klinikum Ingolstadt GmbH

Dazu wurden relevante Schlagwörter verwendet und mit den Booleschen Operatoren AND, OR, NOT kombiniert. Der Zeitraum wurde auf die Jahre 1871 - 2021 eingrenzt. Der Grund für den weit zurückliegenden Suchzeitraum begründet sich in der Suche

nach Gesetzestexten, deren Erscheinen teilweise im Jahr 1871 liegen. Die Literaturrecherche wurde in deutscher sowie englischer Sprache durchgeführt. Zudem wurde auf bereits vorhandene Literatur zurückgegriffen. Die Schlagwörter und Rechercheergebnisse können im Suchprotokoll eingesehen werden.

5.3. Stichprobe und Setting

Als Untersuchungssetting wurde die Klinikum Ingolstadt GmbH festgelegt. Das im Jahre 1982 erbaute Klinikum Ingolstadt ist der zweitgrößte Arbeitgeber in Ingolstadt und eines der größten kommunalen Krankenhäuser in Bayern (Klinikum Ingolstadt GmbH, o.J.b, o.J.c). Das Klinikum entspricht einem Krankenhaus der Versorgungsstufe 2 (Bayerisches Staatsministerium für Gesundheit und Pflege [StMGP], o.J.). Mit über 3700 Mitarbeitern, 1073 stationären Betten und 21 Kliniken und Institute versorgt die Klinikum Ingolstadt GmbH rund 100.000 Patienten jährlich (Klinikum Ingolstadt GmbH, o.J.b).

Um Experten gewinnen zu können, muss zuerst definiert werden was einen Experten ausmacht. Für dieses Forschungsvorhaben wurde die Definition von Meuser und Nagel (1991) verwendet:

> *„Als Experte wird angesprochen, wer in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung oder wer über einen privilegierten Zugang zu Informationen über Personengruppen oder Entscheidungsprozesse verfügt“ (Meuser & Nagel, 1991, : 443).*

Um Experten für dieses Forschungsvorhaben identifizieren zu können, wurden folgende Fragen als Kriterium verwendet (Gläser & Laudel, 2006):

- Welche Experten sind im Besitz von notwendigen Informationen für das vorliegende Forschungsvorhaben?
- Welche Experten können die notwendigen Informationen für die Beantwortung der Forschungsfragen am präzisesten liefern?
- Welche Experten sind im Zeitraum der Datenerhebung für ein Interview verfügbar?
- Welche Experten sind eher bereitwillig die Informationen zu liefern?

Des Weiteren wurden Einschluss- und Ausschlusskriterien für die Interviewteilnahme festgelegt. Damit die Probanden am Interview teilnehmen konnten, musste diese folgende Einschlusskriterien erfüllen:

- Alter ≥18 Jahre
- Deutsches Sprachniveau ≥ B2 nach dem Gemeinsamen europäischen Referenzrahmen für Sprache
- Mitarbeiter deren berufliche Tätigkeit mit dem Umgang von elektronischen Patientenakte zusammenhängt

Folgende Ausschlusskriterien wurden formuliert:

- Alter < 18 Jahre
- Sprachniveau unter dem deutschen Sprachniveau B2 nach dem Gemeinsamen europäischen Referenzrahmen für Sprachen
- Mitarbeiter deren berufliche Tätigkeit nicht mit dem Umgang von elektronischen Patientenakte zusammenhängt

Die Anzahl der durchgeführten Interviews richtet sich nach der Datensättigung (Lettau & Breuer, o.J.). Von einer Datensättigung spricht man:

> *„[…], wenn durch weitere Datenerhebungen keine neuen Informationen mehr gewonnen werden können“ (Mayer, 2018, : 198).*

Anhand der Kriterien sowie der Ein- und Ausschlusskriterien wurden mit Hilfe des Organisationsplanes mögliche Experten identifiziert. Des Weiteren wurden diese Experten gefragt, ob diese noch Experten kennen, welche die Kriterien für diese Forschungsvorhaben erfüllen. Durch dieses Schneeballsystem wurden weitere Experten identifiziert und akquiriert. Insgesamt wurden 17 Experten angesprochen. Von diesen 17 Experten haben 15 an einem Interview teilgenommen. Zwei weitere Experten lehnten die Interviewanfrage ab. Die Experten wurden von mir per E-Mail kontaktiert. Um die datenschutzrechtlichen Anforderungen bezüglich der Kontaktaufnahme einhalten zu können, wurde eine eigene E-Mail-Adresse für dieses Forschungsvorhaben eingerichtet.

5.4. Interviewleitfaden

Für die Erstellung des Interviewleitfadens wurde das SPSS-Prinzip angewendet. SPSS steht hier für Sammeln, Prüfen, Sortieren und Subsumieren. Mit Hilfe dieses Prinzipes kann trotz der zu wahrenden Offenheit, welche bei den Interviews eingehalten werden sollen eine gewisse und auch notwendige Strukturierung vorgegeben werden. Ein weiterer Vorteil besteht in der Vergegenwärtigung und der Auseinandersetzung mit dem eigenen vorhandenen theoretischen Wissens sowie der impliziten Annahmen an die zu entstehenden Gesprächsinhalten (Helfferich, 2011).

Im ersten Schritt 'Sammeln' ('S') werden möglichst viele Fragen zusammengetragen, welche im Kontext des Forschungsgegenstandes steht. In diesem Schritt werden alle Fragen gesammelt, ohne auf die Formulierung oder relevante Frageinhalte zu achten (Helfferich, 2011). Für diese Studie wurden im ersten Schritt insgesamt 45 Fragen generiert, die für den Forschungsgegenstand relevant sein könnten:

- Welche Vorteile haben digitale Dokumentationssysteme im Pflegealltag?
- Welche Nachteile haben digitale Dokumentationssysteme im Pflegealltag?
- Welche Vorteile hat die papiergestützte Dokumentation im Pflegealltag?
- Welche Nachteile hat die papiergestützte Dokumentation im Pflegealltag?

- Auf welche Art und Weise unterstützen digitale Dokumentationssysteme Sie in Ihrer täglichen Arbeit?
- Welche Patientendaten müssen den am Patienten tätigen Personen zur Verfügung stehen, damit sie die Patienten nach dem aktuellen Stand der Wissenschaft pflegen können?
- Welche Patientendaten müssen den am Patienten tätigen Personen mindestens zur Verfügung stehen, damit sie den Patienten im Falle eines fehlenden Datenzugriffs oder bei einem Datenverlust notfallmäßig weiterhin Best möglichst versorgen zu können?
- Wie muss ein Ausfallkonzept gestaltet sein, im Falle das die IT-Infrastruktur nicht verfügbar ist?
- Welche Gründe kann es für einen Ausfall der IT-Struktur geben?
- Welche Gründe gibt es, dass elektronischen Patientenakten anfälliger/vulnerabler gegenüber Cyberangriffen (z.B. Hackerangriffen) sind?
- Welche Auswirkungen können Cyberangriffe auf den Krankenhausbetrieb haben?
- Was versteht man unter dem Begriff Cyberangriff?
- Auf welche Art und Weise können kriminelle Handlungen die elektronische Patientenakte gefährden?
- Welche datenschutzrechtlichen Anforderungen müssen elektronische Patientenaktien erfüllen?
- Wie können datenschutzrechtliche Anforderungen durchgesetzt werden?
- Welche Sicherheitsanforderungen müssen elektronische Patientenakten erfüllen?
- Welche Anforderungen werden an die Datenverfügbarkeit gestellt?
- Welche IT-Struktur muss zur Verfügung stehen um die elektronische Patientenakte Pflegealltag implementieren zu können?
- Wie sieht in Ihren Augen eine erfolgreiche Implementierung elektronischer Patientenakten im Klinikalltag aus?
- Welche gesetzlichen Rahmenbedingungen müssen bei der Implementierung elektronischer Akten berücksichtigt werden?
- Welche elektronischen Endgeräte müssen den am Patienten tätigen Personen zur Verfügung stehen um mit elektronischen Patientenakten arbeiten zu können?
- Welche technischen Anforderungen werden an die elektronischen Patientenakten gestellt?

- Welche Akteure müssen Ihrer Meinung nach bei der Implementierung elektronischer Patientenakten im Krankenhaus miteinbezogen werden?
- Welche finanziellen Rahmenbedingungen müssen berücksichtigt werden?
- Welche weiteren Rahmenbedingungen müssen für bei der Implementierung elektronischer Patientenakten berücksichtigt werden?
- Wieviel Zeit sollte man für eine erfolgreiche Implementierung einer elektronischen Patientenakte einplanen?
- Wie sieht eine erfolgreiche Benutzereinweisung auf die elektronische Patientenakte aus?
- Wie sieht eine erfolgreiche Key-User-Einweisung auf die elektronische Patientenakte aus?
- Wieviel elektronische Endgeräte werden auf den Stationen, welche die elektronische Patientenakte verwenden, benötigt?
- Wie gestaltet sich die Instandhaltung der elektronischen Patientenakte?
- Welche Ausfallkonzepte werden auf den patientenführenden Stationen benötigt, wenn die elektronische Patientenakte während der Wartung nicht verfügbar ist?
- Welche Rolle spielt die Digitalisierung in der Pflege für Sie?
- Wie können kurzzeitige Stromausfälle kompensiert werden, um weiterhin Zugriff auf die elektronischen Patientenakten haben zu können?
- Welche Konzepte gibt es, um auch bei längerfristigen Stromausfällen – Blackouts – Zugriff auf die elektronische Patientenakte haben zu können?
- Welche Ausfallkonzepte gibt es, wenn die Datenintegrität nach einem Hackerangriff nicht mehr gegeben ist, um die Patienten Best möglichst versorgen zu können?
- Welche benutzerspezifischen Anwendungsmöglichkeiten sollte eine elektronische Patientenakte haben?
- Welche Möglichkeiten haben Mitarbeiter, die keinen Zugriff mehr auf Ihre Benutzerdaten haben, um sich in der elektronischen Patientenakte anzumelden?
- Wie gestaltet sich die Betreuung der elektronischen Patientenakten durch die IT, außerhalb der Bürozeiten?
- Welche Berufsgruppen haben Zugriff auf die elektronische Patientenakten?
- Auf welche Daten haben die berechtigten Berufsgruppen Zugriff?
- Auf welche Art und Weise werden Datensätze von elektronische Patientenakten gespeichert?

- Wo sollten Ihrer Meinung nach Datensätze elektronischer Patientenakten gespeichert werden?
- Wie gestaltet sich die Anwendung der elektronischen Patientenakte im Fall einer hausinternen Notlage (z.B. Brand)?
- Im Falle einer Evakuierung des gesamten Gebäudes in eine nahegelegenes Ausweichquartier (z.B. Turnhallen, Pflegeheime, Krankenhäuser). Welche Konzepte gibt es, damit externe Einsatzkräfte/Pflegende Zugriff auf die elektronische Patientenakte haben?
- Welche Kontrollinstanzen werden eingesetzt, um den Zugriff auf elektronische Patientenakten im Rahmen des Datenschutzes zu überwachen?

Im zweiten Schritt 'Prüfen' ('P') werden alle Fragen vom ersten Schritt geprüft. Die Liste wird bearbeitet und die Fragen nach Prüfung deutlich reduziert. Ziel dieses Schrittes sollte es sein nur die für das Forschungsinteresse notwendigen Fragen herauszufiltern. Dies heißt im Umkehrschluss, dass nach der Prüfung ein Großteil der Fragen aus dem weiteren Vorgehen ausgeschlossen werden. Um dieses Ziel erreichen zu können, werden die Fragen mittels Prüffragen durchgesehen (Helfferich, 2011). Nachfolgende Fragen und Stichwörter sind nach der Prüfung noch vorhanden:

- Welche Rolle spielt die Digitalisierung in der Pflege für Sie?
- Welche Vorteile haben digitale Dokumentationssysteme im Pflegealltag?
- Welche Nachteile haben digitale Dokumentationssysteme im Pflegealltag?
- Welche Vorteile hat die papiergestützte Dokumentation im Pflegealltag?
- Welche Nachteile hat die papiergestützte Dokumentation im Pflegealltag?
- Welche Patientendaten müssen den am Patienten tätigen Personen zur Verfügung stehen, damit sie die Patienten nach dem aktuellen Stand der Wissenschaft pflegen können?
    - Im täglichen Pflegealltag?
    - Bei fehlenden Datenzugriff oder Datenverlust?
- Wie muss ein Ausfallkonzept gestaltet sein, im Falle das die IT-Infrastruktur nicht verfügbar ist?
    - Im Falle einer Wartung?
    - Kurzzeitiger Stromausfall?
    - Längerfristige Stromausfälle?
    - Fehlende Datenintegrität?
    - Interne Lagen (z.B. Feuer)?
    - Evakuierung Zugriff auf Patientendaten durch externe Einsatz-/Pflegekräfte?
    - Fehlenden Zugangsdaten?

- Welche Gründe kann es für einen Ausfall der IT-Struktur geben?
- Welche Gründe gibt es, dass elektronischen Patientenakten anfälliger/vulnerabler gegenüber Cyberangriffen (z.B. Hackerangriffen) sind?
    - Auswirkungen von Cyberangriffen auf den Krankenhausbetrieb?
- Welche datenschutzrechtlichen Anforderungen müssen elektronische Patientenaktien erfüllen
    - Durchsetzung?
    - Kontrollinstanzen?
    - Speicherung der Datensätze?
    - Datenzugriff?
- Welche Sicherheitsanforderungen müssen elektronische Patientenakten erfüllen?
- Wie sieht in Ihren Augen eine erfolgreiche Implementierung elektronischer Patientenakten im Klinikalltag aus?
- Welche gesetzlichen Rahmenbedingungen müssen bei der Implementierung elektronischer Akten berücksichtigt werden?
- Welche technischen Anforderungen werden an die elektronischen Patientenakten gestellt?
    - Verfügbarkeit elektronischer Endgeräte zur Verwendung elektronischer Patientenakten?
    - Benötigte IT-Infrastruktur zur Implementierung der elektronischen Patientenakte?
    - Anforderung an die Datenverfügbarkeit?
- Welche Akteure müssen Ihrer Meinung nach bei der Implementierung elektronischer Patientenakten im Krankenhaus miteinbezogen werden?
- Welche Rahmenbedingungen müssen Ihrer Meinung nach bei der Implementierung elektronischer Patientenakten berücksichtigt werden?
    - Finanziell?
    - Technische Anforderungen?
- Wieviel Zeit sollte man für eine erfolgreiche Implementierung einer elektronischen Patientenakte einplanen?
- Wie gestaltet sich Ihrer Meinung nach einer erfolgreichen Einweisung auf die elektronische Patientenakte?
    - Key-User?
    - Benutzer?

- Wie gestaltet sich die Wartung bzw. Instandhaltung der elektronischen Patientenakte?
    - Betreuung der elektronischen Patientenakte außerhalb der Bürozeiten der IT-Abteilung?

Im dritten Schritt 'Sortieren' ('S') werden die noch vorhandenen Fragen und Stichwörter sortiert. Bei dieser Studie wurden die Fragen nach inhaltlichen Aspekten sortiert (Helfferich, 2011). Die Frage 'Welche Rolle spielt die Digitalisierung in der Pflege für Sie?' wurde keinem Themenbereich zugeordnet. Die restlichen Fragen bilden insgesamt fünf verschiedene Themenbereiche:

Vor- und Nachteile elektronischer und papiergestützer Patientenakten

- Welche Vor- und Nachteile haben in Ihren Augen digitale Dokumentationssysteme wie die elektronische Patientenakte im Pflegealltag?
- Welche Vor- und Nachteile haben in Ihren Augen papiergestützte Patientenakten?

Implementierung elektronischer Patientenakten

- Wie sieht in Ihren Augen eine erfolgreiche Implementierung elektronischer Patientenakten im Klinikalltag aus?
- Welche Rahmenbedingungen müssen Ihrer Meinung nach bei der Implementierung elektronischer Patientenakten berücksichtigt werden?
    - Finanziell
    - Technische Anforderungen
    - Gesetzliche Anforderungen
    - Akteure
- Wie gestaltet sich Ihrer Meinung nach einer erfolgreichen Einweisung auf die elektronische Patientenakte?
    - Key-User
    - Benutzer
- Wieviel Zeit sollte man für eine erfolgreiche Implementierung einer elektronischen Patientenakte einplanen?

Anforderung elektronischer Patientenakten im akutstationären Setting bezüglich Datenverfügbarkeit, Datenschutz und Sicherheit

- Welche technischen Anforderungen werden an die elektronischen Patientenakten gestellt in Hinblick auf die Datenverfügbarkeit?
    - Verfügbarkeit elektronischer Endgeräte zur Verwendung elektronischer Patientenakten
    - Benötigte IT-Infrastruktur zur Implementierung der elektronischen Patientenakte

  - Anforderung an die Datenverfügbarkeit
- Welche Patientendaten müssen den am Patienten tätigen Personen zur Verfügung stehen, damit sie die Patienten nach dem aktuellen Stand der Wissenschaft pflegen können?
  - Im täglichen Pflegealltag
  - Bei fehlenden Datenzugriff oder Datenverlust
- Welche datenschutzrechtlichen Anforderungen müssen elektronische Patientenaktien erfüllen?
  - Durchsetzung
  - Kontrollinstanzen
  - Speicherung der Datensätze
  - Datenzugriff
- Welche Sicherheitsanforderungen müssen elektronische Patientenakten erfüllen?
- Wie gestaltet sich die Wartung bzw. Instandhaltung der elektronischen Patientenakte?
  - Betreuung der elektronischen Patientenakte außerhalb der Bürozeiten der IT-Abteilung

Vulnerabilität von elektronischen Patientenakten

- Welche Gründe kann es für einen Ausfall der IT-Struktur geben?
- Welche Gründe gibt es, dass elektronischen Patientenakten anfälliger/vulnerabler gegenüber Cyberangriffen (z.B. Hackerangriffen) sind?
- Auswirkungen von Cyberangriffen auf den Krankenhausbetrieb?

Ausfallkonzept

- Wie muss in Ihren Augen ein Ausfallkonzept gestaltet sein, im Falle das die IT-Infrastruktur nicht verfügbar ist?
  - Im Falle einer Wartung
  - Kurzzeitiger Stromausfall
  - Längerfristige Stromausfälle
  - Fehlende Datenintegrität
  - Interne Lagen (z.B. Feuer)
  - Evakuierung --> Zugriff auf Patientendaten durch externe Einsatz-/Pflegekräfte
  - Fehlenden Zugangsdaten

Im vierten Schritt 'Subsumieren' ('S') werden die vorhandenen Fragen und Stichwörter in die Form eines Leitfadens gebracht. Dazu wird eine Tabelle angelegt. Die erste Spalte erhält die Erzählaufforderung welche dem Befragten gestellt wird. Diese Erzählaufforderung dient dazu den Befragten zu einem Erzählfluss zu bringen. In dem zweiten Spalt befinden sich die Stichwörter, welche entweder bereits bestehen oder aus den Aspekten der bearbeiteten Frageliste generiert werden. Die Stichwörter dienen als Gedächtnisstützte bei Nachfragen und als eine Art Kontrollliste ob bereits alle wichtigen Aspekte abgefragt wurden. Des Weiteren evozieren die Stichwörter einen Erzählimpuls, sollte der Befragte ins Stocken geraten. Wichtig ist hierbei zu erwähnen, dass die Stichwörter erst angesprochen werden, wenn diese nicht zuvor durch den Befragten von allein erwähnt wurden. Die dritte Spalte enthält bereits formulierte Fragen, welche allen Befragten im Interview gestellt werden sollten. Die vierte und letzte Spalte enthält Fragen, welche der Interviewer zur Aufrechterhaltung oder Steuerung des Interviews benötigt. Die Aufrechterhaltungs- und Steuerungsfragen dienen den Interviewer, den Befragten bei zu kurzen Erzählungen zum Weitererzählen zu provozieren und dienen des Weiteren dem Befragten gegenüber Interesse entgegen zu bringe. Wenn die Frage- und Stichwortliste in Leitfadenform gebracht wurde, bleiben möglicherweise einzelne Fragen übrig. Diese einzelnen Fragen sollten am Ende des Leitfadens platziert werden (Helfferich, 2011). Der in Form gebracht und fertige Leitfaden befindet sich in Anhang A.

Der fertige Interviewleitfaden wurde anschließend einem Pretest unterzogen. Der Pretest dient zur Begutachtung des Leitfadens in Hinblick auf (Schnell, 2019):

- Die Interviewdauer
- Den roten Faden innerhalb des Leitfadens
- Die Auswirkungen der Fragenreihenfolge
- Die notwendige Antwortenvielfalt
- Eventuelle Verständnisschwierigkeiten und Belastungen für den Interviewten
- Die Akzeptanz des Interviews

Hierzu wurde der Leitfaden einer Augenscheinvalidität unterzogen. Bei der Augenscheinvalidität, welche zur Inhaltsvalidität gehört, wird das Erhebungsinstrument durch mehrere Personen per Augenschein durchgesehen und anschließend für gut oder schlecht befunden (Brandenburg et al., 2013). Danach wurde für den realitätsnahen Pretest ein Experte ausgewählt, welcher die Kriterien für die Stichprobe erfüllte. Das Interview wurde leitfadengemäß durchgeführt und tontechnisch aufgenommen. Der Pretest ergab folgende Ergebnisse:

- Die Dauer des Testinterviews betrug 22 Minuten und 44 Sekunden.
- Der rote Faden war für den Interviewer und Befragten durchgehend erkennbar.
- Die Reihenfolge der Fragen und Themenblöcke war sinnig und unterstützten den roten Faden durch den Leitfaden hindurch.

- Die Fragen und Fachbegriffe waren klar und verständlich formuliert.
- Es kam zu keiner Belastung des Experten durch das Interview.
- Bei der Befragung konnte festgestellt werden, dass bei der befragten Person durch diese Thematik das Interesse geweckt werden konnte.

5.5. Datenanalyse

Die Experteninterviews wurden tontechnisch aufgezeichnet und anschließend transkribiert. Die Auswertung der Transkripte erfolgt mit Hilfe der qualitativen Inhaltsanalyse nach (Mayring, 2002).

Das oberste Ziel der Inhaltsanalyse besteht darin, Material zu analysieren, das aus einer Form der Kommunikation stammt. Eine einheitliche Definition ist in der Literatur nicht zu finden. Jedoch nannte Mayring (2015) einige Charakteristika wodurch sich die Inhaltsanalyse, wie sie in der Sozialwissenschaft zu finden ist, auszeichnet. Die Technik der qualitativen Inhaltsanalyse zeichnet sich aus durch (Mayring, 2015):

- die Auswertung (fixierter) Kommunikation
- Systematik
- Regelgeleitetheit
- Theoriegeleitetheit
- und will dabei Schlussfolgerungen über eindeutige Kommunikationsaspekte ziehen

Mayring (2015) entwickelte ein Ablaufmodell, wie eine qualitative Inhaltsanalyse ablaufen soll (siehe Abbildung 5.1):

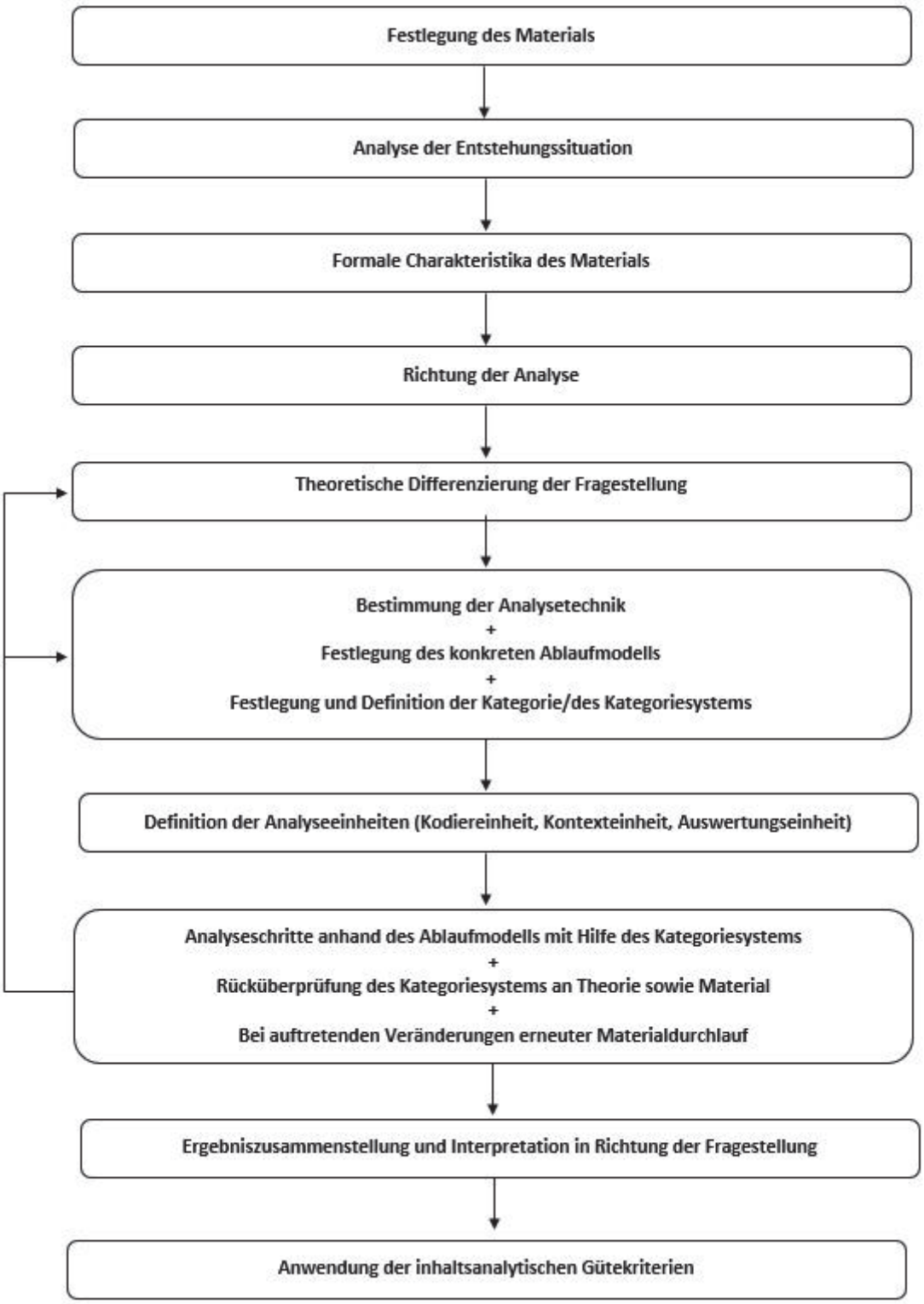


Abbildung 5.1: Inhaltsanalytisches Ablaufmodell allgemein (Angelehnt an: Mayring, 2015, : 62)

Im Verlauf dieser Arbeit wird das Ablaufmodell der inhaltlich strukturierenden und der zusammenfassenden Inhaltsanalyse mit in das allgemeine Ablaufmodell der Inhaltsanalyse integriert.

Bestimmung des Ausgangsmaterials

i) Festlegung des Materials

Im ersten Schritt muss festgelegt werden, welches Material in der qualitativen Inhaltsanalyse bearbeitet werden soll. Aus diesem Grund sollte die Grundgesamtheit definiert werden über welche einer Aussage gemacht werden soll. Zudem sollte der Umfang der gewählten Stichprobe sowie die Art und Weise der Stichprobenziehung definiert werden (Mayring, 2015).

Es wurden 15 Experteninterviews für diese Arbeit geführt. Die Interviews wurden als Einzelinterviews geführt.

In die Analyse werden alle 15 Experteninterviews miteinbezogen, um eine Datensättigung (Mayer, 2018) zu erreichen.

ii) Analyse der Entstehungssituation

In der Analyse der Entstehungssituation sollte genau dargestellt werden, von welcher Person und unter welchen Umständen die Daten erhoben wurden. Hierbei sollten vor allem Informationen dargestellt werden zu den Fragen (Mayring, 2015)_

- Wer ist der Autor und wer sind die Studienteilnehmer?
- Welchen emotional-kognitive Hintergrund und welchen Handlungshintergrund hat Autor?
- Für welchen Adressatenkreis wurde die Daten erhoben?
- Wie war die genaue Situation, in welcher die Daten erhoben wurden?
- Wie ist der soziale und kulturelle Hintergrund?

Die leitfadengestützten Experteninterviews wurde von Herrn Florian Kunze, B.Sc. im Rahmen seiner Masterarbeit im Studiengang ‚Risikoprävention und Katastrophenmanagement' an der Universität Wien geführt. Die Studienteilnehmer wurden aus der Klinikum Ingolstadt GmbH rekrutiert. Die 15 Studienteilnehmer wurden auf Grund ihres beruflichen Hintergrundes aus den Fachdisziplinen ‚Verwaltung', ‚Informationstechnologie', ‚Pflege' und ‚Medizin' des Klinikum Ingolstadts ausgewählt. Alle Studienteilnehmer nahmen freiwillig an den Interviews teil. Die Experten wurden per E-Mail von mir kontaktiert. Den Interviewteilnehmern wurde ein Informationsschreiben, eine Datenschutzerklärung und eine Einverständniserklärung übergeben. Alle drei Dokumente wurden in Papierform übergeben. Ursprünglich waren die Expertengespräche vor Ort und als Face-to-Face Interview geplant. Auf Grund der Pandemielage durch den Virus SARS-CoV-2 und der Verfügbarkeit der Experten wurden acht Interviews (n=8) mit Hilfe von Videokonferenztools (Zoom und MS Teams) durchgeführt. Des Weiteren wurden fünf Interviews (n=5) telefonisch durchgeführt. Lediglich zwei Interviews (n=2) wurde als Face-to-face Interview in der Wohnung der

Befragten durchgeführt. Die Studienteilnehmer wurden gebeten sich eine Stunde für das Interview freizuhalten. Jeder der Interviewteilnehmer nahm sich genügend Zeit für das Interview, sodass die Interviews in einer stressfreien und ruhigen Situation durchgeführt werden konnten.

iii) Formale Charakteristika des Materials

Im dritten Schritt soll nach Mayring (2015) dargestellt werden, in welcher Form die Daten vorliegen, da für die Inhaltsanalyse in den meisten Fällen eine Verschriftlichung vorliegen muss. Dabei spielt es keine Rolle ob dieser Text von Verfasser selbst oder von einer dritten Person stammt. Oftmals werden vor allem bei Interviews diese zuerst tontechnisch aufgenommen. Die tontechnische Aufnahme muss für die Inhaltsanalyse verschriftlicht werden. Dieser Vorgang wird als Transkription bezeichnet, welcher bestimmten Regeln folgt (Mayring, 2015).

In dieser Arbeit wurden die Interviews mit Hilfe von tontechnischem Equipment aufgenommen. Diese Tonaufnahmen wurden anschließend transkribiert. Damit die Transkription regelgeleitet erfolgt, wurden die Transkriptionsregeln an Dresing und Pehl (2011; Dresing & Pehl) angelehnt und adaptiert:

- Die Transkription erfolgt wörtlich
- Dialekte werden nicht transkribiert, sondern Wortgenau in die hochdeutsche Sprache übersetzt. Wenn keine konkrete Übersetzung möglich ist, so ist der Dialekt zu transkribieren
- Verschleifungen von Worten werden nicht verschriftlicht. Die Verschleifung wird so transkribiert, dass es dem Schriftdeutsch entspricht. Die Form des Satzes wird trotz Fehlern beibehalten
- Für bessere Lesbarkeit wird die Interpunktion geglättet
- Stottern wird nicht transkribiert, sondern geglättet oder auch ausgelassen
- Wörter die abgebrochen worden sind werden ignoriert
- Doppelte Wörter werden nur transkribiert, wenn diese als Stilmittel benutzt werden
- Halb angefangene Sätze ohne Endung werden mit '/' gekennzeichnet
- Rezeptionssignale werden nicht transkribiert, sofern sie den Sprachfluss des gegenüber nicht unterbrechen.
- Rezeptionssignale werden transkribiert, wenn Sie als Antwort auf eine direkte Frage gegeben wird
- Pausen ab ca. 3 Sekunden werden durch '(...)' gekennzeichnet
- Äußerungen wie beispielsweise äh, ehm, mhm werden nicht transkribiert
- Wörter welche besonders betont wurden werden durch durchgehend mit Großbuchstaben geschrieben (z.B. HEUTE)

- Jeder Wechsel des Sprechers erhält einen gesonderten Absatz
- Eine leere und freie Zeile zwischen jeden Sprecher
- Kurze Einwürfe eines Sprechers bekommen einen separaten Absatz
- Nach jedem Sprecherwechsel bzw. am Absatzende werden Zeitmarken gesetzt
- Der Interviewer wird mit einem 'I:' und der Befragte mit einem 'B:' gekennzeichnet
- Zeichen sowie verwendete Abkürzungen werden ausgeschrieben
- Begrifflichkeiten in englischer Sprache werden nach deutscher Rechtschreibregeln behandelt
- Anredepronomen der Höflichkeit werden großgeschrieben, alle anderen kleingeschrieben
- Zahlen bis zwölf werden als Namen geschrieben, höhere mit Ziffern
- Zahlen mit kurzen Namen werden ausgeschrieben
- Ungefähre Zahlenangaben wird der Zahlennamen, bei genau gemeinten Zahlen die Ziffernform verwendet
- Feste Konventionen wie beispielsweise Hausnummern, Seitenzahlen, Telefonnummern und Datum werden auf keinen Fall ausgeschrieben
- Redewendungen sowie Idiome werden wörtlich in die deutsche Sprache übernommen
- Wörtlich zitierte Rede wird in Anführungszeichen gesetzt
- Einzelne Buchstaben und Aufzählungen werden mit Großbuchstaben geschrieben ohne Klammer

Des Weiteren wurden an den linken Rand der Transkription fortlaufende Zeilennummerierungen sowie rechts unten fortlaufende Seitennummern verwendet, um eine leichtere Orientierung zu erzielen.

Fragestellung der Analyse

iv) Richtung der Analyse

Auf Grundlage der gewonnenen Daten lassen sich verschiedene Aussagen (z.B. über den Gegenstand) in unterschiedliche Richtungen machen. Die Richtung der Analyse muss vor dem Beginn festgelegt werden. Dabei kann es von Vorteil sein, die gewonnenen Daten (z.B. Text) als Bestandteil der Kommunikationskette zu sehen. Das Ziel besteht darin, die Daten (z.B. Text) in ein inhaltsanalytisches Kommunikationsmodell einzuordnen. Das inhaltsanalytische Kommunikationsmodell nach Mayring ist Abbildung 5.2 zu entnehmen.

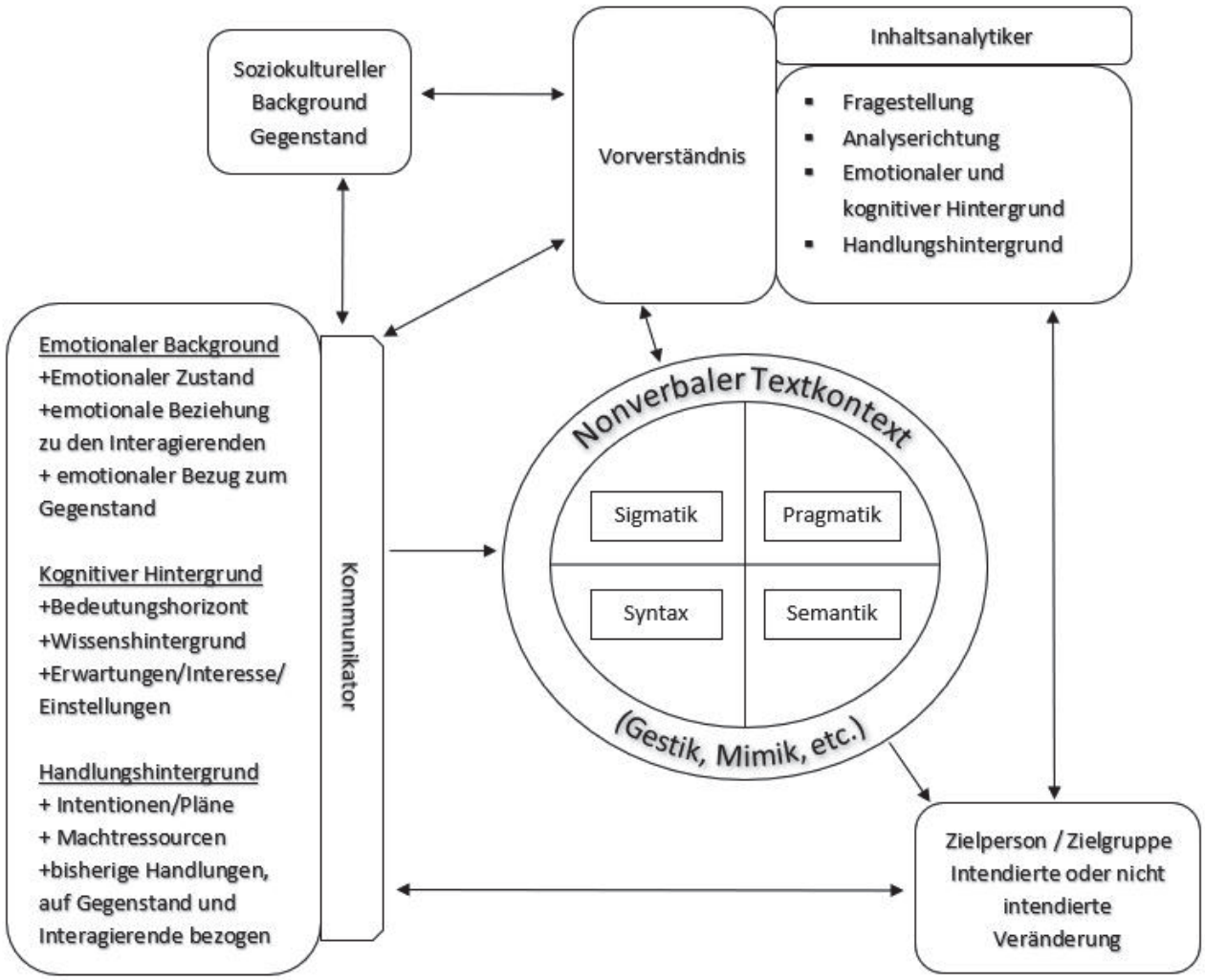


Abbildung 5.2: Inhaltsanalytisches Kommunikationsmodell nach Mayring (Angelehnt an: Mayring, 2015, : 59)

Der Fokus der Analyse liegt auf dem Gegenstand. Dies diente dazu, dass die Befragten mit ihrem Expertenwissen Auskunft zu den folgenden Themen gaben:

- Digitalisierung
- Vor- und Nachteile von elektronischen und papiergestützten Akten
- Implementierung elektronische Patientenakten im Krankenhaus
- Anforderungen an die elektronische Patientenakte, insbesondere Datenverfügbarkeit, Datenschutz und Sicherheit
- Vulnerabilität/Anfälligkeiten von elektronischen Patientenakten
- Ausfallkonzepte

Die Analyse dient der Datengrundlage für die Erarbeitung eines Konzeptes mit dem Schwerpunkt Digitalisierung in der Pflege

v) Theoriegeleitete Differenzierung der Fragestellung

Die qualitative Inhaltsanalyse zeichnet sich unter anderem dadurch aus, dass diese zum einem einer gewissen Regelgeleitetheit unterliegt und zum anderen die

Interpretation theoriegeleitet stattfindet. Der Schritt der Analyse liegt einer eindeutigen theoriegeleiteten Fragestellung zugrunde. Ziel der Theoriegeleitetheit ist es, die Sichtweise nicht einzuengen, sondern die aus der Studie gewonnenen Erkenntnisse anderer Personen ermöglichen. Dies wiederum führt zu einem Erkenntnisfortschritt (Mayring, 2015).

Die Interviews enthalten Aussagen von 15 Experten aus dem Bereich 'Verwaltung', 'Informationstechnologie', 'Pflege'' und 'Medizin' des Klinikum Ingolstadts zum Thema 'Digitalisierung' und 'elektronische Patientenakte'. Alle Experten beschäftigen sich in ihrer tagtäglichen Arbeit mit dieser Thematik.

Die bisherige Literatur spricht davon, dass die Digitalisierung im Krankenhaus bisher noch nicht weit fortgeschritten ist und sich noch auf einem niedrigen Level befindet (BMWi, 2017; Dörries et al., 2017).

Die Digitalisierung bringt nicht nur eine Vielzahl von Potenzialen (z.B. Transparenz, besseres Patientenoutcome) mit sich (BMWi, 2017; Dörries et al., 2017). So kommt es im Rahmen der Digitalisierung auch zu vielen Herausforderungen (z.B. Hackerangriffe, gesetzliche Vorschriften) die bewältigt werden müssen (Kucera, 2020).

In dieser Hinsicht ist es für diese Arbeit interessant, wie Experten auf dem Gebiet der Digitalisierung diese Herausforderungen in der Digitalisierung der Pflege einschätzen und welche Möglichkeiten oder Lösungen sie sehen, um den Herausforderungen gewachsen zu sein. Aus diesem Grund ergeben sich folgende Fragestellungen für die Analyse:

- Was sind die Vorteile von digitalen Dokumentationssystemen gegenüber papiergestützter Dokumentation im akutstationären Setting?
- Welche Patientendaten müssen im Falle eines Ausfalls der IT-Struktur im akutstationären Setting den am Patienten tätigen Personen zur Verfügung stehen, wenn der Zugriff auf die elektronische Patientenakte nicht mehr möglich ist oder Datensätze verloren gegangen sind?
- Sind elektronische Patientenakten im Klinikalltag vulnerabler gegen Cyberangriffe als papiergebundene Patientenakten?
- Welche Anforderungen muss eine elektronische Patientenakte im akutstationären Setting in Hinblick an die Datenverfügbarkeit, den Datenschutz und die Sicherheit erfüllen?
- Welche Rahmenbedingungen müssen erfüllt sein, damit die elektronische Patientenakte im Klinikalltag implementiert werden kann?
- Welche Akteure im Krankenhaus müssen bei der Implementierung der elektronischen Patientenakte miteinbezogen werden, um eine gelungene Einführung der elektronischen Patientenakte zu erreichen?

Ablaufmodell der Analyse

vi) Bestimmung der Analysetechnik

Nach Mayring (2015) kann für die qualitative Inhaltsanalyse auf drei Grundformen zurückgegriffen werden:

- Zusammenfassung
- Explikation
- Strukturierung

Das Ziel der zusammenfassenden qualitativen Inhaltsanalyse besteht darin, das vorhandene Datenmaterial auf die bedeutenden Inhalte hin zu reduzieren und durch Generalisierung ein übersichtliches Gesamtbild zu erschaffen. Wichtig dabei ist zu erwähnen, dass diese Abstraktion immer noch die Grundaussage des ursprünglichen Materials ist (Mayring, 2015).

Das Ziel der explizierenden qualitativen Inhaltsanalyse ist es, durch heranziehen von zusätzlichem Datenmaterial unklare Textstellen genauer zu verstehen und zu erläutert (Mayring, 2015).

Das Ziel der strukturierenden qualitativen Inhaltsanalyse besteht entweder darin, bestimmte Betrachtungsweisen herauszufinden, das vorliegende Material mit Hilfe eines Kategoriensystems einzuordnen oder einen Querschnitt durch im Vorhinein bestimmten Ordnungskriterien durch das vorhandene Datenmaterial zu legen (Mayring, 2015).

Mayring (2015) schlägt diese drei Grundformen vor, lässt jedoch den Spielraum offen diese drei Grundformen miteinander zu kombinieren.

Die explizierende qualitative Inhaltsanalyse eignet sich für diese Studie nicht, da bei der Explikation zusätzliches Datenmaterial zum Verständnis an das erhobene Datenmaterial herangetragen werden muss. Da bei der vorliegenden Thematik wenig vorhandenes Material zur Verfügung steht und das Ziel dieser Masterarbeit darin besteht, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert zu erarbeiten und Handlungsempfehlungen daraus ableiten zu können wird für diese Arbeit eine Mischform (strukturierend-zusammenfassende qualitative Inhaltsanalyse) gewählt. Die Wahl für die Strukturierung lässt sich damit begründen, dass durch den vorliegenden Interviewleitfaden bereits Kategorien gebildet wurden. Diese Kategorien können verwendet werden, um die vorliegenden Transkripte mit Hilfe des Kodierleitfaden bearbeiten zu könne (deduktive Kategorieanwendung). Alle relevanten Textstellen die in der Deduktion dem bestehendem Kategoriesystem nicht zugeordnet werden konnten, werden in einem zweiten Schritt einer zusammenfassenden Analyse unterzogen. Dabei werden die noch vorhandenen Textstellen mithilfe der induktiv gebildeten Kategorien zugeordnet (induktive Kategorieanwendung).

vii) Festlegung des konkreten Ablaufmodells

Im ersten Schritt wird das vorhandene Datenmaterial mit Hilfe der strukturierenden qualitativen Inhaltsanalyse bearbeitet. Für diese Arbeit wurde eine inhaltliche Strukturierung verwendet. Bei dieser Art der Strukturierung wird Textmaterial zu bestimmten Thematiken extrahieren und zusammengefasst. Welche Inhalte

letztendlich isoliert werden, wird durch die im Vorhinein entwickelten Kategorien bestimmt. Sobald das Kategoriesystem auf das Textmaterial angewendet wird, werden die daraus entstandenen Paraphrasen zunächst den Unterkategorien und anschließend den Hauptkategorien zugewiesen (Mayring, 2015). Das Ablaufmodell der inhaltlichen Strukturierung ist Abbildung 5.3 zu entnehmen.

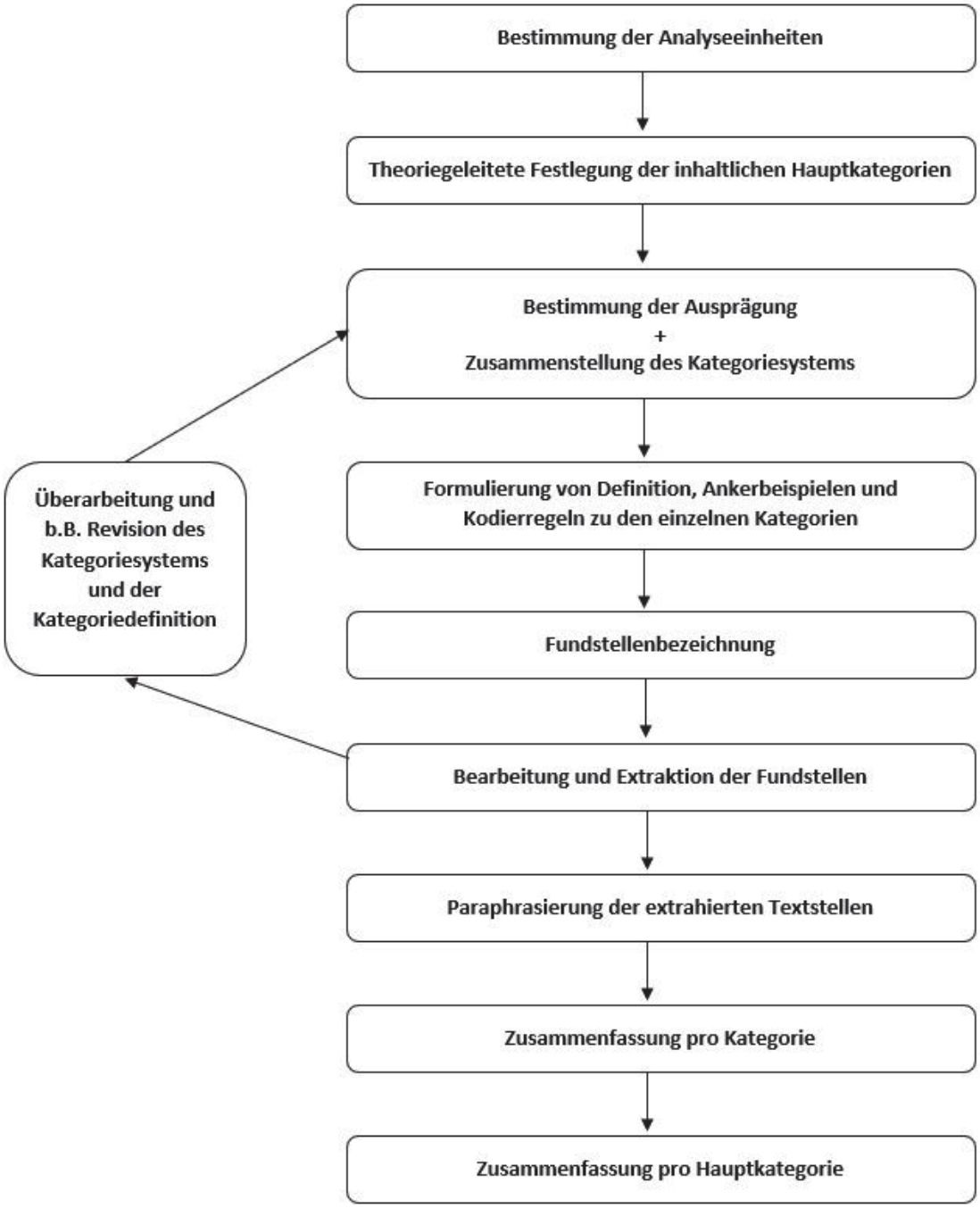


Abbildung 5.3: Ablaufmodell der inhaltlichen Strukturierung (Angelehnt an: Mayring, 2015, : 104)

Alle inhaltstragenden Textstellen, die bei der deduktiven Analyse nicht einer Kategorie zugeordnet werden konnten, wurden in einem zweiten Schritt induktiv mit Hilfe der zusammenfassenden Inhaltsanalyse bearbeitet. Das Ziel der zusammenfassenden Inhaltsanalyse besteht darin, dass alle Abstraktionsebenen der zusammengefassten Texteinheiten exakt definiert sind. Diese wiederum werden mit Hilfe von Makrooperatoren auf das Material moduliert. Die Abstraktionssebene kann Stück für

Stück weiter generalisiert werden, wobei im Zuge dieser Verallgemeinerung die Zusammenfassungen immer abstrakter werden (Mayring, 2015). Das Ablaufmodell der zusammenfassenden Inhaltsanalyse ist Abbildung 5.4 zu entnehmen.

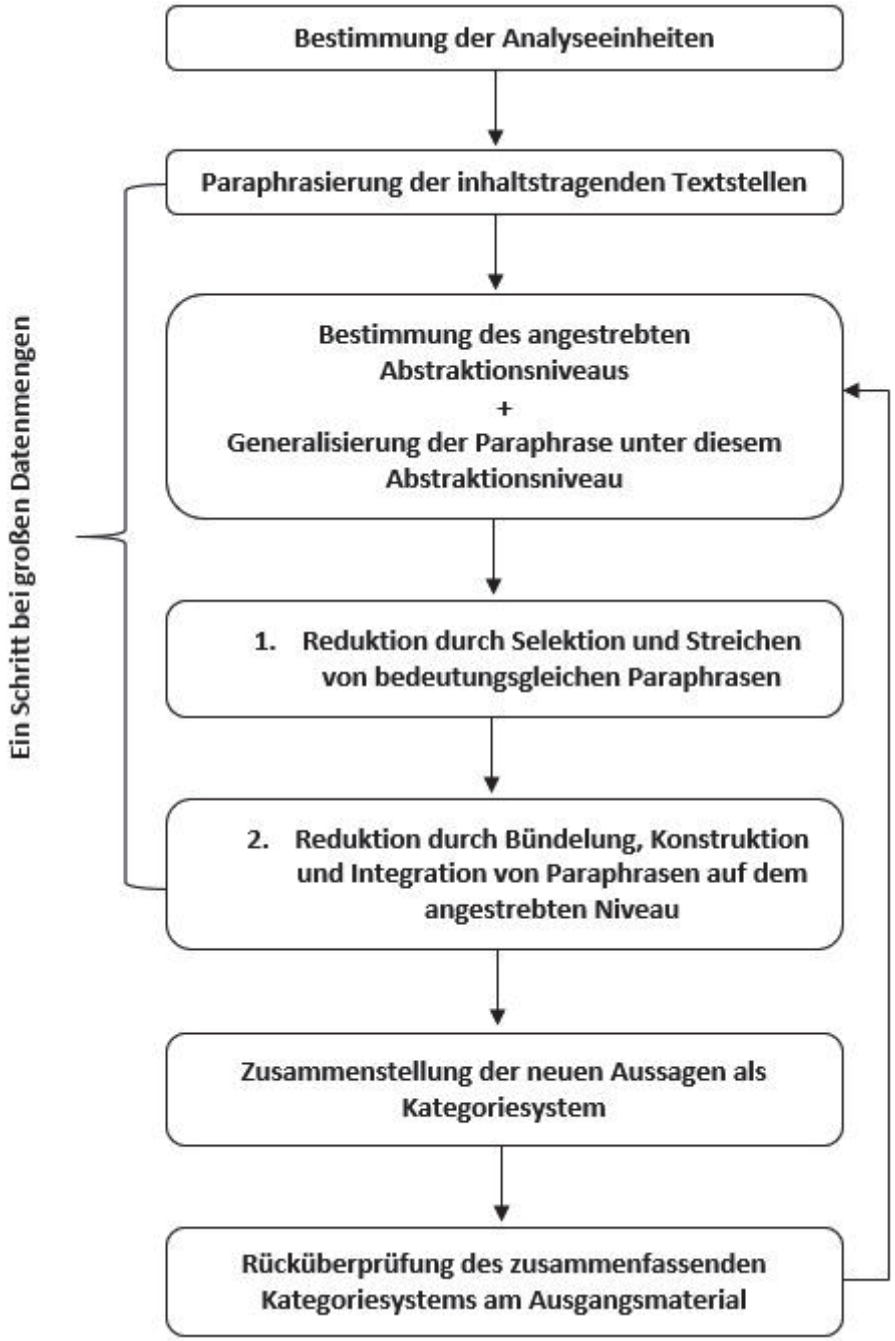


Abbildung 5.4: Ablaufmodell der zusammenfassenden Inhaltsanalyse (Angelehnt an: Mayring, 2015, : 104)

viii) Festlegung und Definition der Kodier-, Kontext- und Auswertungseinheit

Um die Genauigkeit der qualitativen Inhaltsanalyse zu erhöhen werden Analyseeinheiten gebildet (Mayring, 2015).

Die Kodiereinheit definiert den kleinsten Bestandteil eines Datenmaterials, welcher in die Auswertung miteinbezogen werden darf. Dies bedeutet, dass die Kodiereinheit definiert, welcher der kleinste Teil eines Textes ist, der einer Kategorie zugeordnet werden kann. Im Falle dieser Arbeit entspricht die Kodiereinheit einem Einzelwort. Dies

ist von Vorteil, wenn ein Experte in einer Aufzählung verschiedene Themenbereiche anspricht und diese wiederum verschiedenen Kategorien zugeordnet werden können. So können Einzelwörter mit verschiedenen Thematiken verschiedenen Kategorien zugeordnet werden (Mayring, 2015).

Die Kontexteinheit definiert den größten Bestandteil eines Datenmaterials, welcher einer Kategorie zugeordnet werden kann. In dieser Arbeit entspricht eine Kontexteinheit die vollständige Antwort des Befragten auf eine Frage. Durch die Verwendung der gesamten Antwort des Befragten können mehr Informationen zur Beantwortung der Frage herangezogen werden (Mayring, 2015).

Die Auswertungseinheit gibt an, welche Textabschnitte hintereinander analysiert werden. Für diese Arbeit entspricht eine Auswertungseinheit ein gesamtes Interviewtranskript. Für diese Arbeit liegen 15 Auswertungseinheiten vor, da mit 15 Experten ein Interview geführt wurde (Mayring, 2015).

ix) Analyseschritt: Inhaltlich strukturierende Inhaltsanalyse

Bestimmung der Analyseeinheiten

Für die inhaltlich strukturierende Inhaltsanalyse werden insgesamt 15 Auswertungseinheiten zur Bearbeitung herangezogen. Dabei handelt es sich um 15 leitfadengestützte Experteninterviews die dem Autor in transkribierter Form vorliegen.

Die Kontexteinheit repräsentiert eine vollständige Antwort des Interviewten auf eine Frage.

Als Kodiereinheit wird ein einzelnes kommuniziertes Wort festgelegt.

Entwicklung des Kategoriesystems und des Kodierleitfadens

Im ersten Schritt wurden die Oberkategorien gebildet. Diese Oberkategorien ergaben sich aus dem Hauptthemenbereiche, welche im erarbeiteten Interviewleitfaden wiederzufinden sind. Dabei wurden folgende Oberkategorien (OK) gebildet:

- OK 1: Rolle und Notwendigkeit der Digitalisierung in der Pflege
- OK 2: Abwägungen zur elektronischen Patientenakte
- OK 3: Vorteile und Nachteile der elektronischen Patientenakte
- OK 4: Implementierung elektronische Patientenakte im Krankenhaus
- OK 5: Anforderungen an die elektronische Patientenakte
- OK 6: Vulnerabilität von elektronischen Patientenakten
- OK 7: Ausfallkonzepte

Im zweiten Schritt wurde zu einem Teil der Oberkategorien Ausprägungen bestimmt. Auch diese Ausprägungen in Form von Unterkategorien wurden mit Hilfe der Themenbereiche im Leitfaden gebildet. Folgende Unterkategorien (UK) wurden gebildet:

- UK 2.1: Vorteile der papiergebundenen Patientenakte
- UK 2.2: Nachteile der papiergebundenen Patientenakte
- UK 3.1: Vorteile der elektronischen Patientenakte
- UK 3.2: Nachteile der elektronischen Patientenakte
- UK 4.1: Finanzielle Rahmenbedingungen
- UK 4.2: Technische Rahmenbedingungen
- UK 4.3: Gesetzliche Rahmenbedingungen
- UK 4.4: Beteiligte Akteure
- UK 4.5: Benutzereinweisung/Key-User
- UK 4.6: Dauer der Implementierung
- UK 5.1: Datenverfügbarkeit
- UK 5.2: Datenschutz
- UK 5.3: Sicherheit
- UK 6.1: Vulnerabilität gegenüber Cyberangriffen
- UK 6.2: Weitere Grunde für den Ausfall der IT-Struktur
- UK 6.3: Auswirkungen bei Ausfall der IT-Struktur
- UK 7.1: Allgemeines Ausfallkonzept
- UK 7.2: Ausfallkonzept im Falle einer Evakuierung

Im dritten Schritt wurde für jede einzelne Kategorie eine Definition formuliert, ein Ankerbeispiel aus den vorliegenden 15 Analyseeinheiten gesucht und bei Bedarf Kodierregeln aufgestellt, wenn Kategorien nicht trennscharf voneinander unterschieden werden konnten. Das fertige Kategoriesystem und der Kodierleitfaden für diese Analyse befindet sich in Anhang D.

Anwendung der Kategoriesystems und des Kodierleitfadens am Material

Das vorliegende Datenmaterial (n=15 Auswertungseinheiten) wurde unter Zuhilfenahme der QDA-Software "MAXQDA" inhaltsanalytisch aufbereitet. Hierbei wurden inhaltsrelevante Stellen identifiziert und gekennzeichnet. Anschließend wurden die identifizierten Fundstellen isoliert und in einem weiteren Schritt einer Paraphrasierung unterzogen. Die Paraphrase wurde den im Kategoriesystem hinterlegten Kategorien (Unterkategorien und Hauptkategorien) zugeordnet. Im Zuge dieser einzelnen Schritte wurde das bestehende Kategoriesystem und deren Kategoriedefinitionen immer wieder überprüft und gegebenenfalls angepasst. Für die inhaltlich strukturierende Inhaltsanalyse wurde zur besseren Übersicht eine vierspaltige Tabelle (siehe Tabelle 5.1) generiert. Die Darstellung der Ergebnisse dieses Schrittes erfolgt sortiert nach den Kategorien.

Tabelle 5.1: Tabelle deduktive Kategorienanwendung

Dokumente	Originalzitate	Paraphrasen	Bemerkungen
…	…	…	…

x) Analyseschritt: Zusammenfassende Inhaltsanalyse

Bestimmung der Analyseeinheiten

Für die inhaltlich strukturierende Inhaltsanalyse werden insgesamt 15 Auswertungseinheiten zur Bearbeitung herangezogen. Dabei handelt es sich um 15 leitfadengestützte Experteninterviews die dem Autor in transkribierter Form vorliegen

Die Kontexteinheit repräsentiert eine vollständige Antwort des Interviewten auf eine Frage.

Als Kodiereinheit wird ein einzelnes kommuniziertes Wort festgelegt.

Induktive Kategorienbildung

Um die induktive Kategorienbildung durchführen zu können wurde im ersten Schritt eine vierspaltige Tabelle (siehe Tabelle 5.2) generiert.

Tabelle 5.2: Tabelle induktiver Kategorienbildung

Dokumente	**Originalzitate**	**Paraphrasen**	**Generalisierungen**	**Induktive Kategorien**
…	…	…	…	…

Im ersten Schritt wurden die relevanten Textstellen identifiziert und diese anschließend paraphrasiert.

Im nächsten Schritt wurde das Abstraktionsniveau bestimmt und die bestehende Paraphrase nach dem festgelegten Grad der Verallgemeinerung generalisiert. Anschließend wurde eine erste und zweite Reduktion. Im Zuge dessen wurden Paraphrasen gleicher Bedeutung gestrichen und Paraphrasen gebündelt auf dem vorher festgelegten Niveau. Im Anschluss wurden die neu generierten Aussagen in einem Kategoriesystem zusammengestellt. Im Zuge der Analyse fand eine kontinuierliche Rücküberprüfung des neu generierten Kategoriensystems am vorliegenden Material statt.

5.6. Ethik und Datenschutz

An dieses Forschungsvorhaben wurden ethische und datenschutzrechtliche Anforderungen gestellt. So wurden die forschungsethischen Prinzipien nach Schnell und Dunger (2018) für diese Arbeit beachtet:

- Beachtung der Forschergemeinschaft
- Aufklärung über Ziel und Umstände
- Aufklärung über die Methode
- Abschätzung der Folgen
- Ethische Prognose
- Ethische Prävention
- Pflicht zur Wahrheit
- Beachtung der Datenschutzgesetze

Die Prinzipien 1, 2, 3 und 7 wurden dahingehend berücksichtigt, dass alle Interviewten für die Interviews eine informierte Zustimmung (informed consent) gaben. Die informierte Zustimmung bildet den zentralen Aspekt forschungsethischen Verhaltens. Schnell und Heinritz (2006) definierte die informierte Zustimmung als

> *„[…] die bewusste Zustimmung einer Person oder ihres bevollmächtigten Vertreters als Proband an einem Forschungsprojekt teilzunehmen“ (Schnell & Heinritz, 2006, : 20).*

Allerdings unterliegt die Zustimmung bestimmten Kriterien, damit diese ihre Gültigkeit besitzt (Schnell & Heinritz, 2006):

- Der Studienteilnehmer muss umfassend über die Studie informiert werden
- Der Studienteilnehmer hat genügend Zeit und Möglichkeiten zur Beratung um sich eine Meinung über das Projekt bilden zu können
- Die informierte Zustimmung von Eltern bzw. gesetzlichen Vertreter bei unmündigen oder bewusstlosen Personen
- Sofern möglich bei unmündigen/bewusstlosen Personen angepasste Informationen über das Forschungsvorhaben und die Möglichkeit der Zustimmung geben
- Freiwilligkeit bei der Zustimmung wahren. Die Zustimmung darf nicht durch Zwang, Gewalt oder Betrug erzwungen werden

Um diese informierte Zustimmung bei der vorliegenden Studie zu erhalten, wurde jedem Probanden ein schriftliches Informationsschreiben über den Sinn, den Zweck, die erhobenen Daten und den Umfang der Studie ausgehändigt. Zudem wurde im Informationsschreiben der Proband auf die Freiwilligkeit und die Rücktrittsmöglichkeit

von der Studie hingewiesen. Um die informierte Einwilligung schriftlich festhalten zu können, wurde dem Probanden eine schriftliche Einverständniserklärung vorgelegt.

Das 4. forschungsethische Prinzip macht eine Aussage darüber ob die Forschungstätigkeit positive oder negative Folgen für den Probanden mit sich bringen. Wichtig ist hierbei auch, dass die Anwendung der forschungsethischen Prinzipien durch den Forscher zeigen, dass dieser den Probanden als Mensch sieht und ihn auch so behandelt (Schnell & Dunger, 2018). Es ist bei dieser Studie davon auszugehen, dass die Teilnahme des Probanden an dieser Studie keine bzw. positive Folge für diesen hat.

Das 5. forschungsethische Prinzip verpflichtet den Forscher eine Einschätzung der Probandenvulnerabilität durchzuführen und zu überprüfen, welche Auswirkungen die Studie auf den Probanden hat (Schnell & Dunger, 2018).

In dieser Studie werden ausschließlich Interviews mit Experten durchgeführt. Einen Experten macht aus, dass er bereits lange Zeit in seinem Berufsfeld tätig ist und zudem Wissen und Strategien entwickelt hat wie er mit Belastungen umgeht. Dieser Definition nach ist ein Experte keine vulnerable Person und somit auch nicht verletzbar durch die Aufforderung von ihrer täglichen Arbeit zu erzählen (Schnell & Heinritz, 2006). Aus diesem Grund wurde das 6. forschungsethische Prinzip, dass angibt eine ethische Prävention zu etablieren (Schnell & Dunger, 2018), nicht beachtet. Dennoch wurde im laufenden Forschungsprozess die Probandenvulnerabilität stetig evaluiert, um auf Änderungen des Vulnerabilitätsprofils mit vulnerabilitätsangepassten ethischen Präventionen reagieren zu können.

Um die datenschutzrechtlichen Anforderungen (Amt für Veröffentlichungen der Europäischen Union [EUR-OP], 2016; Schnell & Heinritz, 2006) einhalten zu können, wurde den Teilnehmern mit dem Informationsschreiben ein Datenschutzhinweis ausgehändigt.

Zudem wurden die erhobenen Daten anonymisiert. Die Anonymisierung macht den Probanden namenlos und sorgt dafür, dass keinerlei Rückschlüsse auf den Probanden gemacht werden können, um Ihn vor dem Zugriff durch die Öffentlichkeit schützen zu können (Schnell & Heinritz, 2006).

Mit der Erfüllung der datenschutzrechtlichen Anforderungen wurde in dieser Studie das 8. forschungsethische Prinzip berücksichtigt.

Das Expóse wurde dem stellvertretenden Pflegedirektor des Klinikum Ingolstadt sowie dem Betriebsrat zur Durchführungsgenehmigung im Klinikum Ingolstadt vorgelegt. Die Zustimmung für die Durchführung der Masterarbeit und den damit verbundenen Interviews wurde durch die Geschäftsführung, die Pflegedirektion und den Betriebsrat erteilt

5.7. Gütekriterien

Eine wichtige Rahmenbedingung im Bereich der empirischen Forschung stellt die Bewertung der Forschungsergebnisse am Ende des Forschungsvorhabens anhand von Gütekriterien dar.

Die klassischen Gütekriterien (z.B. Reliabilität) wie sie in der quantitativen Forschung angewendet werden können in der qualitativen Forschung nicht unbedingt eins zu eins übernommen werden. Für den Bereich der qualitativen Forschung müssen die Gütekriterien neu betrachtet und definiert werden (Mayring, 2016). Mayring (2016) stelle in seiner Publikation sechs allgemeingültige Gütekriterien für qualitative Forschung auf:

- Verfahrensdokumentation
- Argumentative Interpretationsabsicherung
- Regelgeleitetheit
- Nähe zum Gegenstand
- Kommunikative Validierung
- Triangulation

In dieser Arbeit beschränkt sich die Überprüfung der Ergebnisse anhand der Gütekriterien ‚Verfahrensdokumentation', ‚Argumentative Interpretationsabsicherung, ‚Regelgeleitetheit' und ‚Nähe zum Gegenstand'. Im nachfolgenden werden diese Gütekriterien näher beschrieben:

Verfahrensdokumentation

Bei der Verfahrensdokumentation muss das Forschungsverfahren lückenlos und detailliert dokumentiert und nachvollziehbar dokumentiert werden. Bei quantitativen Forschungsvorhaben gelingt dies bereits durch die Anwendung standardisierter Techniken und Messverfahren. Im Rahmen der qualitativen Forschung besteht die Problematik darin, dass das Vorgehen spezifisch auf den Forschungsgegenstand ausgerichtet ist und dies spezielle Methoden erfordert. Vor allem muss hierbei das Vorverständnis genau erörtert werden, die Auswahl der Analyseinstrumentarien genau begründet und das Vorgehen bei der Datenerhebung genau erläutert werden (Mayring, 2016).

Argumentative Interpretationsabsicherung

Interpretationen von Forschungsergebnissen sind von großer Bedeutung im Zusammenhang mit qualitativen Forschungsansätzen. Interpretationen sind nicht beweisbar und können anders als in der quantitativen Forschung nicht einfach nachgerechnet werden. Das Gütekriterium der argumentativen Interpretationsabsicherung setzt zur Qualitätsabsicherung von Interpretationen voraus, dass diese argumentativ begründet werden. Hierbei spielen folgende Kriterien eine Rolle (Mayring, 2016):

- Das bestehende Vorwissen muss für die Interpretation adäquat sein
- Interpretationen müssen schlüssig sein bzw. Brüche müssen genau erläutert werden
- Suche nach Alternativdeutungen und deren Überprüfung

Regelgeleitetheit

Trotz großer Offenheit beim qualitativen Forschungsdesign und der Bereitschaft Schritte der Analyse im laufenden Prozess anzupassen, müssen diese Vorgänge sich stets an systematische Verfahrensregeln halten. Um das systematische und regelgeleitete Vorgehen einhalten und begründen zu können ist es von Notwendigkeit, Analyseprozesse in einzelne, sinnvolle Teilschritte zu zerlegen. Trotz der Regelgeleitetheit kann in begründeten Fällen von Regeln abgewichen werden (Mayring, 2016).

Nähe zum Gegenstand

Die Gegenstandsangemessenheit bzw. Nähe zum Gegenstand kann erreicht werden, wenn die durchgeführte Forschung sich so nah wie möglich an der Alltagswelt der zu untersuchenden Objekte/Subjekte orientiert. So macht es Sinn für Interviews sich in das 'Feld' zu begeben, in die reale Arbeits- oder Lebenswelt des Interviewpartners. Wichtig in diesem Zusammenhang ist auch eine Interessensübereinstimmung mit dem zu untersuchenden Subjekt. Qualitative Forschungsvorhaben wollen spezifische Sozialprobleme in den Fokus nehmen und die Forschung daran ausrichten. Zudem will qualitative Forschung Offenheit und Gleichberechtigung herstellen. Mit Hilfe der Interessensannäherung ist der Forschungsprozess möglichst nahe am Gegenstand dran. Ob dies gelungen ist, sollte im Nachgang nochmals überprüft werden (Mayring, 2016).

6. Darstellung der Ergebnisse

6.1. Die Rolle und die Notwendigkeit der Digitalisierung in der Pflege

Die Digitalisierung im Pflegebereich spielt eine große Rolle.

Laut dem Bürgerlichen Gesetzbuch sind Pflegeeinrichtungen zur Dokumentation der Behandlung verpflichtet (Bundesministerium der Justiz und für Verbraucherschutz [BMJV] & Bundesamt für Justiz [BfJ], 2021), aber auch gemäß dem Krankenhauszukunftsgesetz müssen sie spätestens ab dem 01.01.2025 elektronische Patientenakten führen (BMG, 2020b). Diese Aussage wird auch durch den Experten E unterstützt: „[…], dass es auch durch dieses Krankenhauszukunftsgesetz auch gesetzlich gefordert ist“ (Interview E, Pos. 346-348).

Nicht nur die gesetzliche Verpflichtung spielt eine erhebliche Rolle, sondern auch der mit der Einführung der digitalen Patientenakte einhergehende Mehrwert. Die Literatur liefert ebenfalls Hinweise auf Potenziale durch die Digitalisierung im Gesundheitswesen (Dörries et al., 2017). Experte E gibt im Interview an, dass komplexe Bereiche in der elektronischen Patientenakte besser dargestellt werden können (Interview E, Pos. 29-30).

Die elektronische Patientenakte sollte nicht als Akte für die Pflege oder die Ärzte gesehen werden, sondern als ganzheitlich den Patienten betreffend. Diese Ansicht vertritt auch Experte B: „Ich selber unterscheide eigentlich ungern zwischen Arzt- und Pflegedokumentation, sondern es gibt um den Patienten herum Dokumentation, die erbracht werden muss“ (Interview B, Pos. 23-25).

Bei der Digitalisierung gibt es aber noch Schwierigkeiten in der Entwicklung. In der Pflege ist diese nach wie vor nicht weit fortgeschritten und verläuft nur schleppend. Diese Meinung äußert auch Experte E: „Also wenn man sich die Industrie anschaut, die sind ja meilenweit voraus. Und gerade in Krankenhäusern, da dümpeln wir so langsam dahin“ (Interview E, Pos. 350-352). Die Experten C und F sind in Bezug auf die schleppende und rückständige Entwicklung ähnlicher Ansicht.

6.2. Bewertungen der Digitalisierungsentwicklung

Die Analyse ergab, dass ein Teil der Experten die Entwicklung der Digitalisierung in der Pflege als positiv bewertet. Diese Ansicht teilt Experte E: „Ich finde es gut. Und es wurde auch endlich Zeit, dass wir auch unsere Prozesse, unsere Dokumentation digitalisieren“ (Interview E, Pos. 36-37). Ähnliche Meinungen äußern die Experten N, G, F, C und B.

Bei einem anderen Teil der Experten gab es zur Thematik ‚Digitalisierungsentwicklung‘ kritische Stimmen. Diese Meinung vertritt unter anderem Experte L: „Zu langsam. Also ich glaube, in Deutschland könnten wir viel fortgeschrittener sein, sind es aber leider Gottes nicht“ (Interview L, Pos. 31-32). Die Experten N, M, J, B und D haben dazu ähnliche Ansichten.

Der Fortschritt und die Entwicklung der Digitalisierung in der Pflege und in den Krankenhäusern bringen auch eine Vielzahl von Herausforderungen mit sich. So beschreibt Pohlmann (2019), dass in Softwareprodukten viele Schwachstellen enthalten sind (Pohlmann, 2019). Es ist aber auch davon auszugehen, dass sich die Verantwortlichkeiten verschieben. Diese Ansicht teilt Experte I: „Einerseits verschieben sich natürlich Verantwortlichkeiten“ (Interview I, Pos. 34-35). Die Selbstverwaltung und die Verantwortung des Erkrankten im Umgang mit seinen Daten steigen. Auch hier unterstützt Experte I die Aussage mit seiner Meinung: „Selbstverantwortung der Patienten, mit ihren eigenen Daten zu arbeiten oder auch Einsicht in diese Daten nehmen zu können“ (Interview I, Pos. 37-38).

Es ist anzunehmen, dass rechtliche Fragestellungen mit der Digitalisierung einhergehen. Dies sieht auch Experte I so: „[…] in rechtlichen, juristischen Fragestellungen wie auch vielleicht Veränderungen in Berufsprofilen oder auch notwendigen Qualifizierungsmaßnahmen für Mitarbeiter im Haus, die mit solchen Veränderungen auch gesellschaftlicher Art und Weise ja umgegangen wird“ (Interview I, Pos. 40-43).

Neben rechtlichen ergeben sich ethische Fragestellungen. Krüger-Brand (2018) beschreibt in ihrem Artikel ebenfalls, dass mit der Digitalisierung viele ethische Fragen auf die Pflegenden zukommen (Krüger-Brand, 2018). Auch hier unterstützt Experte I diese Aussage mit einem Beispiel:

> *„[…] ethischer Aspekt. Wenn Informationen zu einem gewissen Zeitpunkt nicht vorhanden sind – also wir reden immer so ganz abstrakt von Informationen in IT-Systemen, aber wenn jetzt zum Beispiel eine Patientenverfügung zu einem gewissen Zeitpunkt ja nicht vorhanden ist und man reanimiert jemanden gegen seinen Willen vielleicht, dann ist man ja häufig schon in ethischen oder juristischen Fragestellungen drin. Und ich glaube, die Perspektive wird auch immer vergessen“ (Interview I, Pos. 568-574).*

6.3. Vorteile und Nachteile der papiergebundenen Patientenakte

Nach der Analyse der Interviews ist davon auszugehen, dass die papiergebundene Patientenakte eine Vielzahl von Vorteilen mit sich bringt.

Es liegt nahe, dass die physische Papierakte gerade bei Systemabstürzen oder bei Stromausfällen weiterhin genutzt werden kann. Diese Ansicht vertritt auch Experte A: „Papiergestützte Akten können bei Stromausfall und sonstigen Ausfällen immer noch einsehbar sein“ (Interview A, Pos. 15-16). Diese Aussage wird ebenfalls von den Experten O, K, L und H unterstützt.

Aufgrund der flexiblen Erweiterung der Papierakte durch die Anheftung von Dokumenten ist anzunehmen, dass Mitarbeitende schneller und vielfältiger dokumentieren können. Als Beispiel führt Experte I in seinem Interview Folgendes an: „Man kann sehr schnell auch handschriftliche Notizen, Ergänzungen machen“ (Interview I, Pos. 74-75).

Ein weiterer Vorteil liegt darin, dass der Umgang mit der Papierakte bereits routiniert erfolgt. Daraus lässt sich schließen, dass dies den Mitarbeitenden leichter fällt als mit der neuen elektronischen Akte. Diese Aussage wird durch den Experten L bestätigt: „In der Papierakte weiß man, welches Blatt man aufmachen muss, um eben nachzuschauen, was wo ist, ohne viele Klicks zu machen“ (Interview L, Pos. 47-49). Experte F ist ähnlicher Meinung und erwähnt darüber hinaus, dass die Umstellung von der papiergebundenen zur digitalen Akte für die Mitarbeitenden enorm wäre (Interview F, Pos. 69-71).

Durch die einmalige und örtliche Verfügbarkeit der Papierakte ergibt sich höchstwahrscheinlich der Vorteil, dass der Zugriff durch Dritte erschwert möglich ist, was den Schutz der Daten begünstigt. Dies sieht Experte F ähnlich: „dass die natürlich sicherer ist, was den Datenschutz betrifft“ (Interview F, Pos. 63-64).

Ein weiterer Mehrwert der Papierakte scheint die Verifizierungsmöglichkeit erhobener Vitalwerte zu sein, da diese im Gegensatz zur digitalen Akte nicht automatisch übernommen werden. Die Fachkräfte können die Vitalwerte vor der Dokumentation analysieren und bewerten. So können falsche hohe bzw. niedrige Wert infolge von Messfehler gekennzeichnet oder nach erneuter korrekter Messung nicht dokumentiert werden. Diese Ansicht vertritt auch Experte O: „[…] sollte der Patient einfach irgendwelche Falschmessungen von irgendwelchen Werten (...) Klar, die werden von uns nicht so dokumentiert. Es muss natürlich die Einschätzung da sein, dass jetzt zum Beispiel der Blutdruck nicht stimmt“ (Interview O, Pos. 62-65). Durch die Überprüfung der Daten, können Missverständnisse verhindert werden.

Die Analyse brachte aber ebenfalls hervor, dass es bei der papiergebundenen Patientenakte neben den Vorteilen auch Nachteile gibt.

Aufgrund der einmalig vorhandenen Papierakte ist davon auszugehen, dass deren Verfügbarkeit eingeschränkt ist. Diese Aussage teilt Experte O:

> *„Ist der Patient jetzt mal bei der Untersuchung und nimmt seine Akten weg, weiß ich vom Patienten gar nichts. Ich weiß nicht, welche Tabletten er bekommen hat, welche Medikamente, wie die letzten Vitalparameter waren, und kann dann auch, wenn Fragen kommen, nicht antworten. Sei es Visitenärzte, Untersuchungen etc.“ (Interview O, Pos. 54-58).*

Zu einer ähnlichen Ansicht kommen die Experten J, E und C.

Des Weiteren kann durch die Einmaligkeit davon ausgegangen werden, dass nur ein Mitarbeitender zur selben Zeit an der Akte arbeiten kann. Diese Auffassung vertritt auch Experte L: „Die Papierakte, wenn eine Person sie hat, dann ist sie weg. Dann kann die andere Person nicht damit arbeiten“ (Interview L, Pos. 46–47).

Ein weiterer Nachteil, der mit der Einmaligkeit der Papierakte einhergeht, ist deren möglicher Verlust, da diese auch mit den Erkrankten zu Untersuchungen mitgenommen wird. Diese Gefahr sieht auch Experte O in der Befragung: „Es kann verlorengehen natürlich, was auch sehr häufig passiert, leider, dass Akten verlorengehen“ (Interview O, Pos. 51–52).

Darüber hinaus hat jeder Mensch eine einzigartige und individuelle Handschrift (Bundeskriminalamt [BKA], o.J.). Durch die handschriftliche Dokumentation in der Papierakte kann die Lesbarkeit beeinträchtigt werden. Eine vergleichbare Ansicht vertritt Experte I: „[…], dass man vielleicht dann die Handschrift nicht entziffern kann“ (Interview I, Pos. 76–78). Die Experten K und J äußern eine ähnliche Meinung.

Aufgrund der Nichtlesbarkeit mancher Handschriften kann davon ausgegangen werden, dass es zu Übertragungsfehlern in den Folgeakten kommt. Dies sieht auch Experte J so: „ […] fehleranfällig, wenn ich es übertragen muss“ (Interview J, Pos. 55).

Einen weiteren Nachteil stellt höchstwahrscheinlich die geringere Datenqualität der Papierakte dar, wenn Fehleingaben von Daten nicht erkannt werden (Interview B, Pos. 60–63).

Da die Archivierung der Papierakten auf digitalen Datenträgern oder Mikrofilmen viele Jahre zu erfolgen hat, kann angenommen werden, dass dies mit viel Arbeit verbunden ist. Diese Ansicht teilt auch Experte B: „Ich sehe das Problem mit der Archivierung. Entweder man macht eine Mikroverfilmung oder man lagert es ein und am Ende wird es eigentlich digital eingescannt. Dann sollten wir versuchen, gleich von vorneherein auf das digitale Ausfüllen zu gehen“ (Interview B, Pos. 56–59). Darüber hinaus müssen entsprechend gesicherte Archivräume bereitgestellt werden (Interview I, Pos. 82–83).

Es kann vermutet werden, dass durch die Fortschreibung der Papierakten mit einem erhöhten Arbeitsaufwand zu rechnen ist. Dies sieht auch Experte K: „[…], dass man Dinge, die man schonmal notiert hat, immer und immer wieder notieren muss unter Umständen und nicht übernehmen kann“ (Interview K, Pos. 40–42).

Gerade im Gesundheitssektor spielt die Vernetzung der an der Behandlung beteiligten Akteure eine bedeutsame Rolle. So können durch die Digitalisierung Informationen gewonnen und zum Informationsaustausch an andere Akteure weitergeleitet werden (Ebert et al., o.J.). Dies ist mit der Papierakte nur erschwert oder gar nicht möglich. Dieser Meinung ist auch Experte I: „Man hat natürlich keine Vernetzung zwischen den unterschiedlichen Akteuren im Gesundheitswesen. Also das ist natürlich dann schwierig, da einen Austausch zwischen dem ambulanten und stationären Bereich zu haben“ (Interview I, Pos. 83–86).

Ein weiterer Nachteil der Papierakte scheint die fehlende Möglichkeit zu sein, automatische Kontroll- und Erinnerungsfunktionen für die Mitarbeitenden in Bezug auf die Dokumentation oder Erneuerung gewisser Daten einzubauen. Diese Ansicht vertritt auch Experte C: „Ich kann was eintragen, ich kann es auch lassen. Es erinnert mich niemand an irgendetwas“ (Interview C, Pos. 72–73).

6.4. Vorteile und Nachteile der elektronischen Patientenakte

Die Einführung der elektronischen Patientenakte bringt viele Vorteile mit sich (Dörries et al., 2017). Diese Ansicht vertritt auch Experte G: „Vorteile gibt es viele“ (Interview G, Pos. 36)

Durch die digitale Verfügbarkeit ist ein ortsunabhängiger Aktenzugriff mit jedem elektronischen Endgerät möglich, das die digitale Patientenakte unterstützt. Diesen

Vorteil beschreibt auch Kropp (2016) in seiner Arbeit. Außerdem wird diese Aussage durch den Experten M in seinem Interview bestätigt:

> *„Digitalisierung ist insoweit von Vorteil, dass halt alle Berufsgruppen auf die gleiche Akte Zugriff haben, unabhängig von den anderen, was halt bei der Papierakte nicht möglich war. Wenn die zu einer Untersuchung war oder so, dann konnte niemand mehr auf die Akte zugreifen“ (Interview M, Pos. 27–30).*

Auch die Experten N, L, C und B sind der Ansicht, dass sich durch die Gleichzeitigkeitssituation und die Nutzung der elektronischen Patientenakte an jedem unterstützen Endgerät die Verfügbarkeit im Allgemeinen verbessert.

Durch die Digitalisierung in der Pflege kann die Effizienz im Pflegealltag gesteigert werden (Dörries et al., 2017). Die Vermutung liegt nahe, dass dies Zum Teil an der Übersichtlichkeit und Transparenz der in der elektronischen Patientenakte dargestellten Prozesse liegt. Letztere können so reibungslos und schneller voranschreiten. Dies spiegelt auch Experte I in seinem Interview wider: „Prozesse schneller laufen“ (Interview I, Pos. 57). Daraus kann geschlossen werden, dass durch die gesteigerte Effektivität der Prozesse die Versorgungsqualität gesteigert und die Kosten gesenkt werden können.

Des Weiteren hält der Einsatz von künstlicher Intelligenz (KI) im Pflegealltag immer mehr Einzug (Elsner & Koch, o.J.). Infolgedessen können den Mitarbeitenden in Problemsituationen Entscheidungshilfen an die Hand gegeben werden (Interview B, Pos. 39–40). Daraus lässt sich die Empfehlung ableiten, den Einsatz von künstlicher Intelligenz im Pflegebereich zu fördern, um den Beschäftigten die Arbeit beispielsweise durch KI-gestützte Entscheidungsfindung zu erleichtern und damit einen lösungsorientierten Ansatz zu verfolgen. Durch die Verwendung elektronischer Endgeräte zur Eingabe von Daten werden diese in einheitlicher Darstellung wiedergegeben. Demzufolge ist die elektronische Patientenakte von jedem Mitarbeitenden lesbar. Experte G bestätigt dies im Interview: „keine handschriftlichen Sachen, die man nicht lesen kann“ (Interview G, Pos. 37–38).

Zudem ist davon auszugehen, dass Lese- und Interpretationsfehler durch die einheitliche digitale Darstellung ausgeschlossen werden können. Dies sieht Experte K im Interview ähnlich (Interview K, Pos. 32–33).

Aufgrund der Datendigitalisierung liegt die Vermutung nahe, dass der Aktenzugriff durch mehrere Mitarbeitende gleichzeitig gewährleistet werden kann. Darüber hinaus können Daten schneller und leichter zwischen den an der Behandlung beteiligten Akteuren ausgetauscht werden, was wiederum die Versorgungsqualität erhöhen kann (Dörries et al., 2017). Dies bestätigt auch Experte K in seiner Befragung: „[…] Daten verfügbar sind und weitergereicht werden können, man auch einen Datenaustausch betreiben kann auf relativ einfachem Weg“ (Interview K, Pos. 33–35). Experte I vertritt eine ähnliche Meinung.

Durch den Einsatz von Erinnerungs- und Kontrollfunktionen in der digitalen Akte können Mitarbeitende vermutlich darauf hingewiesen werden, bestimmte Daten zu

dokumentieren oder zu aktualisieren. Das betont auch Experte C: „Diesen Vorteil hat natürlich die digitale Dokumentation durchaus, dass man Reminder mit einbauen kann, dass man gewisse Prozesse einfach mit einfordert und abbildet“ (Interview C, Pos. 77–7). Experte J geht noch einen Schritt weiter und schlägt die Hinterlegung einer Warnfunktion vor, um „[…] Warnungen zu generieren“ (Interview J, Pos. 46). Daraus lässt sich ableiten, dass eine solche Funktion etwa beim Management von Medikamenten eingesetzt wird, um Mitarbeitende vor einer Überdosierung zu warnen.

Ein weiterer Vorteil der elektronischen Patientenakte besteht darin, dass große Mengen archiviert werden können (Dujat, 2014). Durch die digitalen Daten und deren leichtere Handhabung ist eine statistische Auswertung schnell und unkompliziert durchzuführen. Diese Ansicht vertritt auch Experte J im Interview (Interview J, Pos. 45).

Darüber hinaus kann der Erkrankte durch die Bereitstellung digitaler Inhalte aus der Patientenakte am Genesungsprozess beteiligt werden. Dies kann beispielsweise im Rahmen des Patienten-Empowerments oder der Informierten Einwilligung passieren (Dörries et al., 2017; Schnell & Heinritz, 2006). Somit werden die Mündigkeit des Patienten gefördert und die Patienteninformiertheit erhöht. Diesen Standpunkt vertritt auch Experte I: „[…], dass der Patient da zu einem mündigeren Patienten wird und vielleicht auch mehr Einsicht bekommt“ (Interview I, Pos. 54–55).

Genauso wie bei der papiergebundenen gibt es bei der elektronischen Patientenakte Herausforderungen. Besonders bei deren Einführung können zu überbrückende Hindernisse auftreten. Diese Ansicht teilt auch Experte B: „Ich sehe eigentlich gar keine Nachteile. Nachteil, da mag ich das Wort nicht. Es gibt halt Herausforderungen“ (Interview B, Pos. 37–38).

Bei einer nicht benutzerfreundlich gestalteten elektronischen Patientenakte kann angenommen werden, dass diese durch die Vielzahl von Prozessen, die darin abgebildet werden müssen, umständlich und kompliziert zu nutzen ist. Dieser Meinung ist auch Experte M bei der Befragung: „Also aktuell mit diesen Programmen, die wir jetzt aktuell zur Verfügung haben, ist es oftmals zu umständlich noch“ (Interview M, Pos. 40–41). Die Experten O, L, F und E äußern in der Befragung ähnliche Meinungen. Daraus lässt sich für die Praxis ableiten, dass die elektronische Patientenakte die Prozesse möglichst unkompliziert und übersichtlich darstellen und die Dokumentation flexibel und übersichtlich gestaltet sein sollte.

Eine weitere Herausforderung besteht, wenn die fehlende Verfügbarkeit der elektronischen Patientenakte (z.B. bei einem Stromausfall) zu Verzögerungen und Schwierigkeiten bei der Patientenversorgung führt. Das Problem mit Stromausfällen nannten auch Höhne und Lenz (2019) in ihrem Artikel. Experte O gibt an, dass es zu Problemen bei der Medikamentengabe kommen kann: „Sollte das Internet mal nicht funktionieren, wenn wir irgendwelche Ausfälle haben sollten, stelle ich mir schwierig vor, dann Medikamente zu geben“ (Interview O, Pos. 44–46). Auch die Experten L und G sehen Herausforderungen bei der fehlenden Verfügbarkeit der digitalen Patientenakte. Daraus lässt sich schließen, dass es bei einem Ausfall des

elektronischen Systems zu schwerwiegenden Einschränkungen bis hin zum vollständigen Stillstand des Prozessablaufes kommt.

Aufgrund der automatischen Übernahme der Vitalwerte vom elektronischen Messgerät in die digitale Patientenakte kann die Gefahr bestehen, dass falsch gemessene Vitalzeichenwerte – beispielsweise durch Artefakte – bei den anderen Mitarbeitenden zu Missverständnissen führen. Dies kann dadurch bedingt sein, dass die Mitarbeitenden bei der Messung nicht anwesend waren und die Umstände nicht kennen. Eine ähnliche Meinung vertritt auch Experte O: „Oder was natürlich dann bei der elektronischen Akte wahrscheinlich genauso übernommen wird, wo es natürlich dann auch zu Missverständnissen kommen kann“ (Interview O, Pos. 65–67). Draus lässt sich für die Praxis ableiten, dass die Datenintegrität bei der Übernahme jedes gemessenen Vitalzeichenwertes nicht gegeben ist, da die Umstände der Messsituation durch das Messgerät nicht dokumentiert worden sind. Dies kann verhindert werden, wenn vor der Übertragung der gemessenen Vitalzeichenwerte eine Überprüfung durch die Fachkraft stattfinden kann und diese auch die Möglichkeit hat, die Umstände der Messsituation am Messgerät festzuhalten. So können Falschmessungen für die lückenlose Dokumentation gekennzeichnet und dadurch nachfolgende Missverständnisse verhindert werden.

Durch die hohe Verfügbarkeit der Daten ist anzunehmen, dass es zu datenschutzrechtlichen Herausforderungen kommen kann. Bei der elektronischen Patientenakte müssen die rechtlichen Grundlagen genauso erfüllt werden wie bei der papiergebundenen (BMG, 2020c). Gerade durch den Umstand, dass mehrere Personen auf die elektronische Patientenakte zugreifen können, sieht Experte A hierbei ein Problem:

> *„Ich denke, der Datenschutz ist ein Riesenproblem. Gerade, wenn man in Häusern ist, in denen das Personal in verschiedenen Bereichen arbeitet, sehe ich es als sehr schwierig, weil einmal das Problem ist, dass zu viele Daten freigegeben werden für einen Mitarbeiter“ (Interview A, Pos. 27–30).*

Daraus lässt sich für die Praxis ableiten, dass bei der Implementierung und im Betrieb der elektronischen Patientenakte die datenschutzrechtlichen Grundlagen einbezogen und in das System integriert werden. Zudem müssen die Mitarbeitenden für das Thema Datenschutz sensibilisiert werden, da sie mit der elektronischen Patientenakte arbeiten und damit für deren Schutz verantwortlich sind. Darüber hinaus müssen individuelle und berufsgruppenspezifische Rollen- und Berechtigungskonzepte entwickelt und den Mitarbeitenden zugeordnet werden, damit nur das am Erkrankten tätige Personal auf die Daten zugreifen kann, für die es verantwortlich ist.

Es besteht die Annahme, dass elektronische Patientenakten durch die spezialisierten Fähigkeiten von Cyberkriminellen kompromittiert werden können. Diese Gefahr sieht auch Experte I: „Nachteile natürlich die Sicherheit der Systeme allgemein. Da sind natürlich sensible Informationen hinterlegt, die nun entsprechend durch die Krankenhäuser auch geschützt werden müssen“ (Interview I, Pos. 64–66). Demgegenüber gibt Experte B zwar an, dass digitale Akten angreifbar sind, aber er

gibt zu bedenken, dass es statistisch gesehen annähernd viele Zwischenfälle mit der Papierakte (z.B. durch Brand) wie mit der elektronischen Patientenakte (z.B. Verschlüsselungen) gab (Interview B, Pos. 43–46).

Die Vermutung liegt nahe, dass nichttechnikaffine Mitarbeitende Schwierigkeiten bei der Benutzung der elektronischen Patientenakte haben. Daraus lässt sich ableiten, dass diese Mitarbeitenden oftmals vor Problemen im Umgang mit der Technik stehen. Dieser Meinung ist auch Experte I: „Nachteil vielleicht für Leute, die jetzt nicht so Digital Natives sind, auch Zugang zu dieser neuen Dokumentation bekommen, sowohl von Mitarbeiterperspektive als auch von Patientenperspektive“ (Interview I, Pos. 66–69). Diesen Standpunkt vertreten auch die Experten E und F. Folglich besteht die Gefahr, dass die Akzeptanz gegenüber der elektronischen Patientenakte und deren täglicher Benutzung sinkt. Die Handlungsempfehlung kann dahingehend sein, dass nichttechnikaffinen Mitarbeitenden umfangreichere und an sie angepasste Schulungen angeboten werden, um den Umgang mit der elektronischen Patientenakte zu lernen. Eine mögliche Folge davon könnte sein, dass die Akzeptanz demgegenüber steigt.

Eine weitere Herausforderung stellen die finanziellen Aspekte für das Krankenhaus dar. Die Einführung von neuen Software- und Hardwareprodukten ist für Unternehmen immer mit hohen Investitionskosten verbunden (Deutsches Krankenhausinstitut [DKI] & BDO, 2019). Betriebe müssen auf Wirtschaftlichkeit achten, dennoch sollte bei der Digitalisierung der Patientenakten nicht gespart werden. Dieser Meinung ist auch Experte B: „[…] wirtschaftlich sein soll, aber ich meine halt, dass man dann dazu auch schon Geld in die Hand nehmen muss, weil dazu braucht es dann einfach Tablets für die Umsetzung, zum Beispiel. Und das kostet dann natürlich auch Geld“ (Interview F, Pos. 55–57). Daraus lässt sich für die Praxis ableiten, dass alle notwendigen Ressourcen für die Digitalisierung zur Verfügung gestellt werden müssen. Dies sollte jedoch unter der Berücksichtigung wirtschaftlicher Gesichtspunkte ablaufen. Im Vorfeld sollte geprüft werden, welche Funktionalitäten die elektronische Patientenakte haben muss und ob die angeschafften Systeme skalierbar sind.

6.5. Implementierung einer elektronischen Patientenakte im Krankenhaus

Es liegt nahe, dass die Implementierung einer elektronischen Patientenakte für ein Krankenhaus ein großes Projekt darstellt, das von vielen Faktoren abhängig ist. Dies sieht auch Experte K ähnlich: „[…] das ist ein Irrsinns-Projekt, weil es verzahnt werden muss in alle möglichen Richtungen“ (Interview K, Pos. 52–53). Die Analyse zeigt, dass sich die Vorbereitung und Vorplanung vor allem auf die drei großen Bereiche ‚Anforderungen an das System‘, ‚Technik‘ und die ‚Finanzierung‘ beziehen sollen. Diese Ansicht vertritt auch Experte E: „[…], wenn man das umsetzt, dass man wirklich sehr gut von vornherein plant, finanziell, aber auch technisch mit der technischen Ausstattung“ (Interview E, Pos. 121–123). Die Experten K, I und B tätigen ähnliche Aussagen zu dieser Thematik.

Es ist zu vermuten, dass die Umstellung von der Papierakte auf die digitale Akte für die Mitarbeitenden nur praktikabel ist, wenn sie komplett in einem Zug erfolgt. Dieser Meinung ist auch Experte N in der Befragung:

> *„Wie gesagt, am schlechtesten ist jetzt, wenn man beides hat, also wenn man zwar probiert, auf der einen Seite, die Digitalakte einzuführen, und auf der anderen Seite aber trotzdem immer nur auf Papier dokumentiert. Also, das ist, glaube ich, das Ungünstigste, weil das versteht irgendwann keiner und dann wird es auch nicht so genutzt“ (Interview N, Pos. 78–82).*

Die Experten M und O sind ähnlicher Meinung.

Es ist davon auszugehen, dass die Erfolgsindikatoren für eine erfolgreiche Implementierung immer individuell sind. Dennoch gibt es nach der Analyse der Interviews bestimmte Indikatoren, die für eine erfolgreiche Einführung sprechen. Einer davon besteht darin, dass sich die Mitarbeitenden in der Patientenakte wiederfinden (Interview N, Pos. 69–70). Das heißt auch, dass alle die berufsgruppenspezifischen Informationen benötigen, darauf Zugriff haben und das unabhängig von jeglicher Papierakte möglich ist (Interview M, Pos. 53–55). Experte K ist der Meinung, dass die Implementierung erfolgreich ist, wenn alle Mitarbeitenden gemeinsam in der elektronischen Patientenakte arbeiten können (Interview K, Pos. 55–57). Ein weiterer Indikator ist nach Experte F, wenn die elektronische Patientenakte eine Entlastung für alle Berufsgruppen ist und keinen Mehraufwand mit sich bringt (Interview K, Pos. 55–57). Daraus lässt sich für die Praxis ableiten, dass es Teil der Vorplanung ist, auch die Indikatoren für eine erfolgreiche Einführung der elektronischen Patientenakte individuell festzulegen. Aufgrund der Aussagen der Experten ist nämlich davon auszugehen, dass jeder Experte und jedes Unternehmen andere Ansichten und einen anderen Anspruch an eine erfolgreiche Implementierung haben.

Mitarbeitende müssen im Hinblick auf eine erfolgreiche Implementierung der elektronischen Patientenakte einen gewissen Grad an Akzeptanz, Mut und Motivation mitbringen müssen, da es laut dem Experten N zu Problemen kommen kann, wenn Beschäftigte nicht einbezogen werden: „Weil sonst wird es sehr schwierig, sonst wird es ja nicht akzeptiert. Also das ist ganz ein großes Akzeptanzproblem dann“ (Interview N, Pos. 70–71). Des Weiteren gehören zu einer Implementierung eine gewisse Vision sowie der Mut, Neues zu probieren. Diese Ansicht vertritt auch Experte B: „Man muss an der Stelle schon einen gewissen Mut zu einer Vision mitbringen, auch Dinge mal zu fordern, die es vielleicht heute noch nicht gibt, oder Dinge zu kaufen, schon ein bisschen esoterisch, Science-Fiction, aber am Ende wird man feststellen, dass es vielleicht eine gute Entscheidung ist, etwas getan zu haben, was in fünf Jahren sich erst etabliert. Dann ist man zumindest am Markt als Pionier oder Early Adopter mit dabei“ (Interview B, Pos. 72–77).

Es ist davon auszugehen, dass Mitarbeitende motivierter sind, wenn ein Bezug zu ihrer Profession hergestellt wird. Diese Aussage betont Experte C im Interview:

> *„[…] im Voraus die Mitarbeiter sensibilisieren muss, dass wir Vorbehaltsaufgaben haben, dass wir den Pflegeprozess abbilden müssen, dass das unsere Profession mitbringt, dass wir den Patienten aus professioneller pflegerischer Sicht in diesen Pflegeprozessen, in der Pflegeplanung abbilden und uns der ganzen Sache mit annehmen“ (Interview C, Pos. 96–100).*

Die mit der digitalen Pflegeakte einhergehende Transparenz sollte auch dazu genutzt werden, Erstere weiterzuentwickeln. Auch Dörries et al. (2017) führen die Kommunikation, die durch die digitalisierte Patientenakte ebenfalls transparent ist, als Faktor zur Verbesserung der Versorgungsqualität an. Eine ähnliche Ansicht hat Experte C:

> *„[…], sondern auch ganz gezielt diese Transparenz, dass das System mitbringt, nutzen und schauen: Wie wird es denn überhaupt verwendet? Sind noch Anwendungsfehler drin oder Lücken, die entstehen? Oder umgeht irgendjemand irgendwie die Dokumentation? Wo muss man nochmal nachschulen? Dass das Transparente auch genutzt wird“ (Interview C, Pos. 180–184).*

6.6. Finanzielle Rahmenbedingungen

Die Investitionskosten für die Implementierung einer digitalen Patientenakte sind hoch (DKI & BDO, 2019). Dies sieht auch Experte D im Interview ähnlich (Interview D, Pos. 105). Es ist davon auszugehen, dass die genaue Höhe von den Anforderungen und der vorhandenen technischen Infrastruktur der Klinik abhängig ist. Dass die Kosten im Bereich mehrerer Millionen Euro liegen, ist laut dem Experten N sicher: „Für so ein größeres Klinikum, denke ich, geht es schon in die Millionen, denke ich mal, wenn man das wirklich umsetzen möchte“ (Interview N, Pos. 87–89). Auch Experte H gibt eine ähnliche Einschätzung ab.

Es scheint ratsam, die Finanzierung der elektronische Patientenakte im Voraus zu planen. Diese Finanzierungsfrage sieht auch Experte I im Interview: „Genau, also vielleicht tatsächlich noch ein Punkt, der aber jetzt nicht so in das ganze Thema mit einfließt, aber für Krankenhäuser wahrscheinlich doch immer noch relevant ist, ist natürlich das Thema: Wie finanziert sich denn das Ganze?“ (Interview I, Pos. 534–537).

Daher sollte auch im Rahmen der Finanzierungsplanung analysiert werden, ob sich das einzuführende Projekt rentiert oder es Alternativen gibt. Es liegt nahe, dass Systeme und Projekte, die sich nicht rentieren, abgelehnt werden sollten. Dies sieht auch Experte B so:

> *„Also man sollte mal den Mut haben, zu sagen: Ein Projekt, das sich nicht wirklich sauber rechnet, das macht man nicht. Und ein Projekt, wo wieder nur von Anfang an gespart wird, sollte man vielleicht auch mal ablehnen. Das heißt nicht, dass ich das Geld in vollen Händen rausschmeiße. Aber diese ständige Diskussion, alles muss immer noch billiger werden, das sorgt nicht für Qualität“ (Interview B, Pos. 149–154).*

Es ist davon auszugehen, dass die meisten Kosten bei der Anschaffung von Hard- und Software entstehen. Dieser Meinung ist auch Experte N: „Die Endgeräte kosten wahrscheinlich Geld. Dann die Software, wenn es eine spezielle Software ist, oder wenn es eine ist, die man vielleicht gemeinsam mit einer Firma erarbeitet. Das kostet natürlich Geld“ (Interview N, Pos. 85–87).

Der Analyse nach stellen die personellen Ressourcen für Schulungen einen weiteren Kostenfaktor für das Unternehmen dar: „[…] nicht finanziert werden kann, das ist die personelle Implementierungsbegleitung. Also das heißt, da muss das Unternehmen unbedingt dazu bereit sein, personelle Ressourcen freizugeben und bereitzustellen, dass man dieses Mammutprojekt auch tatsächlich schaffen kann“ (Interview C, Pos. 174–177). Auch die Experten G, I, E und A treffen ähnliche Aussagen.

Trotz der hohen Kosten scheint es ratsam zu sein, bei der Implementierung nicht zu sparen. Dies betonen auch die Experten E und F. Wenn an den Kosten gespart wird, liegt die Vermutung nahe, dass die Implementierung der digitalen Patientenakte scheitern wird. Dieser Meinung schließt sich auch Experte B an: „Wenn ich keine vernünftige Software kaufe, dann spare ich halt bei der dritten Säule. Jetzt habe ich schon beim Personal gespart, jetzt sparen wir auch noch bei der Software. Dann wird es irgendwann nicht mehr rund“ (Interview B, Pos. 156–158). Hier sind sich die Experten O, K, E und B einig, dass Investitionsfehler auch Jahre nach der Einführung noch zu Schwierigkeiten führen können.

Langfristig werden sich durch die elektronische Patientenakte Kosten einsparen lassen (Breinich-Schilly, 2021). Dies lässt sich vermutlich auf die höhere Verfügbarkeit der Mitarbeitenden für andere Tätigkeiten zurückführen. Auch Experte N vertritt diese Meinung:

> *„[…] im Endeffekt vielleicht trotzdem irgendwo eine Ersparnis hat, weil die Leute wieder mehr verfügbar sind auf der Station. Man kann sich dann vielleicht vorstellen, dass die Pflegekraft direkt gleich am Bett dokumentiert oder über ein Tablet dokumentiert, dass das praktisch schon im Arbeitsablauf integriert ist. Also ich denke schon, dass man da irgendwo den wirtschaftlichen Nutzen letzten Endes hat“ (Interview N, Pos. 89–94).*

Daraus lässt sich schließen, dass sich langfristig trotz der hohen Investitionskosten eine Kostenersparnis einstellt, da die Mitarbeitenden wieder mehr am Erkrankten verfügbar sind.

Da die Investitionskosten für eine elektronische Patientenakte nicht über das Diagnosis Related Groups System abgerechnet werden können, müssen Krankenhäuser sie selbstständig aufbringen (Hillienhof, 2019). Experte I bestätigt diese Aussage:

> *„Also klassisch ist ja das Konzept im Krankenhaus darauf ausgelegt, dass es eine Patientenbehandlung gibt und es dann eine gewisse DRG-Ziffer gibt, einen Schwergrad, und dann kriegt man eine gewisse Pauschale. Diese ganzen, ich sage jetzt mal, Digitalisierungsthemen oder auch der Betrieb der IT-Abteilung, der*

> *findet sich ja aktuell nicht in irgendeiner Vergütung wieder oder in irgendeiner nachhaltigen Finanzierung. Das heißt, das ist, glaube ich, schon immer so ein übergeordneter Punkt, der da mitspielt. Also alles muss aus dem Tagesgeschäft irgendwo erwirtschaftet werden, dass solche Projekte umgesetzt werden können, bzw. gibt es aktuell noch keinen Digitalisierungszuschlag für Krankenhäuser, damit auch sowas sicher und nachhaltig betrieben werden kann“ (Interview I, Pos. 537–547).*

Um einen Teilersatz für die Investitionskosten zu erhalten, wurde das Krankenhauszukunftsgesetz verabschiedet. Damit sollen Krankenhäuser bei ihren Digitalisierungsvorhaben finanziell unterstützt werden (BMG, 2020b). Diese Hoffnung erwähnt auch Experte G in seinem Interview: „Da wir gerade mit dem Krankenhauszukunftsgesetz gute Chancen haben, viele Sachen digital umzustellen – darunter läuft jetzt wahrscheinlich auch, dass wir die Pflegedokumentation implementieren können –, da können wir schon viel Geld abdecken“ (Interview G, Pos. 73–76). Eine ähnliche Meinung vertreten die Experten I, E und C. Diesen Wunsch nach finanzieller Unterstützung würde die Forderung des Experten E zu einem Teil erfüllen: „[…] endlich mal eine Zeit gekommen, dass auch die Gelder seitens der Regierung oder Länder zur Verfügung gestellt werden, dass man endlich diesen Prozess auch in Kliniken nach vorne bringt“ (Interview E, Pos. 348–350).

6.7. Technische Rahmenbedingungen

Vor der Implementierung sollte in der Regel eine Bedarfsanalyse hinsichtlich der benötigten technischen Komponenten durchgeführt werden. Dieser Ansicht ist Experte I ebenfalls: „[…] in einem dritten Schritt eine Analyse durchzuführen: Welches System würde denn passen und über welchen Implementierungszeitraum sprechen wir denn eigentlich?“ (Interview I, Pos. 98–100). Auch Experte A äußert einen vergleichbaren Standpunkt.

Es ist zu vermuten, dass der komplette Behandlungsprozess gut und übersichtlich abgebildet werden muss. Diese Ansicht vertritt auch Experte J: „Also man muss als erstes sich ein System suchen, was eben den gesamten Prozess möglichst gut abbildet“ (Interview J, Pos. 100–101). Auch Experte E sieht dies ähnlich.

Daraus kann für die Praxis geschlossen werden, dass die Softwareprodukte in Rücksprache mit den Mitarbeitenden – denn diese müssen die elektronische Patientenakte letztendlich nutzen – bezüglich der Anforderungen angeschafft werden müssen.

Es besteht Grund zur Annahme, dass die in den Krankenhäusern bereits vorhandene digitale Technologie aktualisiert und bei Bedarf ausgetauscht werden sollte, damit die Implementierung der elektronischen Patientenakte reibungslos vonstattengeht. Dieser Meinung ist auch Experte M:

> *„Und das ist ja nicht nur die Anschaffung, sondern dass man auch drauf guckt, wenn ich mir das jetzt einmal anschaffe, dass es nicht hier zehn Jahre bestehen bleibt, sondern es muss auch drauf geguckt werden, dass man immer die neueste*

> *Hardware zur Verfügung hat, um das nutzen zu können“ (Interview M, Pos. 82–86).*

Auch die Experten A und I vertreten den Standpunkt, dass die alte und überholte technische Infrastruktur in den Krankenhäusern dringend gewartet und verbessert werden muss. Dies spricht für die Praxis, dass Unternehmen ihre bestehenden digitalen Technologien prüfen, warten und gegebenenfalls austauschen lassen, um die zukünftige Digitalisierung in der Pflege vorantreiben zu können.

Es ist naheliegend, dass die Kompatibilität eine Anforderung an das System darstellt. Da sowohl unterschiedliche Software- als auch Hardwareprodukte im Krankenhaus verwendet werden, ist davon auszugehen, dass diese Systeme untereinander kommunizieren müssen. Dies sieht auch Experte K in der Befragung so: „Also es gibt sicher gute Lösungen, die auf dem Markt schon verfügbar sind, die man verwenden kann. Aber man muss unbedingt dafür sorgen, dass die dann auch alle miteinander kommunizieren“ (Interview K, Pos. 95–97). Eine ähnliche Ansicht vertritt Experte D.

Es ist davon auszugehen, dass bei der Implementierung eine ausreichende Anzahl von elektronischen Endgeräten zur Verfügung stehen muss. Experte E hebt diese Aussage nochmals hervor:

> *„[…] muss mir auch bewusst sein als Geschäftsführer, dass wir entsprechende Hardware auch benötigen. Also als Beispiel, wenn ich eine digitale Pflegedokumentation einführe, kann es ja nicht sein, dass wir nur mit den kleinen Geräten ausgestattet sind, wie zum Beispiel Tablets, weil da kann ich nicht die gesamte Dokumentation abbilden, aber wohl einen bestimmten Teil, zum Beispiel Wundversorgung. Aber für die gesamte Dokumentation benötige ich eine Hardware mit größeren Bildschirmen, wo ich dann sehr gut arbeiten kann, ohne hin- und herscrollen zu müssen“ (Interview E, Pos. 110–117).*

Die Experten O, M, H, F, D und B sprechen sich ebenfalls für genügend Geräte aus. Daraus folgt, dass für die Implementierung und den Betrieb der elektronischen Patientenakte eine ausreichende Anzahl von Endgeräten zum Datenabruf zur Verfügung stehen muss. Die Anzahl und die Art der Endgeräte müssen in Zusammenarbeit mit den Mitarbeitenden erörtert und festgelegt werden, die für die Bedienung der digitalen Akte zuständig sind.

Bei der Anschaffung der Systeme liegt die Vermutung nahe, dass deren Skalierbarkeit hinsichtlich der sich ändernden und wachsenden Anforderungen des Krankenhauses eine entscheidende Rolle spielt. Folglich muss im Vorfeld geplant werden, wie die zukünftige Entwicklung und der Ausbau der Systeme ablaufen soll. Experte B ist ähnlicher Meinung: „Die Technik muss skalierbar sein. Das heißt, einmal hinsichtlich der Datenmengen, aber auch was die Technik anbelangt mit neuen Tablets, schnelleren PCs oder mal von PC, Notebook runter auf ein Tablet“ (Interview B, Pos. 142–145).

Um Schnittstellenprobleme zwischen den Softwaresystemen zu verhindern, kann die Lösung darin bestehen, alle Funktionen in einer einzigen Software abzubilden. Auf

diese Weise ist keine Kommunikation zwischen verschiedenen Softwareprodukten notwendig und Schnittstellenprobleme bleiben aus. Experte J bestätigt diese Aussage:

> *„Also ich habe das Problem der Schnittstellen und deswegen brauche ich für die Grundfunktionalitäten, die ich am Patienten machen muss, also sprich die Arztdokumentation, Pflegedokumentation, Therapeutendokumentation, Leistungsanforderungen, Medikation, möglicherweise auch Terminplanung brauche ich möglichst ein System, in dem diese Dinge komplett abgebildet sind" (Interview J, Pos. 88–93).*

Es besteht Grund zur Annahme, dass die elektronische Patientenakte eine stabile und gute Internet- bzw. WLAN-Verbindung benötigt. Dies impliziert auch, dass Letztere den gesamten Arbeitsbereich abdecken muss. Experte F unterstützt diese Aussage: „WLAN wäre wichtig, dass das funktioniert, also überall im Haus dann" (Interview F, Pos. 99). Ähnliche Aussagen treffen auch die Experten O und H. Daraus kann als Handlungsempfehlung abgeleitet werden, dass bei der Implementierung und beim Betrieb der digitalen Patientenakte darauf geachtet werden muss, dass die Soft- und Hardware an jedem Ort der Station über eine stabile und aktive Internet- bzw. WLAN-Verbindung verfügt.

Jeder Mitarbeitende benötigt einen individuellen, gesicherten und berufsspezifischen Zugang zur elektronischen Patientenakte, um den Zugriff von Dritten zu unterbinden. Die Idee eines individualisierten Berechtigungskonzepts zum Schutz sensibler Daten erwähnte auch Kropp (2016) in seiner Arbeit. Diese Aussage wird durch den Experten O bestätigt: „Auf jeden Fall einen Zugang. Also jede Berufsgruppe, die quasi mit diesem arbeiten soll, muss einen Zugang haben zu diesem System. Sei es über einen Zugang, der direkt über die Station stattfindet mit Passwort, oder individuell" (Interview O, Pos. 104–106). Auch Experte D vertritt eine vergleichbare Ansicht. Hieraus lässt sich für die Praxis die Empfehlung ableiten, dass jeder Mitarbeiter einen Zugang zum System hat und ihm die relevanten benötigten Informationen zur Verfügung gestellt werden.

Es liegt die Vermutung nahe, dass die Umstellung von der Papierakte auf die digitale Akte in einem Schritt die praktikabelste Lösung für die Mitarbeitenden darstellt. Experte B unterstreicht diese Aussage: „Man muss digital werden. Komplett. Da gibt es kein ‚zwischendrin mal' oder ein Ausdrucken" (Interview B, Pos. 32–33). Dies heißt für die Praxis, dass die Umstellung nicht stückweise erfolgen soll, sondern in einem kompletten Durchgang.

Im Bereich der Technik sollten keine Kompromisse bezüglich der Kosten eingegangen werden, da anzunehmen ist, dass diese Einsparungen in der Zukunft zu Schwierigkeiten führen können. Experte B ist ähnlicher Ansicht: „Bitte keine Kompromisse. Also ich würde bei der Technik heute noch weniger Kompromisse eingehen als in der Vergangenheit" (Interview B, Pos. 137–138). Dies gilt auch für die Einführung und den Betrieb der elektronischen Patientenakte.

Die technische Betreuung durch die IT-Abteilung sollte zu jeder Tages- und Nachtzeit bzw. ‚24/7' gewährleistet sein, damit auf Probleme und Fragen zeitnah eingegangen

werden kann. Experte A ist vergleichbarer Meinung: „Es müsste 24 Stunden, 7 Tage die Woche über einen sehr langen Zeitpunkt jemand verfügbar sein, der einem helfen kann, wenn es zu Problemen kommt. Die Handbücher sind sehr dick, sehr unverständlich. Es ist schon eine Riesensache, sowas umzusetzen“ (Interview A, Pos. 47–50). Eine praktische Handlungsempfehlung ist daher, den Mitarbeitenden gerade in der Implementierungsphase eine ‚24/7‘-Betreuung hinsichtlich der elektronischen Patientenakte zur Verfügung zu stellen.

Es ist davon auszugehen, dass das Pflegedokumentationssystem technisch sowohl in das bereits vorhandene Krankenhaussystem als auch in ein cloudbasiertes System integriert werden kann. Experte C ist der Meinung, dass die erste Variante sinnvoll ist (Interview C, Pos. 204–207).

6.8. Gesetzliche Rahmenbedingungen

Die Digitalisierung in der Pflege schreitet immer weiter voran. Dies liegt unter anderem daran, dass sie in den Gesundheitseinrichtungen gesetzlich verpflichtend ist (BMG, 2020b). Das Krankenhauszukunftsgesetz fördert zum großen Teil die Digitalisierung im Gesundheitswesen. Einrichtungen in diesem Bereich haben bis zum 31.12.2024 die Chance, die Digitalisierung umzusetzen. Dabei müssen vor allem die notwendigen digitalen Dienste bereitgestellt werden. Diese werden in § 19 Abs. 1 S. 1 Nr. 2 bis 6 der Krankenhausstrukturfonds-Verordnung dargestellt. Hierunter fällt auch die in Satz 3 genannte elektronische Dokumentation von Pflege- und Behandlungsleistungen. Ab dem 01.01.2025 können Gesundheitseinrichtungen sanktioniert werden, in denen nicht alle notwendigen digitalen Dienste zur Verfügung stehen. Diese Sanktionen finden in Form von Abschlägen bis zu 2 % des Rechnungsbetrages statt. Dies gilt sowohl für vollstationäre als auch für teilstationäre Behandlungsfälle (BMG, 2020b) und stimmt mit der Aussage des Experten J überein:

> *„[…] gesetzliche Verpflichtung, diese Pflegedokumentation zu machen, und meines Wissens ist es sogar auch jetzt schon gefordert, das digital zu machen. Spätestens 2025 wird es Strafen geben, wenn wir Dinge wie die Pflegedokumentation im Rahmen des Krankenhauszukunftsgesetzes nicht digital abgebildet haben“ (Interview J, Pos. 116–120).*

Der Datenschutz spielt eine erhebliche Rolle, wenn es um die elektronische Patientenakte geht, da diese sensiblen Daten enthält (Kropp, 2016). Nach der Analyse scheinen hierbei sowohl die europäische Datenschutzgrundverordnung als auch die Datenschutzrichtlinien bedeutsam zu sein. Dass diese Thematik relevant ist, spiegelt auch die Aussage des Experten N wider: „Die Datenschutzverordnung, die muss natürlich eingehalten werden“ (Interview N, Pos. 98–99). Aber auch die Experten O, L, K, I, H, F, E, D, C, B und A teilen diese Ansicht.

Es liegt nahe, dass es durch die Einhaltung datenschutzrechtlicher Anforderungen oftmals zu Problemen im täglichen Pflegebetrieb kommt. Dies sieht auch Experte K ähnlich: „[…] das uns auch ganz furchtbar behindert oft, weil uns der Datenschutz an manchen Stellen so einschränkt, dass man fast Angst haben könnte, dass wir den

Patienten nicht mehr behandeln können“ (Interview K, Pos. 110–112). Auch Experte L wird dadurch und infolge der daraus resultierenden Einschränkungen bei der täglichen Arbeit behindert: „[…] das macht das Leben im Krankenhaus sehr schwer. Und ich glaube bei der elektronischen Akte, dass man die implementiert, wenn man diese Datenschutzbestimmungen einhalten muss. Da wird man sehr viele Schwierigkeiten haben, um an die Akte dranzukommen“ (Interview L, Pos. 77–80).

Auch das Sozialgesetzbuch (SGB) Fünftes Buch (V) forderte die Einführung sowie die Entwicklung der Digitalisierung in Gesundheitseinrichtungen (Bundesministeriums der Justiz und für Verbraucherschutz [BMJV] & Bundesamts für Justiz [BfJ], 1988). Dies wird auch durch die Aussage des Experten N bestätigt: „Ansonsten ist ja die Digitalisierung, sage ich mal, auch im SGB V verankert, also dass das vorangetrieben werden sollte“ (Interview N, Pos. 103–105).

Für die Digitalisierung der Dokumentation ist ebenfalls den Vorgaben des Gemeinsamen Bundesausschusses (G-BA) (Höhl, 2020) Folge zu leisten. Des Weiteren bleibt zu vermuten, dass auch die Prüfungen durch den Medizinischen Dienst der Krankenversicherung (MDK) hinsichtlich der Vorgaben für die Digitalisierung einzuhalten sind. Dies wird auch durch den Experten I untermauert: „[…] Anforderungen vom GBA, wie so eine Dokumentation auszusehen hat“ (Interview I, Pos. 147–148).

Die Daten in der elektronischen Patientenakte unterliegen je nach Art des Datensatzes und der gesetzlichen Vorgabe einer Aufbewahrungsfrist, die in der Berufsordnung der Ärzte grundsätzlich für zehn Jahre vorgeschrieben wird, sofern sie durch keine andere gesetzliche Regel längerfristig erforderlich ist (Bayerische Landesärztekammer [BLÄK], o.J.). Solche Aufbewahrungsfristen werden beispielsweise in der Röntgenverordnung (30 Jahre) (Bundesministeriums der Justiz und für Verbraucherschutz [BMJV] & juris GmbH, 1987) oder im Transfusionsgesetz (15–30 Jahre) (Bundesministeriums der Justiz und für Verbraucherschutz [BMJV] & Bundesamts für Justiz [BfJ], 1998) festgelegt. Trotz der zehnjährigen Frist in der Berufsordnung der Ärzte empfiehlt die Bayerische Landesärztekammer, die Dokumente 30 Jahre lang aufzubewahren. Dies wird damit begründet, dass die eventuell haftungsrechtlichen Ansprüche in Einzelfällen bis zu 30 Jahre rückwirkend geltend gemacht werden können (BLÄK, o.J.). Auch Experte I unterstützt diese Aussage im Interview: „Aufbewahrungsfristen, Archivfristen irgendwo berücksichtigen, je nach Art der Daten zwischen zehn Jahre und 30 Jahre, je nach Information“ (Interview I, Pos. 150–151).

Des Weiteren ist zu vermuten, dass eine Vielzahl von anderen Gesetzen eine Rolle spielen. Dazu zählen im Bereich der IT-Sicherheit das IT-Sicherheitsgesetz und der UP KRITIS für Krankenhäuser (Interview B, Pos. 174–178; Interview I, Pos. 408). Zudem sind Security by Design sowie Löschvorgaben zu beachten (Interview B, Pos. 164–165). Für die elektronische Patientenakte und die Digitalisierung in der Pflege sind ebenfalls das Medizinproduktegesetz und die neue Medical Device Regulation relevant (Interview B, Pos. 169–170). Auch durch das Pflegeberufegesetz werden Fachkräfte dazu verpflichtet, im Rahmen ihrer Vorbehaltsaufgaben den Pflegeprozess zu dokumentieren (Interview E, Pos. 127–129).

Es gilt zu beachten, dass auch länderspezifische Gesetzgebungen im Bereich der Digitalisierung in der Pflege einzuhalten sind. So wird im Bayerischen Krankenhausgesetz in Artikel 27 vorgegeben, dass die Datenhaltung am Standort zu erfolgen hat (Bayerische Staatskanzlei [BStK], 2007). Dies führt Experte I weiter aus:

> *„[…] Spezialgesetze der Länder berücksichtigen, zum Beispiel in Bayern gibt es den Artikel 27 des Bayerischen Krankenhausgesetzes. Der würde zum Beispiel vorschreiben, dass eine Datenhaltung am Standort erfolgen muss. Das heißt, Lösungen, die da auf Cloudanbieter setzen, die könnte man Stand jetzt nicht umsetzen, weil es aufgrund dieses Spezialgesetzes des bayerischen Datenschutzbeauftragten oder des Bayerischen Krankenhausgesetzes nicht möglich wäre“ (Interview I, Pos. 156–162).*

Im Bürgerlichen Gesetzbuch werden die behandelnden Einrichtungen in § 630f dazu aufgefordert, ihre Behandlungen zu dokumentieren (BMJV & BfJ, 2021). Dies erwähnt auch Experte E in der Befragung: „Also § 630f BGB verpflichtet ja uns auch zum Zweck der Dokumentation, dass wir in unmittelbaren zeitlichen Zusammenhang die Behandlung von den Patienten auch dokumentieren, das heißt, entweder in Papierform oder elektronisch“ (Interview E, Pos. 24–27).

Die Vermutung liegt nahe, dass sich auch die externen Kooperationspartner und Dienstleister an dieselben rechtlichen Anforderungen halten müssen wie das Krankenhaus selbst. Diese Aussage bestätigt Experte A: „Also da kommen ja ganz viele Aspekte mit rein, die sektorenübergreifend nicht nur in der Klinik, sondern auch bei den externen Versorgern zum Tragen kommen“ (Interview A, Pos. 80–82). Daraus kann für die Praxis abgeleitet werden, dass die rechtlichen Vorgaben mit den externen Kooperationspartnern und Dienstleistern besprochen und entsprechend dokumentiert werden müssen.

6.9. Beteiligte Akteure

Es ist zu vermuten, dass ein entscheidender Faktor für ein erfolgreiches Implementierungsvorhaben darin besteht, über ein Projektmanagement zu verfügen, das eine koordinierte Projektorganisation durchführt. Dies sieht Experte K ähnlich: „[…] ordentliche Projektorganisation, die das ganze koordiniert“ (Interview K, Pos. 77). Auch Experte J vertritt diese Ansicht. Dazu sollte eine Projektleitung bestimmt werden, die die Koordinierung und Steuerung der Prozesse übernimmt. Experte E ist ebenfalls dieser Meinung: „[…], dass man jemanden hat, der als Projektleiter dient für das gesamte Haus“ (Interview E, Pos. 82–83). Daraus lässt sich in Bezug auf die Praxis schließen, dass für eine Implementierung einer digitalen Akte eine Projektleitung beauftragt werden muss. Diese kann bei Bedarf durch ein Projektteam erweitert werden. Die Aufgabe des Projektleiters oder des Projektteams sollte darin liegen, vor, während und nach der Einführung der elektronischen Patientenakte alle Planungsaufgaben (z.B. die Anforderungsanalyse, Finanzen, Einweisungen) zu übernehmen und zu koordinieren.

Es ist naheliegend, dass alle Personen am Implementierungsprozess beteiligt werden sollten, die zukünftig an oder mit der elektronischen Patientenakte arbeiten müssen. Diese Meinung vertritt auch Experte E: „[…] wenn man von der gesamten Digitalisierung spricht, dann müssten alle an einem Strang ziehen“ (Interview E, Pos. 100–101). Die Experten O, G, F, E und A teilen diese Haltung ebenfalls.

Demgegenüber gibt es aber auch die Ansicht, dass nur die für den Prozess relevanten Mitarbeitenden sowie Fachabteilungen an der Implementierung beteiligt werden sollen. Diese Ansicht vertritt auch Experte J: „[…] müssen halt die relevanten Leute dabei sein, wobei meine Erfahrung zeigt, dass es sinnvoll ist, kein Riesenteam zu machen. Je größer das Team wird, desto mehr verwässert es und desto länger braucht man dafür“ (Interview J, Pos. 109–112). Die Experten N, M, L, K und D sind vergleichbarer Meinung.

Für die Implementierung selbst liegt es nahe, ein multiprofessionelles Projektteam zu bilden. Dies sieht auch Experte I ähnlich:

> *„[…] multiprofessionelles Team zusammenstellen aus verschiedenen Bereichen, sowohl aus Bereich Pflege, Medizin, aber auch Verwaltung. Das heißt, Abrechnung, IT-Abteilung, um wirklich am Anfang alle Bedarfe zu dokumentieren, zusammenzubringen und eben ein großes Projektteam zu haben, damit eben alle Aspekte berücksichtigt sind“ (Interview I, Pos. 94–98).*

Die folgenden Berufsgruppen könnten an der Implementierung der elektronischen Patientenakte beteiligt sein:

- Berufsgruppe der Pflege
    - Gesamtes Pflegefachpersonal (Interview H, Pos. 55)
- Berufsgruppe der Therapeuten
    - Logopädie, Physio- und Ergotherapie (Interview O, Pos. 92–93)
- Berufsgruppe der Mediziner
    - Alle ärztlichen Qualifikationen (Interview E, Pos. 103)
- Informationstechnologie/EDV
    - Softwareentwickler (Interview K, Pos. 71)
    - Systemtechniker (Interview K, Pos. 71)
    - Anwendungs- und Schnittstellenbetreuer (Interview K, Pos. 71; Interview C, Pos. 150–151)
    - Abteilung IT/EDV (Interview J, Pos. 108)
- Führungskräfte
    - Stationsleitungen, Pflegedienstleitungen und Direktion (Interview C, Pos. 157–158)
- Verwaltung

    - Qualitätsmanagement (Interview N, Pos. 73)
    - Risikomanagement (Interview N, Pos. 73)
    - Kodierung (Interview J, Pos. 108–109)
    - Abrechnung (Interview G, Pos. 68)
    - Logistik und Lager (Interview B, Pos. 109–112)
- Stabsstelle Pflegewissenschaft (Interview O, Pos. 90)
    - Pflegewissenschaftler
- Fallmanagement
    - Sozialarbeiter und Fallmanager (Interview L, Pos. 67)
- Externe Dienstleister
    - Softwareunternehmen (Interview D, Pos. 82–83)

Die Kooperationspartner und am Behandlungsprozess beteiligten Akteure sollten von Anfang an in die Implementierungsplanung einbezogen werden. Damit können auch die zukünftige Netzwerkarbeit und der Informationsaustausch gewährleistet werden (Dörries et al., 2017). Experte F bringt ein Beispiel dafür, welche Vorteile die Vernetzung mit der Apotheke mit sich bringt: „[…], die die Medikamente bestellen, dass so Prozesse dann angepasst werden, dass sie dann auch in der Apotheke gestellt wird, was das ja auch nochmal sicherer macht“ (Interview F, Pos. 105–107). Des Weiteren können mit den weiteren Akteuren Möglichkeiten der Prozessoptimierung besprochen werden. Folglich kann für die Praxis die Handlungsempfehlung gegeben werden, die Kooperationspartner in den Digitalisierungsprozess zu integrieren und so die Vernetzung sowie den Austausch untereinander zu verbessern. Darüber hinaus sollten mit den Kooperationspartnern mögliche Prozessverbesserungen besprochen werden. Ein Beispiel für die Praxis wäre hier die Vernetzung der digitalen Medikationsliste mit der Klinikapotheke. Medikamente könnten mithilfe von Kommissionierungsrobotern in der Apotheke automatisch gestellt und anschließend auf die Station geliefert werden. Durch den Wegfall des Medikamentenstellens können die Arbeit der Pflegenden auf der Station erleichtert und Kosten langfristig eingespart werden. Zudem ist durch die Automatisierung eine geringere Fehlerquote zu erwarten.

6.10. Benutzereinweisung/Schulungen

Es ist anzunehmen, dass vor der Implementierung ein Testlauf mit Versuchspersonen stattfinden sollte. Diese Ansicht vertritt auch Experte O: „[…] Testpersonen oder erstmal Test ablaufen“ (Interview O, Pos. 75–76). Daraus lässt sich schließen, dass die Anforderungen und die Benutzerfreundlichkeit des Systems durch den vorab stattfindenden Test nochmal überprüft und eventuelle Schwachstellen aufgedeckt werden können.

Experte H spricht sich für Schulungen im Umgang mit der elektronischen Patientenakte aus: „[…], quasi jeder eingearbeitet werden kann in den Umgang mit der Akte“ (Interview H, Pos. 50–51). Für die Praxis lässt sich ableiten, dass jeder

Mitarbeitende im Umgang mit dem elektronischen Dokumentationssystem geschult werden muss.

Die Analyse hat ergeben, dass für eine ordnungsgemäße, individualisierte und ausreichende Schulung ein Schulungsverantwortlicher beauftragt werden muss. Es liegt nahe, dass er die Aufgabe hat, den Mitarbeitenden durch Schulungen und Informationen das Dokumentationssystem näherzubringen. Diese Schulungen sollten in unterschiedlichen Formen durchgeführt werden, um so die Bedürfnisse und Fähigkeiten der einzelnen Mitarbeitenden anzusprechen. Diese Meinung wird durch den Experten I unterstützt: „[…] Schulungsverantwortlichen, einen Produktverantwortlichen oder wie auch immer man diese Rolle, Funktion im Haus bezeichnen möchte, dann implementiert wird, der auch wirklich die Leute in unterschiedlichen Schulungsformaten anspricht“ (Interview I, Pos. 176–178).

Es ist anzunehmen, dass die Mitarbeitenden bereits bei der Implementierung mit dem System arbeiten müssen. Daher ist es ratsam, die Schulung schon im Voraus anzubieten. Dadurch kann die Einführung schneller ablaufen und die Akzeptanz der Mitarbeitenden gegenüber der elektronischen Patientenakte steigt. Diesen Standpunkt vertritt auch Experte I: „[…] eine Benutzereinweisung nicht erst stattfindet, wenn sozusagen das fertige System in Betrieb genommen wird, sondern dass eben auch schon vorher da entsprechende Schulungen und Informationen stattfinden“ (Interview I, Pos. 172–175). Auch die Experten O, N und C sind ähnlicher Meinung. Diese vorab durchgeführten Schulungen sind ein wichtiges Instrument zur Einbindung der Mitarbeitenden in den Implementierungsprozess. Hierbei können diese das System kennenlernen und eventuelle Verbesserungen bereits von Anfang an einbringen. Dieser Ansicht ist auch Experte C: „[…] wertvoll wäre es, wenn sich die Mitarbeiter hier insofern einbinden lassen und auch mitarbeiten und diesen Prozessen mitgestalten“ (Interview C, Pos. 126–128).

Die Mitarbeitenden sollten eine Grundschulung erhalten, um ein Basisverständnis im Bereich der digitalen Patientenakte zu erlangen. Diese Meinung vertritt ebenfalls Experte K: „Es ist ganz zwingend erforderlich, dass die Leute erstmal, wenn sie zum Beispiel neu ins Haus kommen, erstmal eine Grundschulung kriegen“ (Interview K, Pos. 84–85). Dieser Ansicht schließt sich Experte J an.

Des Weiteren sollten Mitarbeitenden regelmäßig Wiederholungskurse zur Wissensauffrischung angeboten werden. Eine ähnliche Ansicht hat Experte K: „[…] die Möglichkeit haben nach einiger Zeit, in der sie da arbeiten, Sachen wieder auffrischen zu können“ (Interview K, Pos. 86–87).

Es liegt nahe, dass neben den Grund- und Wiederholungskursen bei einem Update oder einer Funktionserweiterung entsprechende Folgeschulungen angeboten werden sollten. Experte J sagt hierzu: „Schulungen bei Einführung eines neuen Programmpakets oder bei relevanten Änderungen im Rahmen eines Upgrades“ (Interview J, Pos. 249–250). Vergleichbarer Meinung ist auch Experte K.

Es ist zu vermuten, dass die Akzeptanz und das Interesse der Mitarbeitenden durch eine schnelle und einfach durchgeführte Schulung gewonnen werden können. Dies sieht Experte L ähnlich: „Einfach und schnell“ (Interview L, Pos. 60).

Für die Schulungen sollte ein Mix aus verschiedenen methodisch-didaktischen Strategien gewählt werden, um jeden Mitarbeitenden und jede Berufsgruppe individuell ansprechen zu können (Studiengemeinschaft Werner Kamprath Darmstadt GmbH [SGD], o.J.). Dies sieht auch Experte I so: „[…] Methodenmix darauf an, aber dass wirklich da strukturiert auch geschult wird und dieses Angebot auch kontinuierlich zur Verfügung steht“ (Interview I, Pos. 180–182). Bei den Schulungen gilt es zu beachten, dass diese in kleinen Gruppen und berufsspezifisch durchgeführt werden, damit die individuellen Bedürfnisse berücksichtigt werden können. Diese Ansicht teilt Experte G ebenfalls: „Man sollte in kleineren Gruppen schulen, damit man auf jeden Einzelnen richtig eingehen kann und das ihm zeigen kann“ (Interview G, Pos. 87–89). Auch Experte M vertritt eine ähnliche Meinung.

Es ist naheliegend, die Vorschulungen und alle weiteren Schulungen mithilfe von E-Learning zu bewältigen. Vergleichbarer Ansicht ist Experte C:

> *„Da sehe ich zwei Faktoren. Zum einen, wie gesagt, im Voraus das Grundverständnis der Pflege zu klären, dann im direkten Handling eventuell im Voraus schon E-Learning-Angebote zu machen, in denen schrittweise die einzelnen Bedienelemente dargestellt werden, wo man auch nochmal nachschauen kann, wo man sich nochmal draufklinken kann“ (Interview C, Pos. 114-118).*

Das E-Learning kann mithilfe von Erfolgskontrollen evaluiert werden. Dies sieht auch Experte B so: „[…] in jedem Fall E-Learning. Ich würde aber auch nicht davor zurückschrecken, ein paar Fragen zu stellen im Sinne von Lernerfolgskontrollen“ (Interview B, Pos. 124–126).

Es ist anzunehmen, dass auch die Verwendung von Handbüchern und Nachschlagewerken für die Mitarbeitenden eine Hilfestellung in Problemsituationen darstellen kann. Diese Ansicht vertritt auch Experte D: „[…] Nachschlagewerk, wo ich darauf zugreifen kann zu jeder Zeit, zur Tages- und Nachtzeit, um zu gucken, ob die Frage, die mir jetzt gerade unterkommt, möglicherweise schonmal ein anderer hatte und dann da nachschlage in einer Art internem wachsendem Antwortkatalog“ (Interview D, Pos. 260–263). Auch Experte I sieht Handbücher als eine Möglichkeit zur Problemlösung.

6.11. Key-User

Die Analyse zeigte, dass es bei der Implementierung immer wieder zu Problemen und Fragen kommen kann. Es liegt nahe, dass den Mitarbeitenden auf den Stationen entsprechend geschulte Key-User zur Verfügung stehen sollten. Diese Ansicht vertritt ebenfalls Experte M:

> *„Wichtig ist aber, wenn sowas implementiert wird, dass es auch längerfristig begleitet wird und zum Beispiel auch nicht irgendwann wieder aufhört, denn es gibt einen hohen Durchlauf zum Beispiel in der Pflege. Es kommen viele neue Mitarbeiter. Und wenn die immer nur wieder von anderen Mitarbeitern eingewiesen*

> *werden, nach einer bestimmten Zeit schleichen sich da vielleicht auch Anwenderfehler ein oder vielleicht Nachlässigkeiten. Die werden ja dann gleich an diese neuen Mitarbeiter eingegeben“ (Interview M, Pos. 63–70).*

Auch die Experten K, N, J, I, G, D und C kamen zu einem vergleichbaren Schluss.

Es lässt sich vermuten, dass den Key-Usern entsprechende zeitliche Ressourcen zur Verfügung stehen müssen, damit diese ihre Kollegen begleiten können. Dies sieht auch Experte E ähnlich: „[…], dass die Key User auf den Stationen vorhanden sind, die auch genügend zeitliche Ressourcen zur Verfügung bekommen, um das Ganze zu begleiten“ (Interview E, Pos. 84–86).

Es sollten daneben auch ausreichende personelle Ressourcen geschaffen werden, um die Implementierung zu begleiten. Dazu ist es ratsam, den Mitarbeitenden auf Station über einen Zeitraum von mindestens sechs Monaten ein bis zwei zu Key-Usern ausgebildete Kollegen ausschließlich zur Begleitung der elektronischen Patientenakte zur Verfügung zu stellen. Um diese Hilfestellung gewährleisten zu können, ist es naheliegend, dass die Arbeitszeit der Key-User in diesem Zeitraum zwischen 50 % und 100 % einer Vollzeitstelle betragen sollte. Diese Ansicht vertritt auch Experte E:

> *„Begleitung auf den Stationen muss eigentlich durch eine Person oder zwei Personen kontinuierlich durchgeführt werden, dass die zu 0,5 VK oder eine Vollkraft, dass sie bei der Einführung für die, ich sage mal, sechs Monate auf den Stationen sind, die eigentlich nichts anderes machen als die Begleitung für die Einführung, und dass sie den Kollegen immer zur Verfügung stehen, wenn sie Fragen haben“ (Interview E, Pos. 88–93).*

Auch die Experten C und D geben an, dass eine entsprechende Anzahl von Key-Usern verfügbar sein muss.

Es ist davon auszugehen, dass Mitarbeitende dahingehend sensibilisiert werden müssen, dass die Key-User keine Kontroll- oder Prüfungsfunktion haben, sondern ihnen kollegial zur Seite stehen, wenn es zu Problemen und Fragen hinsichtlich der digitalen Akte kommt. Zudem zeigte die Analyse, dass diese kollegiale Zusammenarbeit eine Chance für die Weiterentwicklung des Systems bedeutet. Diese Aussage wird durch den Experten C unterstützt: „[…] nicht als negativer letztendlich bei den Mitarbeiterinnen und Kollegen in den Fokus gerät, dass diese Key User jetzt zu Prüfern und zu Kontrolleuren werden, sondern eher im positiven Sinne“ (Interview C, Pos. 191–194).

Eine weitere Möglichkeit neben dem Key-User-Konzept stellen vermutlich neutrale Spezialisten dar. Es ist davon auszugehen, dass diese auf den Stationen eingesetzt werden, um die Mitarbeitenden zu unterstützen. Daraus kann abgeleitet werden, dass das selbstständige Lernen durch kollegiale Hilfe auf Station unterstützt werden kann. Diese Ansicht vertritt auch Experte B: „Key-User-Konzept, was man früher gemacht hat, bin ich kein großer Anhänger mehr. Also ich selber würde sagen, es gibt dann im Haus Neutralspezialisten, die die Leute unterstützen, aber man muss dieses eigene Lernen viel mehr aktivieren“ (Interview B, Pos. 130–132).

6.12. Implementierungsdauer

Es sollte in der Planungsphase eine Analyse des benötigten Zeitumfangs für das Implementierungsprojekt durchgeführt werden. Dieser Meinung ist auch Experte F: „[…] würde ich mir die Prozesse vorher angucken, um was es genau geht, digital, was genau eingeführt werden soll. Das schon mal im Vorfeld zu planen. Dann hier auch die Prozesse genau zu analysieren“ (Interview F, Pos. 122–124). Daraus lässt sich für die Praxis ableiten, dass vor der eigentlichen Implementierung eine Prozessanalyse vorgenommen werden sollte. So kann unter anderem die benötige Dauer eingeschätzt werden.

Die analysierten Interviews zeigen bei der Frage nach der Dauer der Implementierung unterschiedliche Einschätzungen. Die kürzeste Zeit für die Implementierung wird mit drei Monaten (Interview O, Pos. 123–124) und die längste mit drei Jahren (Interview N, Pos. 75–77) angegeben. Die Mehrheit der Experten vertritt die Ansicht, dass eine erfolgreiche Implementierung einer elektronischen Patientenakte zwischen einem und zwei Jahren in Anspruch nimmt: „[…], bis man alle Mitarbeiter abgeholt hat, bis man es wirklich implementiert hat, dann kann es schon ein Jahr, zwei Jahre dauern, mindestens“ (Interview E, Pos. 143–145).

Nach Expertenmeinung sind jedoch vermutlich auch Implementierungsdauern zwischen sechs und zwölf Monaten möglich. So gibt Experte B in der Befragung Folgendes an: „[…], zwischen sechs und zwölf Monaten sollte man solche Module dann entsprechend umsetzen. Im ganzen KIS müsste man es neu betrachten, aber wie gesagt, aus meiner Erfahrung, sechs Monate ist ein guter Sprint“ (Interview B, Pos. 186–189). Er betont hierbei, dass eine Implementierungsdauer von unter sechs Monaten falsch veranschlagt wurde: „Persönlich sage ich mal, alles unter sechs Monaten ist irgendwie falsch aufgesetzt oder in die Tasche gelogen“ (Interview B, Pos. 183–184). Eine Dauer von über 12 Monaten birgt die Gefahr, dass sich die Mitarbeitenden langweilen: „alles ab zwölf Monate, da kommt meines Erachtens ein bisschen diese Langeweile auf“ (Interview B, Pos. 190–191).

Es besteht aber möglicherweise auch Grund zur Annahme, dass nur ein ungefährer Zeitraum als Einschätzung vorliegen kann. Hierbei wurden Implementierungsdauern von einigen Monaten (Interview L, Pos. 86) bis zu mehreren Jahren genannt (Interview K, Pos. 128–129).

Es ist davon auszugehen, dass ein so komplexes und großes Dokumentationssystem laufend aktualisiert sowie gewartet werden muss – und dies über den gesamten Produktlebenszyklus andauert. Diese Ansicht vertritt auch Experte D: „Wenn man unsere Größenordnung, unser Haus anschaut, wo ja nahezu alle Fachabteilungen oder alle Fachbereiche einer Klinik vertreten sind plus ein großes Labor plus Psychiatrie plus, plus, plus, und alle Berufsgruppen. Jahre. Eigentlich ununterbrochen“ (Interview D, Pos. 145–148).

Die Vorschulung der Mitarbeitenden könnte bei der Implementierung einen wesentlichen Zeitfaktor darstellen. Sie sollte der Analyse nach bereits ein halbes Jahr vor der Implementierung begonnen werden. Diese Aussage unterstützt Experte F: „[…] die Schulung der Mitarbeiter. Ich würde das schon auf alle Fälle ein halbes Jahr für im

Vorfeld und dann für die Begleitung auch nochmal“ (Interview F, Pos. 124–126). Auch die Experten A und G sind der Ansicht, dass die Vorschulung viel Zeit in Anspruch nimmt. Es ist zu empfehlen, die vorzeitige Schulung der Mitarbeitenden auf das elektronische Dokumentationssystem ein halbes Jahr vor der eigentlichen Implementierung durchzuführen.

Neben den Vorschulungen müssen die Mitarbeitenden auch während der Implementierung und danach umfassend betreut und begleitet werden. Dies sieht Experte F ähnlich: „[…] danach halt auch begleitet werden soll und nicht, dass dann kein Ansprechpartner mehr da ist“ (Interview F, Pos. 127–128).

Ein mit vorzeitigen Schulungen höchstwahrscheinlich einhergehender Vorteil besteht darin, dass die Implementierung anschließend schneller voranschreitet. Diese Aussage unterstreicht Experte C: „Meine Hoffnung ist, dass wir mit Vorabschulungen und E-Learning relativ straight durchs ganze Haus zeitgleich beginnen können“ (Interview C, Pos. 214–216).

6.13. Datenverfügbarkeit

Krankenhäuser sind 24 Stunden am Tag, sieben Tage die Woche und 365 Tage im Jahr in Betrieb (Klinikum Ingolstadt GmbH, o.J.a). Damit ihre Mitarbeitenden optimal mit der elektronischen Patientenakte arbeiten und darauf zugreifen können, ist es naheliegend, dass die Datenverfügbarkeit rund um die Uhr zu gewährleisten ist. Dies verdeutlicht auch Experte I im Interview: „[…] geht ja immer von der Hochverfügbarkeit dieser Systeme aus, also am besten 24/7 stehen diese Daten und Informationen zur Verfügung ohne Systemunterbrechungen“ (Interview I, Pos. 188–190). Auch die Experten N, K, J, G, F, D und B sind ähnlicher Meinung.

Vermutlich kann eine durchgehende ‚24/7‘-Verfügbarkeit der elektronischen Patientenakte nicht gewährleistet werden. Dies liegt daran, dass technische Systeme ausfallen können oder zu Wartungsarbeiten abgeschaltet werden müssen. Experte J unterstreicht diese Aussage: „keine hundertprozentige Verfügbarkeit“ (Interview J, Pos. 134). Für die Praxis heißt dies, dass die Mitarbeitenden dafür sensibilisiert werden müssen, dass die elektronische Patientenakte nicht immer zur Verfügung steht. Hier gilt es, entsprechende Redundanzen und Ausfallkonzepte zu implementieren.

Es ist anzunehmen, dass jeder der am Erkrankten Leistungen erbracht hat die Möglichkeit haben, diese auch dokumentieren zu können. Experte N unterstützt diese Aussage: „Also erstens einmal muss gewährleistet sein, dass jeder dokumentieren kann, und es muss gewährleistet sein, dass jeder Daten einsehen kann, der halt die Berechtigung dazu hat“ (Interview N, Pos. 127–130).

Auch die örtliche Verfügbarkeit der elektronischen Patientenakte spielt eine relevante Rolle. Da viele Mitarbeitende auch in anderen Bereichen im Krankenhaus tätig sind, müssen sie von jedem Ort in der Klinik mithilfe eines unterstützenden Endgeräts auf die Daten zugreifen können (Kropp, 2016). Dies bestätigt Experte E ebenfalls: „Und die Verfügbarkeit muss an jedem Ort und jedem zugänglich sein“ (Interview E, Pos. 157–158). Auch die Experten E, C, F, L und N gelangen zu ähnlichen Ansichten. Für

die Praxis lässt sich daraus ableiten, dass den Mitarbeitenden an jedem patientennahen Arbeitsplatz und in jedem Arzt- bzw. Stationszimmer ein elektronisches Endgerät mit Anbindung an die elektronische Patientenakte zur Verfügung stehen muss, um die Dokumentationsmöglichkeit und den berechtigten Datenzugriff zu gewährleisten.

Um die datenschutzrechtlichen Anforderungen einhalten zu können, bedarf es eines Rollen- und Berechtigungskonzeptes für den Zugang auf die Patientendaten. Diesen darf nur derjenige haben, der auch am betreffenden Erkrankten arbeitet. Das Ziel dieses Konzeptes sollte es sein, dass Mitarbeitende nur berufsspezifisch und stations- bzw. abteilungsspezifisch auf die relevanten und auch nur auf die benötigten Patientendaten zugreifen können. Auch Kropp (2016) sieht in seiner Arbeit ein Berechtigungskonzept als sinnvoll an, um nur auf die Daten zugreifen zu können, die das spezifische Zugriffsrecht auch gewährt. Dieser Ansicht ist auch Experte E: „[…] datenschutzrechtlich gesichert sein, dass ich Zugriff nur auf meine Patienten habe und nicht, dass ich dann quer durch das Haus mir die Patientenakte anschauen kann. Das heißt, wirklich die Daten, die ich benötige, müssten zur Verfügung gestellt werden“ (Interview E, Pos. 180–183). Auch die Experten M, B, A, L, K, J und F treffen ähnliche Aussagen. Daraus lässt sich für die Praxis ableiten, dass bei der Implementierung einer elektronischen Patientenakte ein berufsgruppenspezifisches und abteilungs- bzw. stationsspezifisches Rollen- und Berechtigungskonzept zur Verfügung steht, um die Patientendaten vor Dritten zu schützen, die keine Berechtigung oder Notwendigkeit haben, auf die Daten zuzugreifen.

Bei der Vergabe von Rollen und Berechtigungen kommt die Frage auf, welche Daten die Mitarbeitenden am Erkrankten brauchen, um dessen ganzheitliche Pflege gewährleisten zu können. Diese Frage wurde von den Experten unterschiedlich beantwortet. Die Kategorien zeigen an, welche Datensätze Mitarbeitende am Erkrankten der Expertenmeinung nach in der täglichen Arbeit vermutlich zur Verfügung stehen müssen. Die Datenkategorien können Abbildung 6.1 entnommen werden. Es ist für die Praxis ratsam, den Mitarbeitenden die in der o.g. Abbildung aufgeführten Datenkategorien im Rahmen ihres berufsspezifischen und abteilungsspezifischen Rollen- und Berechtigungskonzeptes für ihre tägliche Arbeit am Erkrankten bereitzustellen.

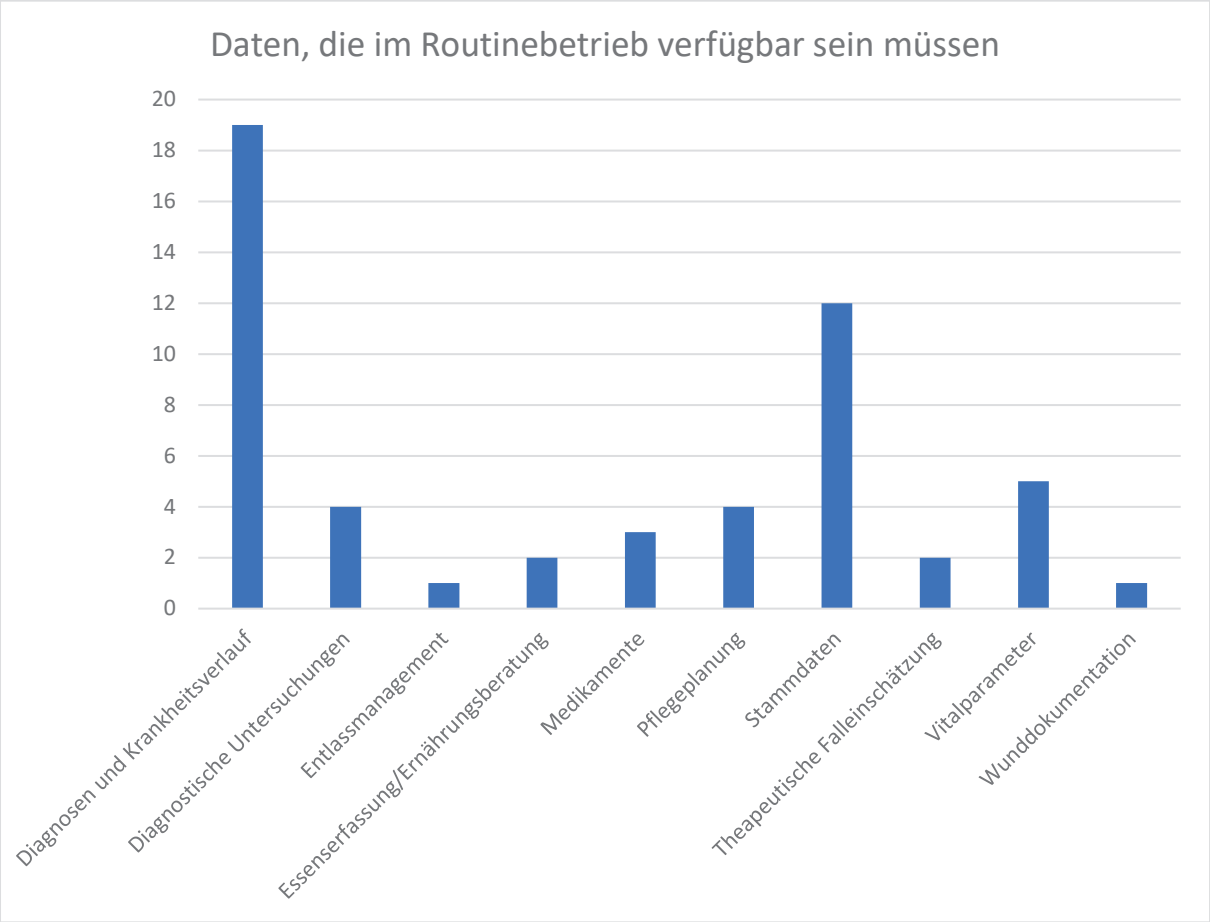


Abbildung 6.1: Daten für den Routinebetrieb

Es ist grundsätzlich davon auszugehen, dass den Mitarbeitenden alle für die Behandlung und Pflege des Erkrankten benötigten Daten zu Verfügung stehen müssen. Nur so kann davon ausgegangen werden, dass eine ganzheitliche Patientenbetreuung garantiert werden kann. Diese Ansicht vertritt auch Experte N: „[…] auf alle Fälle die aktuellen Daten, also die im Moment notwendig sind zur Betreuung des Patienten, auf alle Fälle zur Verfügung sein“ (Interview N, Pos. 151–153). Auch die Experten D und E sind der Meinung, dass den Mitarbeitenden alle für die Behandlung und Diagnostik notwendigen Daten vorliegen müssen.

Die Vermutung liegt nahe, dass der Berufsgruppe der Pflegenden, der Ärzte und der Therapeuten nach Expertenmeinung die Gesamtheit aller Daten des Erkrankten zur Verfügung stehen sollte – und das ohne Einschränkung. Diesen Standpunkt teilt auch Experte J: „[…] gibt es für mich da keine Einschränkung und wir haben es auch so geregelt, dass Ärzte und Pflegende und Therapeuten selbstverständlich Zugriff auf die Patientendaten haben“ (Interview J, Pos. 185–188). Experte L vertritt ebenfalls diese Ansicht.

Darüber hinaus ist davon auszugehen, dass die Pflegenden, die Ärzte und die Therapeuten ebenfalls Zugriff auf die in Voraufenthalten erhobenen Daten des Erkrankten bekommen sollten. Dies hat bei wiederkehrenden Erkrankten höchstwahrscheinlich den Vorteil, dass daraus zusätzliche Informationen erhalten

werden können, um so eine ganzheitliche Betrachtung des Erkrankten zu ermöglichen. Diese Meinung teilt auch Experte N:

> *„Und aber auch, wenn es notwendig ist – da kann man vielleicht irgendwelche Sicherheiten einbauen – auch ältere Daten. Also man kann ja zum Beispiel welche aus Voraufenthalten, irgendwelche Informationen dann auch nutzen. Das, denke ich, ist einer der größten Vorteile, gerade bei oft wiederkehrenden Patienten“ (Interview N, Pos. 153–157).*

Dennoch sollte überlegt werden, die Daten aus den Voraufenthalten, die den Pflegenden, den Ärzten und den Therapeuten zur Verfügung gestellt werden sollen, zeitlich zu begrenzen. Wenn sie älter als sechs Monate sind, ist davon auszugehen, dass Pflegende hierauf keinen Zugriff mehr haben müssen – außer es handelt sich um chronische Erkrankungen. Ärzte sollten vermutlich Zugang zu Daten aus Voraufenthalten der letzten zwei Jahre erhalten. Diese Ansicht vertritt auch Experte B: „[…] älter ist als sechs Monate oder nicht unter chronisches Leiden läuft, muss die Pflege jetzt nicht sehen. Der Arzt vielleicht die letzten zwei Jahre“ (Interview B, Pos. 228–230).

Für die Arbeit mit den digitalen Daten ist es unabdingbar, dass diese möglichst übersichtlich und unkompliziert dargestellt werden sowie Freiräume für die individualisierte Gestaltung gelassen werden. Dies bedeutet möglicherweise, dass auf nicht benötigte Datenfelder verzichtet wird. Dies wird durch den Experten C im Interview bestätigt: „[…] eine möglichst individualisierte Ansicht vorhanden ist, und keine Platzhalter, die unnötig irgendwie den Raum voll machen von dieser Patientenakte, sondern individuell die Informationen, die erfasst werden, möglichst alle, in einer übersichtlichen Form darzustellen“ (Interview C, Pos. 358–361). Dadurch kann die Arbeit mit der Patientenakte erleichtert und die Akzeptanz der Mitarbeitenden ihr gegenüber gesteigert werden. Des Weiteren ist davon auszugehen, dass durch die Übersichtlichkeit dokumentierte Auffälligkeiten schneller erkannt werden.

Es ist davon auszugehen, dass Mitarbeitende in Notfallsituationen (z.B. bei einem Strom- oder IT-Ausfall) weiterhin wichtige Daten für die Versorgung der Erkrankten benötigen, wenn die elektronische Patientenakte nicht zur Verfügung steht. Die Experten wurden gefragt, welches Mindestmaß an Patientendaten Pflegende am Bett benötigen, wenn beispielsweise die IT-Struktur ausfällt. Die in den Antworten vorkommenden Datenkategorien können Abbildung 6.2 entnommen werden. In der Praxis ist es ratsam, den Mitarbeitenden diese Daten in einer Notfallsituation im Rahmen ihres berufs- und abteilungsspezifischen Rollen- und Berechtigungskonzeptes bereitzustellen.

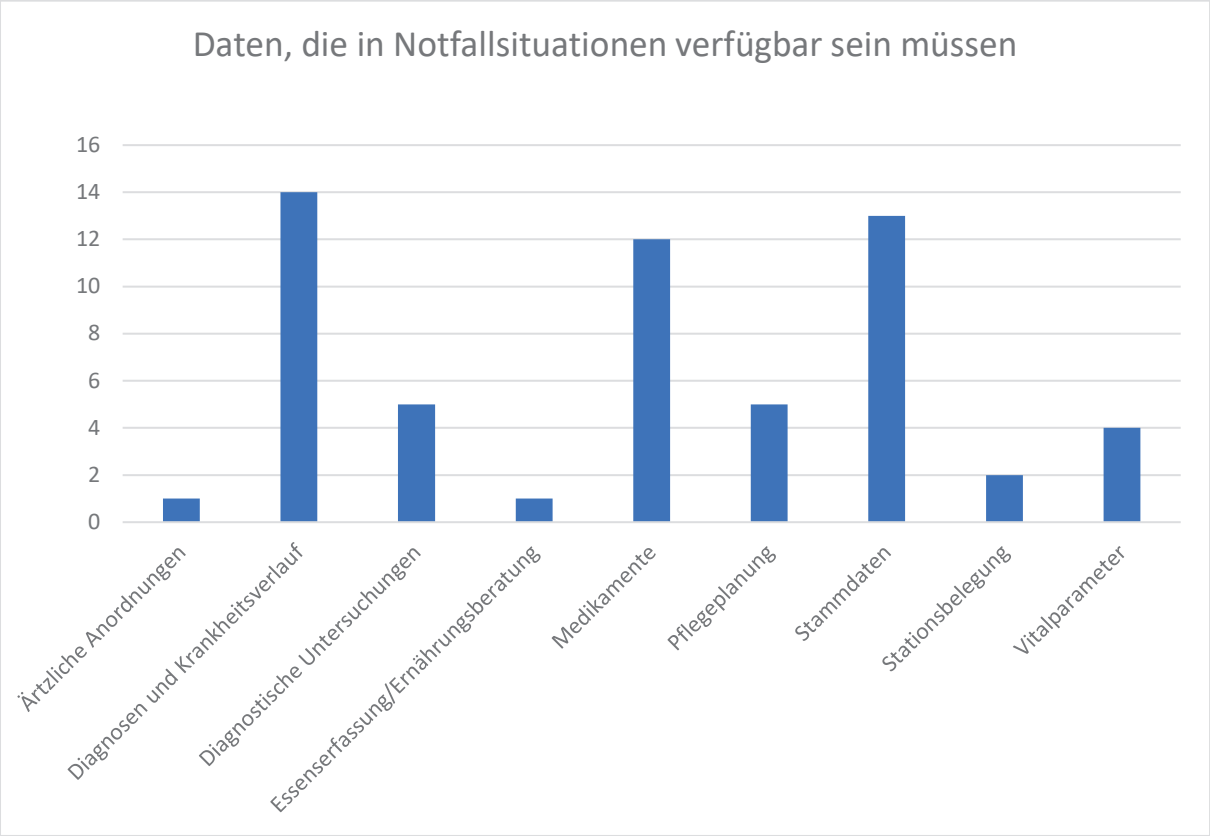


Abbildung 6.2: Daten für Notfallsituationen

Es hängt von der jeweiligen Abteilung oder Fachrichtung ab, welche Patientendaten in Notfallsituationen wirklich zur Verfügung stehen müssen. Die Mitarbeitenden in der Notaufnahme benötigen höchstwahrscheinlich andere Daten als diejenigen im Fallmanagement. Dieser Ansicht ist auch Experte K: „Ist auch wieder eine Frage der Brille, weil bei einer Notfallklinik zum Beispiel die aktuelle Medikation, sage ich mal, relativ wurscht ist, auf einer Station das aber wieder ganz anders gesehen wird natürlich“ (Interview K, Pos. 166–169). Für die Praxis kann daraus abgeleitet werden, dass sich jede Abteilung und jede Fachrichtung darüber Gedanken machen muss, welche Daten sie brauchen, wenn die elektronische Patientenakte nicht mehr verfügbar ist und die Erkrankten trotzdem weiter versorgt werden müssen.

Falls die elektronische Akte nicht mehr zur Verfügung steht, ist eine detaillierte und ausführliche mündliche Übergabe der Erkrankten unerlässlich. Nur so kann sichergestellt werden, dass alle relevanten den Erkrankten betreffenden Aspekte an Kollegen weitergegeben und so Informationsverluste vermieden werden, die wiederum zu gefährlichen Situationen führen können. Dies sieht auch Hieber (2018) in seinem Fachartikel ähnlich. Darin beschreibt er die Notwendigkeit der Pflegeübergabe sowie die Fehler bei der mündlichen Durchführung und fordert deren Übung. Diese Meinung vertritt auch Experte K: „[…], wenn ich jetzt einen kompletten Ausfall habe, muss die Übergabe nochmal ein Stück intensiver erfolgen, denke ich, weil man dann Informationen zum Patienten kriegt“ (Interview K, Pos. 171–173). Für die Praxis lässt sich daraus ableiten, dass die Durchführung einer detaillierten mündlichen Übergabe

des Erkrankten bei fehlendem Zugriff auf die digitale Patientenakte von Vorteil ist. Hierbei ist es ratsam, ein strukturiertes Übergabeformular zu entwickeln, um den Mitarbeitenden eine Hilfestellung zu geben. Diese Übergabeprotokolle können digitalisiert und den elektrischen Patientenakten zugeordnet werden, wenn Letztere wieder zur Verfügung stehen. So können wichtige dokumentierte Informationen aus den Übergabeprotokollen die Patientenakte erweitern und so dafür sorgen, dass trotz des Ausfalls der digitalen Patientenakte weiterhin Dokumentationen über den Erkrankten geführt werden können.

Auch für den weiteren Betrieb der digitalen Patientenakte nach der Implementierung werden vermutlich elektronische Endgeräte benötigt. Im Rahmen der Interviews wurden die Experten gefragt, welche Endgeräte sie zum Datenabruf benötigen. Die Antworten darauf können Abbildung 6.3 entnommen werden. Es ist für die Praxis ratsam, den Mitarbeitenden die in der Abbildung 6.3 aufgeführten Endgeräte zur Verfügung zu stellen, um die Daten für die tägliche Arbeit abrufen zu können.

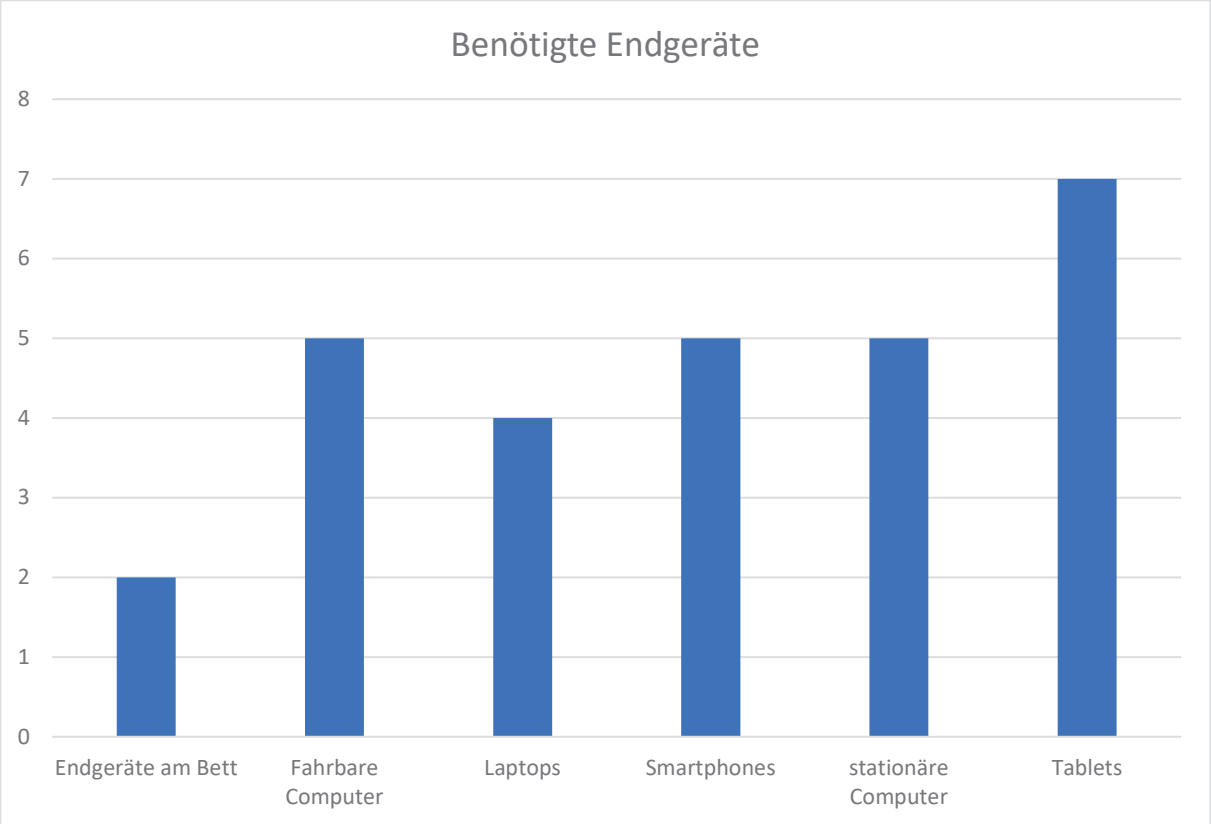


Abbildung 6.3: Benötigte Endgeräte

Es ist davon auszugehen, dass die elektronischen Endgeräte nicht nur benutzerfreundlich sein sollten, sondern auch an die Anforderungen des Krankenhauses und die zu dokumentierenden Daten angepasst werden müssen. Experte K unterstützt diese Aussage:

> *„[…], wenn ich viel tippen muss zum Beispiel, also wenn ich zum Beispiel eine Anamnese oder sowas mache und ich muss viel schreiben, bietet sich natürlich*

> *ein anderes Gerät an, als wenn ich nur ganz schnell ein paar Vitalparameter aufnehmen will“ (Interview K, Pos. 139–142).*

Die Benutzerfreundlichkeit kann den Mitarbeitenden vermutlich die Arbeit erleichtern, daher sollte die Endgeräte ein intuitives und selbsterklärendes Design haben. Dieser Meinung ist auch Experte K: „So bedienfreundlich wie irgend möglich“ (Interview K, Pos. 138). Für die Praxis kann daraus abgeleitet werden, dass im Vorhinein geprüft werden muss, welche Endgeräte für welchen Dokumentationszweck benötigt werden. Zudem sollten die Mitarbeitenden in die Entscheidung über die Anschaffung und über die Art der Endgeräte einbezogen werden, da sie täglich damit arbeiten müssen. So können für sie passende und benutzerfreundliche Endgeräte zur Verfügung gestellt werden.

Um alle Funktionalitäten der digitalen Patientenakte nutzen zu können, ist es vermutlich von Vorteil, verschiedene Arten von elektronischen Endgeräten anzuschaffen. Dies kann durch die Aussage des Experten I bestätigt werden: „Aber es sollte auch ein Mix sein“ (Interview I, Pos. 205-206).

Des Weiteren ist davon auszugehen, dass den Mitarbeitenden eine ausreichende Anzahl von elektronischen Endgeräten bereitgestellt werden muss. Wenn jeder Mitarbeitende die Chance zur Durchführung der Dokumentation hat, ohne dabei auf seine Kollegen warten zu müssen, ist eine schnelle und informationsverlustfreie Dokumentation möglich. Dies sieht auch Experte E so: „[…] ausreichend Geräte vorhanden sein“ (Interview E, Pos. 162). Für die Praxis kann daraus geschlossen werden, dass eine ausreichende Anzahl von elektronischen Endgeräten zur Verfügung stehen muss, damit jeder Mitarbeitende zeitnah und ohne Wartezeit seine erbrachte Leistung dokumentieren kann. Die Anzahl muss je nach Station oder Bereich individuell betrachtet werden.

Die Akkukapazität und -laufzeit spielen bei der Beschaffung elektronischer Endgeräte vermutlich eine entscheidende Rolle. Mitarbeitende sind mit hoher Wahrscheinlichkeit auf Geräte mit hoher und stabiler Akkuleistung angewiesen. Es ist davon auszugehen, dass Geräte mit geringer Akkuleistung für die Mitarbeitenden zu einem erhöhten Arbeitsaufwand führen. Dies bestätigt auch Experte E im Interview: „[…], es bringt nichts, kleine Geräte zu haben oder irgendwelche Laptops, wo die Akkuleistung sehr schwach ist. Und da fange ich gerade an zu dokumentieren und da ist ein Akku aus“ (Interview E, Pos. 167–169). Auch Experte C vertritt diese Meinung. Es liegt die Vermutung nahe, dass durch eine hohe Akkukapazität eine reibungslose und unterbrechungsfreie Dokumentation erfolgen kann. Des Weiteren kann angenommen werden, dass bei Endgeräten ohne ausreichende Akkukapazität die Möglichkeit besteht, diese bei Bedarf gemäß den individuellen Anforderungen zu erweitern und auszubauen. Für die Praxis ist zu empfehlen, bei der Anschaffung von elektronischen Endgeräten auf eine hohe und stabile Akkulaufzeit zu achten, um den Mitarbeitenden eine unterbrechungsfreie Dokumentation zu ermöglichen. Außerdem sollte eine skalierbare Akkukapazität berücksichtigt werden.

Darüber hinaus ist wahrscheinlich auch die Größe des Monitors ein relevantes Thema. Laptops besitzen oftmals nur eine Bildschirmdiagonale von 14 bis 20 Zoll (Axel

Springer SE, 2020), was die Lesbarkeit der elektronischen Patientenakte erschwert. Fest verbaute 23-Zoll-Monitore auf Visitenwagen können die Lesbarkeit und die Benutzerfreundlichkeit der elektronischen Patientenakte höchstwahrscheinlich steigern. Eine ähnliche Ansicht vertritt auch Experte C:

> *„[…], dann kriegt der einen größeren Monitor. Wir hatten bisher einen verbauten Laptop und jetzt soll dann der 23-Zoll-Monitor drauf, entsprechend ein relativ leistungsstarker PC in diesen Wägen mit verbaut, und aber auch noch eine externe Akku-Andockstation, die man auch an separater Stelle laden kann und entsprechend wieder austauschen“ (Interview C, Pos. 281–286).*

Die Vermutung liegt nahe, dass die digitale Patientenakte von einer stabilen und flächendeckenden WLAN-Verbindung abhängig ist. Dadurch können mit hoher Wahrscheinlichkeit ein effektives Arbeiten ermöglicht sowie Verluste von Informationen und Daten verhindert werden. Auch Experte C äußert eine ähnliche Ansicht:

> *„Wenn die Pflegenden der Meinung sind, sie haben jetzt den Blutdruck weggeschickt oder das ist alles eingegeben, und dann schauen sie später in die Akten rein und da kam nichts an, weil das WLAN leider doch nicht funktioniert hat, das sind so Sachen, das ist unglaublich zermürbend für die ganzen Bemühungen, die man da hineinsteckt, weil das Vertrauen letztendlich von den Mitarbeitern verloren geht, was das ganze angeht“ (Interview C, Pos. 298–304).*

Für die Praxis ist eine lückenlose WLAN-Abdeckung in allen Bereichen zu empfehlen, in denen die elektronische Patientenakte verwendet wird. Zudem sollte darauf geachtet werden, dass die Konfigurationen des WLAN-Systems auf die Anforderungen der Endgeräte zugeschnitten ist.

Nicht nur bei Software-, sondern auch bei Hardwaresystemen muss vermutlich die Datensicherheit gewährleistet sein. Diese Meinung vertritt auch Experte C: „All das gebietet aber natürlich immer noch mehr Sicherheitsaspekte, die man dann wiederum bedenken müsste“ (Interview C, Pos. 272–273). Für die Praxis lässt sich daraus die Handlungsempfehlung ableiten, dass die Beschäftigung mit der Thematik Datensicherheit bereits vor der Anschaffung der elektronischen Endgeräte erfolgen muss. Hierzu müssen die Anforderungen an die Datensicherheit im Vorhinein festgelegt und mit dem Hersteller der Endgeräte besprochen werden.

Es besteht die Möglichkeit, die elektronische Patientenakte cloudbasiert zu führen. Diese Lösung kann als Managed Service betrieben werden, was bedeutet, dass der Anbieter des Cloudsystems dessen Einrichtung, Wartung und Aktualisierung übernimmt (Telekom Deutschland GmbH, o.J.). Dies kann höchstwahrscheinlich von Vorteil sein, da eigene personelle Ressourcen eingespart und anderweitig (z.B. Prozessoptimierung) genutzt werden können. Dies sieht auch Experte B so: „Dann hätte ich mit dem Personal mehr Zeit für die Prozessunterstützung. Radikaler Ansatz. Raus damit, alles in die Cloud, von einem Dritten betreiben lassen bzw. als Managed

Service. Aus eigenen Kräften werden wir diese Verfügbarkeit nicht mehr hinbringen“ (Interview B, Pos. 213–216).

Ein weiterer möglicher Vorteil besteht darin, dass Systeme von Cloudanbietern zumeist weniger störanfällig als hausinterne Systeme sind. Dies sieht Experte B ebenso: „[…] gute Cloud bei einem großen Anbieter fällt weniger aus, als wenn das Krankenhaus das selber macht“ (Interview B, Pos. 212–213).

Zum Schluss gibt Experte B noch einen Hinweis zum Besitz von Hard- und Software:

> *„[…], da bin ich eher ein Anhänger von Cloud-Computing und sage: Der Besitz an Soft- und Hardware ist heute nicht mehr erstrebenswert. Also es muss nicht sein, dass das Zeug alles heute im Krankenhaus steht und auch dem Krankenhaus gehört. Dann hätten Sie nämlich das Thema mit dieser Verfügbarkeit. Sie können das heute kaufen. Da gibt es am Markt genügend Anbieter“ (Interview B, Pos. 207–211).*

6.14. Datenschutz

Gerade im Krankenhaussektor werden viele sensible Daten von Erkrankten kumuliert, weshalb der Datenschutz auch dort einen wichtigen Stellenwert einnimmt (Braun, 2017). Diese Ansicht vertritt Experte D ebenfalls: „Datenschutz im Krankenhaus ist genauso ernst zu nehmen oder noch viel ernster zu nehmen wie Datenschutz außerhalb des Krankenhauses, aber mir wäre jetzt nicht bewusst, dass es da irgendwelche Sonderregelungen geben muss oder vielleicht gibt für das Krankenhaus“ (Interview D, Pos. 209–212).

Zwei wichtige Konzepte im Bereich Datenschutz sind zum einen die europäische Datenschutzgrundverordnung und zum anderen die berufliche Schweigepflicht zu sein. Diese Meinung teilt auch Experte N. Sie finden sich in den entsprechenden gesetzlichen Grundlagen (Bundesministeriums der Justiz und für Verbraucherschutz [BMJV] & Bundesamts für Justiz [BfJ], 1871; EUR-OP, 2016). Diese Aussage wir durch den Experten B in ähnlicher Weise vertreten: „DSGVO aufschlagen, einmal durchgehen. Das alles muss erfüllt sein. Da gibt es ein paar technische Vorgaben, da gibt es eine sogenannte Orientierungshilfe, Krankenhausinformationssysteme von der Datenschutzkonferenz“ (Interview B, Pos. 245–248).

Einer der wichtigsten Aspekte, die bei diesem Thema beachtet werden müssen, sind die Prinzipien des Datenschutzes. Diese sind in Artikel 5 der europäischen Datenschutzgrundverordnung zu finden. Sie lauten (EUR-OP, 2016):

- Rechtmäßigkeit, Verarbeitung der Daten nach Treu und Glauben, Transparenz,
- Bindung an einen Zweck,
- Minimierung der Daten,
- Richtigkeit,
- Begrenzung der Speicherung,

- Integrität und Vertraulichkeit
- sowie Pflicht zur Rechenschaft

Diese Ansicht vertritt Experte I ebenfalls, aber er nennt dabei lediglich zwei Grundsätze des Datenschutzes: „[…] Grundprinzipien des Datenschutzes - Datensparsamkeit, Datenvermeidung“ (Interview I, Pos. 253–254).

Mitarbeitende sollten nur auf die für sie und die für die Behandlung und Pflege ihrer Erkrankten benötigten Daten zugreifen können (Kropp, 2016). Diese Ansicht wird auch durch Experten F unterstützt: „[…] nur die Berufsgruppen auf die Daten zugreifen können, die mit den Patienten arbeiten, die auch von Nöten sind nur für die Berufsgruppe“ (Interview F, Pos. 174–176). Auch die Experten C, D, E, G, I, J, K, M und N äußern in der Befragung ähnliche Meinungen.

Damit Beschäftigte nur auf die für sie benötigen Daten zugreifen können, bedarf es eines Rollen- und Berechtigungskonzeptes (Kropp, 2016). Dies sieht auch Experte E so: „[…] Rollenzuordnung und Zuordnung der Rechte muss sichergestellt werden“ (Interview E, Pos. 204–205). Diese Ansicht teilen auch die Experten G, I, J, K, M, und N.

Es ist anzunehmen, dass die Vergabe von Rechten im Rahmen der Rollen- und Benutzerkonzepte arbeitsaufwendig und zeitintensiv ist. Dies liegt vermutlich an den hohen berufsspezifischen und stationsspezifischen Anforderungen, die dabei bedacht werden müssen. Diesen Standpunkt vertritt auch Experte K: „Das ist auch was, was uns in unserem System sehr, sehr viel beschäftigt, wo wir permanent mit der Pflege der Daten beschäftigt sind, um Zugriffe zu gewähren oder auch wieder zu unterbinden“ (Interview K, Pos. 194–196).

Es ist davon auszugehen, dass Mitarbeitende trotz der Rollen- und Benutzerkonzepte in gerechtfertigten Situationen Zugriff auf Patientendaten von anderen Stationen erhalten können, beispielsweise wenn durch einen Personalausfall deren Hilfe benötigt wird. Dabei ist es zum Schutz der Daten höchstwahrscheinlich notwendig, dass der Zugriff auf die stationsfremden Erkrankte schriftlich im System dokumentiert und dies mit einer Eingabe des eigenen Benutzerpasswortes bestätigt wird. Diese Ansicht vertritt auch Experte L im Interview:

> *„[…] wirklich den Grund angeben, warum man auf die Daten zugegriffen hat. Also ich kann jetzt da nichts genau sagen, aber ich finde, wenn ich jetzt in eine Akte reinkomme (...) Naja, warte mal. Wenn ich den Patienten versorge, dann muss ich mich höchstwahrscheinlich nicht rechtfertigen, warum ich in die Akte reingekommen bin, weil das wäre dann zu viel. Aber wenn der Patient jetzt nicht in meinem Versorgungsbereich liegt, dann müsste ich wirklich kennzeichnen, warum ich da reingekommen bin, und das müsste machbar sein, so wie jetzt auch mit einem richtigen Grund“ (Interview L, Pos. 133–140).*

Es besteht Grund zur Annahme, dass in den Systemen ein lückenloses und detailliertes Protokoll (z.B. Zugriff, Veränderungen im Hintergrund) geführt werden

muss, um die Zugriffe auf die Patientendaten überwachen und überprüfen zu können. Dieser Meinung ist auch Experte I: „[…] gesamte System als zusätzlicher Schutzmechanismus natürlich die Protokollierung von Zugriffen, Zugriffszeiten und dann auch Veränderungen im System“ (Interview I, Pos. 296–298). Die Experten G, F, und D vertreten ebenfalls diese Ansicht.

Auch Experte B unterstützt diese Haltung, gibt aber zu bedenken, dass die protokollierten Zugriffe sicher verwahrt und nur dazu benutzt werden, bestimmte Fragestellungen beispielsweise aus Datenschutzsicht zu beantworten:

> *„Da plädiere ich dafür, dass das System im Background perfekt Logbuch führt. Da muss ich wirklich sagen, auf die Sekunde genau: Wer hat wann was mit wem mit welchem Dokument gemacht? Sogar er hat einfach nur die Übersicht der Station geöffnet. Denn Festplatten- oder Rechenkapazität kostet heute nichts mehr. Diese Logbücher würde ich dann aber extrem stark wegsperren und eigentlich am liebsten gar keinen Zugriff geben auf die komplette Datenbank, sondern dann auf diese Logbücher und auf diese Datenbanken Sichten bauen, die dann eben konkrete Fragestellungen beantworten“ (Interview B, Pos. 261–268).*

Es ist zu erwarten, dass Verstöße gegen den Datenschutz für die Mitarbeitenden sofortige arbeitsrechtliche und ggf. strafrechtliche Konsequenzen nach sich ziehen. Diese Aussage wird durch den Experten J bestätigt: „[…] man muss eben dann auch durch Logfiles das sozusagen kontrollieren: Wer hat denn tatsächlich zugegriffen? Wenn man dann feststellt, dass Leute zugegriffen haben, die kein Recht darauf hatten, dann muss das auch Konsequenzen haben dienstrechtlich“ (Interview J, Pos. 214–217).

Daraus lässt sich für die Praxis ableiten, dass die elektronischen Dokumentationssysteme eine lückenlose Protokollführung im Hintergrund ermöglichen sollten, um so überprüfen zu können, welche Zugriffe zu welcher Zeit durch wen stattgefunden haben und welche Veränderungen in der elektronischen Patientenakte vorgenommen worden sind.

Es erscheint notwendig einen Datenschutzbeauftragen zu beauftragen, da das Thema Datenschutz und seine rechtlichen Anforderungen komplex sind und hierbei ein fundiertes Expertenwissen benötigt wird. Die Experten N und D nennen diese Position in der Befragung „Datenschutzbeauftragten“ (Interview N, Pos. 178) und „interne Datenschützer“ (Interview D, Pos. 218). Experte D erwähnt ebenfalls die Stelle des „Bundesdatenschutzbeauftragten“ (Interview D, Pos. 217).

Es ist naheliegend, für die Datenschutzüberwachung Kontrollinstanzen zu etablieren. Diese sollten vermutlich die Möglichkeit haben, Prüfungen in Hinblick auf datenschutzrechtliche Fragestellungen durchzuführen. Dazu berichtet Experte K Folgendes:

> *„Wir werden aber auch von Externen geprüft, und Externe in zweierlei Sinn. Einmal extern durch Kräfte bei uns im Haus. Also wir haben eine eigene IT-Sicherheitsabteilung und einen Datenschutz natürlich, die unsere Datenhaltung*

> *überprüfen und stichprobenartig alle möglichen Sachen checken und auch immer wieder die Rechenschaft abgeben müssen über verschiedene Dinge. Und extern auch nochmal von außen. Es gibt regelmäßige BSI-Audits zum Beispiel, wo externe Prüfer unsere Systeme durchchecken, Interviews machen, sich verschiedene Strukturen vorlegen lassen, wir Dinge ausarbeiten müssen, um das zu belegen, wie wir damit umgehen. Ja, es ist schon ziemlich umfangreich" (Interview K, Pos. 206–214).*

Des Weiteren kann angenommen werden, dass die Rechtsabteilung eine weitere Kontrollinstanz darstellt, die ebenfalls stichprobenartig datenschutzrechtliche Prüfungen durchführt. Diese Ansicht vertritt auch Experte I: „[…] juristischer Seite muss eine Prüfung stattfinden" (Interview I, Pos. 268).

Es ist zu vermuten, dass die Kontrollinstanzen mithilfe der IT-Abteilung datenschutzrechtliche Fragestellungen aus den Logprotokollen ableiten können. Dies bestätigt auch Experte C: „[…] in der EDV die Möglichkeit, diese Kontrollgeschichten auszuleiten" (Interview C, Pos. 405–406). Es ist davon auszugehen, dass die Logdateien durch die Prüfung in Hinblick auf datenschutzrechtliche Fragestellungen kritisch betrachtet werden und einer Überprüfung zugeführt werden können: „[…], dass man da durchaus kritisch auf die Sachen draufschauen, um entsprechend dem Datenschutz Rechnung zu tragen" (Interview C, Pos. 411–412).

Dabei ist es unumgänglich, dass die Überprüfung der Logdateien und der Datenschutzprotokolle immer nach dem Vier- bzw. Sechs-Augen-Prinzip durchgeführt wird, um Datenmissbrauch zu verhindern. Hauser (2014) plädiert auch für ein Vier-Augen-Prinzip beim unberechtigten Zugriff auf Datensätze. Experte B ist ähnlicher Meinung: „Und das erstmal nur immer ein Level mit ‚Schau mal, da ist ein Überblick, und jetzt im nächsten Schritt kannst du vielleicht nach Vier-Augen- oder Sechs-Augen-Prinzip eins tiefer gehen und die Details anschauen'" (Interview B, Pos. 276–278).

Die Aufbewahrungsfristen und die Speicherung medizinischer sowie pflegerischer Dokumente spielen beim Thema Datenschutz ebenfalls eine relevante Rolle und müssen über zehn bis 30 Jahre gewährleistet werden (BLÄK, o.J.; BMJV & juris GmbH, 1987; BMJV & BfJ, 1998). Dies sieht auch Experte N ähnlich: „Die Speicherung, die muss ich auch (...) Ich sage mal, die gesetzlichen Aufbewahrungsfristen müssen natürlich da berücksichtigt werden" (Interview N, Pos. 187–188).

Es liegt nahe, dass eine regelmäßige Archivspeicherung der elektronischen Patientenakte und eine lückenlose Dokumentation gewährleisten werden müssen. Experte E bestätigt diese Aussage: „[…] Speicherung der Daten muss eigentlich in regelmäßigen Abständen erfolgen" (Interview E, Pos. 220–221). Auch die Experten N und G haben ähnliche Ansichten.

Die archivierten Datensätze müssen im digitalen Langzeitarchiv zugriffssicher abgelegt werden. Dies bedeutet, dass die Daten nur von einem kleinen Kreis berechtigter Personen abgerufen werden können, aber zu jeder Zeit. Auch Semler (2000) vertritt in seiner Arbeit diese Ansicht und Experte E sieht dies ebenfalls ähnlich: „Im Archivierungsprogramm. Also es muss auch ein digitales Archiv vorhanden sein,

wo diese Daten archiviert werden für längere Zeit, wo man jederzeit auch Zugriff hat“ (Interview E, Pos. 216–218). Experte K ist dabei ähnlicher Meinung, dennoch merkt er an, dass die Datensätze bei immer wiederkehrenden Erkrankten zur Verfügung stehen sollten, um so den Verlauf ihrer Erkrankung nachvollziehen zu können: „Aber Patienten kommen teilweise immer wieder ins Haus. Heißt, ich muss unter Umständen dann doch wieder Zugriff auf die alten Daten haben, auch weil ich den Krankheitsverlauf eines Patienten nachvollziehen können muss“ (Interview K, Pos. 222–225). In der Praxis kann der Zugriff auf ältere Daten beispielsweise durch ein berufsgruppenspezifisches Rollen- und Berechtigungskonzept ermöglicht werden, damit eine ganzheitliche Betrachtung der Erkrankten unter Einbezug ihrer Voraufenthalte stattfinden kann.

Die Systeme sollten so programmiert sein, dass Datensätze nach Ablauf der gesetzlichen Aufbewahrungsfrist automatisch gelöscht werden. Es liegt nahe, dass eine Erinnerungs- bzw. Warnfunktion integriert werden kann, die den Benutzer auf die bevorstehende endgültige Löschung hinweist. Diese Ansicht äußert auch Experte I im Interview:

> *„Idealerweise ist ein Konzept schon implementiert, das es ermöglicht, dass man abhängig von bestimmten Datenarten oder Datenkategorien schon eine Speicherdauer definieren kann. Das heißt, dann würden nach einem gewissen Zeitpunkt – sechs Monate, zehn Jahre – die Daten nach vielleicht kurzem Erinnern, ‚Es würden jetzt folgende Daten gelöscht werden‘, automatisch gelöscht werden bzw. vielleicht mit der Vorstufe. Die werden dann erstmal gesperrt und dann nochmal gelöscht“ (Interview I, Pos. 301–306).*

Nach der europäischen Datenschutzgrundverordnung hat jeder Betroffene Rechte bezüglich seiner Daten (EUR-OP, 2016). Diese Aussage unterstreicht Experte I: „Betroffenenrechte - die Patienten können ja ihre Rechte geltend machen“ (Interview I, Pos. 255). Betroffene müssen unter anderem über datenschutzrechtliche Aspekte aufgeklärt und um schriftliche Zustimmung gebeten werden (EUR-OP, 2016). Dies sieht auch Experte A ähnlich: „Der Patient muss bei Aufnahme oder oft schon vor Aufnahme darüber informiert werden, was eben bei den Datenschutzvereinbarungen vorhanden ist, an wen diese Daten weitergegeben dürfen in welchem Rahmen. Das auch gegen Unterschrift“ (Interview A, Pos. 124–127). Auch Experte F teilt diese Ansicht.

Ein weiteres Betroffenenrecht ist das Recht auf Auskunft in Bezug auf die persönlichen Daten (EUR-OP, 2016). Dies sieht auch Experte I ähnlich: „[…], wenn jemand Auskunft haben möchte, dann muss er die idealerweise auf Knopfdruck bekommen, welche Daten gespeichert sind“ (Interview I, Pos. 256–258).

Informationen über den Zweck und die Verwendung der Daten kann der Betroffene ebenfalls einfordern (EUR-OP, 2016). Dies wird vom Experten I im Interview bestätigt: „[…] transparent sein, zu welchen Zwecken auch die Daten in dem System verarbeitet werden. Es muss transparent sein, welche Daten wie lange aufbewahrt werden“ (Interview I, Pos. 258–260).

Das Betroffenenrecht gibt auch die Möglichkeit, Daten korrigieren oder löschen zu lassen (EUR-OP, 2016). Dies sieht auch Experte I so: „Er darf diese Daten berichtigen lassen, wenn sie falsch sind, und er darf oder kann auch fordern, dass die Daten gelöscht werden“ (Interview I, Pos. 261–263). Experte B gibt zu bedenken, dass bei Krankenhauspersonal aktuell noch Angst davor besteht, Datensätze von Erkrankten auf Wunsch zu löschen. Hier macht Experte B Mut, auch diesen Schritt in Zukunft zu wagen:

> *„Wir haben das Thema mit Löschung, das ist eine ganz spannende Herausforderung. Momentan haben wir immer ein bisschen Angst, Daten zu löschen. Vielleicht muss man da mal den Mut haben, zu sagen: Ja, wenn der Patient das wünscht, dann löschen wir es“ (Interview B, Pos. 252–255).*

Nach erster Analyse ist davon auszugehen, dass Mitarbeitende im Krankenhaus bei der Einstellung eine Datenschutzvereinbarung unterschreiben müssen, an die sie dauerhaft gebunden sind. Die Vermutung liegt nahe, dass dies für die Mitarbeitenden eine Dienstpflicht darstellt. Experte A bestätigt diese Ansicht: „Soweit ich weiß, steht das ganze zumindest bei uns in der Klinik im Arbeitsvertrag“ (Interview A, Pos. 130–131). Auch die Experten A und L sind ähnlicher Meinung.

Es sollte auch darauf geachtet werden, dass den datenschutzrechtlichen Anforderungen durch die zur Verfügung gestellten Systeme selbst und die Verträge mit den externen Dienstleistern Genüge getan wird. Eine ähnliche Ansicht vertritt Experte I: „[…] sichergestellt sein, dass das System an und für sich datenschutzkonform ist. Das fängt in der vertraglichen Gestaltung schon an, dass zum Beispiel keine Unterauftragnehmer aus Russland zum Beispiel eingesetzt sind“ (Interview I, Pos. 265–267).

Die Daten müssen vor Zugriffen durch Dritte und von außerhalb geschützt werden (EUR-OP, 2016). Diese Meinung teilt auch Experte F während der Befragung: „[…] Zugriff von außen geschützt ist“ (Interview F, Pos. 176). Auch die Experten L und C vertreten einen ähnlichen Standpunkt wie Experte F.

Damit dies garantiert werden kann, sollten unterschiedliche Sicherheitsmaßnahmen ergriffen werden. Es scheint unumgänglich, dass die Sicherheit der IT-Struktur sowie der technischen Systeme auch durch eine Fachperson aus dem Bereich IT-Sicherheit gewährleistet wird. Diese Aussage unterstreicht Experte D: „IT-Sicherheit muss geregelt sein durch entsprechende Fachleute und Systeme natürlich und Sicherungssysteme“ (Interview D, Pos. 220–221).

Um die Sicherheit zu erhöhen, können verschiedene Authentifizierungsverfahren angewendet werden. So kann dies durch eine Zwei-Faktor-Authentifizierung oder eine Multi-Faktor-Authentifizierung erfolgen (Bundesamt für Sicherheit in der Informationstechnik [BSI], o.J.b; Microsoft, 2020; Pohlmann, o.J.). Das Ziel ist es, eine Identifikation von den Leuten zu ermöglichen, die über die Zugriffsberechtigung für die elektronische Patientenakte verfügen. Diese Meinung vertritt auch Experte I:

> *„[…] sichere Authentifizierungsmethode wählen, vorangestellt auch mit einem sicheren Anmeldeprozess. Das heißt also, dass auch Leute identifiziert und überprüft werden. Ist das tatsächlich diese Person, die jetzt Zugriff auf diese Daten nehmen möchte? Genau, wie gesagt, sicherer Zugriff, am besten Zwei-Faktor- oder Multi-Faktor-Authentifizierung“ (Interview I, Pos. 284–288).*

Auch der automatische Logout aus dem System nach einer bestimmten Zeit ohne Nutzung sollte vermutlich als Sicherungsmaßnahme in Betracht gezogen werden. Diese Ansicht teilt Experte I ebenso: „[…] automatischer Logout stattfindet, wenn man eine gewisse Zeit inaktiv ist, um da eben auch einen unbefugten Zugriff zu vermeiden“ (Interview I, Pos. 289–290).

Es liegt nahe, dass Zugriffe auf Daten begründet und in Verbindung mit einem Passwort freigeschaltet werden müssen, damit die sensiblen Daten geschützt sind. Dies sieht auch Experte F ähnlich: „[…] mit Passwörtern arbeitet, auch Begründungen, warum man darauf zugreift jetzt“ (Interview F, Pos. 177–178).

Es scheint selbstverständlich, dass die Verschlüsselung der Software- und Hardwareprodukte auf dem aktuellen Stand gehalten werden muss, damit ein Zugriff auf diese Systeme erschwert wird. Dieser Ansicht ist auch Experte B: „[…] das Thema Verschlüsselung uns überlegen. Welche Daten sind wo verschlüsselt, damit ein Angreifer eben sie nicht sofort erhält?“ (Interview B, Pos. 250–252).

Es ist ebenfalls davon auszugehen, dass die verwendeten Hardwareprodukte vor Diebstahl geschützt werden sollten. Diesen Standpunkt vertritt auch Experte E: „[…] auch sichergestellt werden, dass diese Hardware auch nicht einfach so mitgenommen werden kann durch Fremde“ (Interview E, Pos. 238–239).

Ein weiterer bedeutsamer Faktor im Bereich des Datenschutzes und der IT-Sicherheit liegt darin, die ‚Standardsicherheit (Security) by Design‘ zu gewährleisten, die gemäß der Datenschutzgrundverordnung gefordert wird (EUR-OP, 2016). Security by Design beschreibt ein Konzept, dass Sicherheitsaspekte eines Systems als Kriterium in der Designentwicklung berücksichtigt, um damit die Sicherheit des Systems zu gewährleisten (Tschersich, o.J.). Diese Meinung wird auch durch den Experten B vertreten: „[…], DSGVO geltende Standardsicherheit by Design muss gewährleistet sein“ (Interview B, Pos. 256–257).

Bei allen Angelegenheiten, die datenschutzrechtliche Fragen aufwerfen, sollte möglichst nach dem Vier-Augen-Prinzip oder mit einem erweiterten technischen Schutz vorgegangen werden. Auch Hauser (2014) sieht das Vier-Augen-Prinzip als Möglichkeit dazu, sensible Daten zu sichern. Diese Aussage wird auch durch den Interviewten I bestätigt: „[…] für die Systembetreuung muss natürlich auch ein sicheres Verfahren gewählt werden, idealerweise dann auch noch mit dem Vier-Augen-Prinzip bzw. mit einem Schutz oder einer entsprechenden Dokumentation, warum denn jetzt da Zugriff auf diese Daten genommen wurde“ (Interview I, Pos. 293–296).

Einen ganz anderen Ansatz im Bereich des Datenschutzes verfolgt Experte L. Dieser ist der Meinung, dass die Datenschutzerklärung gelockert werden muss: „Da müsste es ein bisschen gelockert werden“ (Interview L, Pos. 127). Für die Praxis ist fraglich,

ob eine solche Lockerung der Datenschutzerklärung einen positiven Effekt auf deren Rechtssicherheit hat.

6.15. Sicherheit

Die Sicherheit spielt bei der Implementierung einer elektronischen Patientenakte eine große Rolle. Diese muss nämlich eine hohe Sicherheitsanforderung erfüllen, da in ihr und mit ihr sensible Daten bearbeitet werden (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2020). Auch Experte A vertritt diese Ansicht: „Eine sehr hohe Sicherheitsanforderung, weil sehr, sehr sensible Daten dort hinterlegt sind“ (Interview A, Pos. 136–137).

Obwohl die Sicherheitsanforderungen in Bezug auf die elektronische Patientenakte hoch erscheinen, liegt die Vermutung nahe, dass dennoch auch nach wirtschaftlichen Faktoren zu bewerten ist, ob jede Schwachstelle im System behoben werden muss. Diesen Standpunkt äußert auch Experte B: „[…] Immer nach wirtschaftlichen Gesichtspunkten. Man muss nicht jede Schwachstelle, egal um welchen Preis, abstellen“ (Interview B, Pos. 307–309).

In der täglichen Arbeit kann vermutlich oftmals die falsche Hoffnung aufkommen, dass das System und die darin enthaltenen Daten durch die hohen Sicherheitsanforderungen immer zur Verfügung stehen und es kein Risiko mehr gibt. In dieser Hinsicht müssen die Mitarbeitenden höchstwahrscheinlich dahingehend sensibilisiert werden, dass trotz aller präventiven Maßnahmen ein Restrisiko existiert (e-mergency AG, 2020). Demnach sollte auch ein vollständiger Datenverlust in die Risikoanalyse einbezogen werden. Diese Aussage deckt sich ebenfalls mit der der Meinung des Experten B: „Aber man kann nicht glauben, nur weil es digital ist, da kann nichts mehr passieren. Auch da warne ich davor, zu sagen, digital heißt auch sicher. Auch da muss man einen Totalverlust mit einkalkulieren und den selbigen dann im Risiko beschreiben, was die Konsequenz wäre“ (Interview B, Pos. 295–298).

Mitarbeitende müssen ein Bewusstsein dafür entwickeln, dass auch menschliches Fehlverhalten technische Sicherheitsvorkehrungen aushebeln kann (Brockhaus, 2021). Dass die Mitarbeitenden geschult werden müssen, damit sie zu einem Teil des Sicherheitssystems werden, sieht auch Experte B:

> *„Und ganz am Ende entsteht auch Sicherheit, indem man die Mitarbeiter schult, schult, schult, also Awareness-Kampagnen, und sagt: "Ja, die Software ist so. Du musst dich mit einem Kennwort anmelden. Der Bildschirm sperrt sich nach einer gewissen Zeit zu." Das sollte man auch nicht vergessen, also die Sicherheit beim Faktor Mensch mit einkalkulieren, weil der oft alle anderen Konzepte aushebelt“ (Interview B, Pos. 312–317).*

Daraus lässt sich für die Praxis ableiten, dass die Mitarbeitenden entsprechend geschult und sensibilisiert werden müssen, besonders in Hinblick auf das Öffnen von E-Mailanhängen oder die Installation klinikfremder Software. Sie müssen ein Teil des Sicherheitssystems werden, um die elektronische Patientenakte und die darin befindlichen sensiblen Daten zu schützen.

Es liegt nahe, dass die Pflege und die Wartung der elektronischen Patientenakte sowie der dazugehörigen Systeme die Aufgabe der IT-Abteilung und der entsprechenden IT-Fachkräfte sein sollte. Diese Ansicht teilt auch Experte M: „Ich meine, dafür gibt es ja auch Fachleute, IT-Fachleute in einer großen Einrichtung, wie es uns gibt. Und denjenigen unterliegt das und die müssen das halt auch regelmäßig kontrollieren und warten“ (Interview M, Pos. 150–153). Eine Aufgabe der IT-Sicherheit stellt vermutlich die Überprüfung der Systeme dar, indem sie Test- und Prüfverfahren (z.B. simulierte Angriffe) einleiten und die Prüfergebnisse den beteiligten Akteuren zur Verfügung stellen. Diesen Standpunkt vertritt auch Experte K:

> *„Und es gibt die gleichen Prüfmechanismen, die ich vorher auch schon beschrieben habe. Es wird intern immer wieder geprüft, es werden intern Tests auch, also eine Art simulierte Angriffe zum Beispiel gefahren, um zu gucken: Haben wir irgendwo eine Lücke, irgendwas, was wir vielleicht übersehen haben könnten? Und wir werden auch da extern geprüft mit entsprechenden Prüfberichten, die bis zur Geschäftsführung dann ausgearbeitet und zur Geschäftsführung vorgelegt werden“ (Interview K, Pos. 254–260).*

Es könnte von Vorteil sein, eine Stabsstelle IT-Sicherheit zu implementieren. Diese kann sich vermutlich um alle Sicherheitsbelange hinsichtlich der elektronischen Patientenakte und deren Systeme kümmern. Dazu ist es ebenfalls notwendig, dass diese Stabsstelle eine entsprechende Anzahl von Fachpersonal erhält (Fracis & Maier, 2017). Auch Experte J kommt zu einer ähnlichen Ansicht: „[…] muss man die IT fragen. Oder wir haben ja dazu extra eine Stabsstelle für IT-Sicherheit“ (Interview J, Pos. 223–224).

Der Zugriff auf die Daten durch Dritte und von außerhalb muss verhindert werden (EUR-OP, 2016). Diese Meinung deckt sich mit der Aussage des Experten K: „In allererster Linie die Angreifbarkeit von außen“ (Interview K, Pos. 241). Aber auch die Experten A, E, G, L und N vertreten ähnliche Meinungen wie Experte K. Es ist anzunehmen, dass die Sicherheitsanforderungen verhindern sollen, dass beispielsweise Hacker von außen in das System gelangen, um dort Patientendaten zu stehlen oder diese so zu manipulieren, dass ein Schaden entsteht. Diese Aussage wird durch den Experten J unterstützt: „[…] natürlich um Hackerangriffe, also das ist sozusagen mutwillige Beschädigung, dass man das vermeidet. Das man vermeidet, dass auf Daten zugegriffen werden kann, dass die Daten verfälscht werden können“ (Interview J, Pos. 226–228). Experte F äußert zwar, dass der Zugriff von Unbefugten mit ausreichenden Mitteln verhindert werden soll, jedoch gibt er zu bedenken, dass dies nicht immer gewährleistet werden kann: „Zugriff durch Unbefugte sollte also auf jeden Fall verhindert werden mit ausreichenden Mitteln. Ich weiß, das kann man nicht immer 100 Prozent gewährleisten“ (Interview F, Pos. 188–190).

Auch die Sicherheit der Netzwerke muss garantiert sein. Besonders im Bereich der Netzwerksicherheit nimmt die Risikoanalyse einen hohen Stellenwert ein. Hier gibt es die Standardisierung ISO-80001, in der der Umgang mit Medizingeräten und IT-Netzwerken geregelt wird (Deutsches Institut für Normung [DIN], 2011). Diese Ansicht

vertritt auch Experte B: „[…] für die Netzwerke gibt es zum Beispiel eine ISO-80001, da ist beschrieben, wie man mit Medizingeräten in IT-Netzwerken umgeht. Das ist immer eine Risikobewertung, das ist eine Schwachstellenanalyse, das ist ein Abstellen der Schwachstellen“ (Interview B, Pos. 304–307). Für die Praxis lässt sich daraus ableiten, dass die Sicherheit der Netzwerke und seiner Schnittstellen genau geprüft werden muss. Dazu kann als Handlungshilfe die ISO-80001 herangezogen werden. Die Netzwerksicherheit sollte mithilfe einer Risikoanalyse bewertet und es sollten entsprechende Maßnahmen zur Behebung von Schwachstellen eingeleitet werden.

Um auch die Sicherheit der Datenintegrität zu gewährleisten, ist es unabdingbar, dass im Unternehmen das System mit Backups hinterlegt ist (Rahmati-Georges & Groves, 2018). Diese Ansicht teilt auch Experte D:

> *„Ich kann nicht nur einen Server, wo alles draufliegt, haben, sondern ich muss regelmäßig Backups fahren, dass wenn ich in die Situation komme, dass meine Systeme nicht mehr funktionieren oder durch ein Geschehnis, ein unvorhersehbares Geschehnis, außer Gefecht gesetzt sind, muss ich eine Rücksicherung haben“ (Interview D, Pos. 234–238).*

Auch die Experten B und C schließen sich der Meinung des de Experten D in ähnlicher Weise an.

Des Weiteren liegt die Vermutung nahe, dass die Backups auf verschiedene Arten redundant sein sollten. Die Abspeicherung der Datensätze auf zwei unterschiedlichen Systemen könnte eine Möglichkeit darstellen. Diese Ansicht teilt auch Experte J: „[…] Daten verteilt abspeichert“ (Interview J, Pos. 236). Vermutlich sind tägliche PDF-Speicherungen auf besonders gesicherten über das Haus verteilen PCs aber ebenso eine Option. Auch Experte B unterstreicht diese Aussage: „[…] alle Akten in Form von PDF-Dateien auf ausgewählten Rechnern einmal am Tag noch einmal in Anführungszeichen ausdruckt oder ablegt“ (Interview B, Pos. 288–289). Für die Praxis lässt sich daraus schließen, dass ein Backupsystem unbedingt verfügbar sein muss, um die Arbeit der Mitarbeitenden zu erleichtern, die Patientensicherheit und die Versorgungsqualität zu erhöhen und einen Datenverlust zu verhindern. Nach dieser Analyse liegt der Entschluss nahe, dass die elektronische Patientenakte täglich im PDF-Format gesichert werden sollten und diese Backups auf im Haus verteilten und gesicherten Rechnern oder für die bessere Mobilität und Handhabung auf Tablets gesichert werden.

Es ist davon auszugehen, dass auch die Zuverlässigkeit der Dienstleister bei der Sicherheit der Systeme eine entscheidende Rolle spielt. Sie sollte vermutlich im Voraus überprüft werden, um im Falle eines Problems kompetente und schnelle fachliche Unterstützung zu erhalten. Dies sieht auch Experte I ähnlich: „[…] zuverlässige Hersteller oder Produzenten sein, die diese Produkte anbieten, vertreiben“ (Interview I, Pos. 329–330).

Die angeschafften Systeme müssen den Anforderungen und Wünschen des Krankenhauses gerecht werden. Nur so ist anzunehmen, dass die geplante Implementierung zum Erfolg wird. Eine vergleichbare Haltung hat auch Experte E: „[…]

es muss auch sichergestellt werden, dass man auch die Hardware sich anschafft, die für das Krankenhaus geeignet ist“ (Interview E, Pos. 236–237).

Die elektronischen Endgeräte müssen Hygieneanforderungen an die Hardware erfüllen. Diese dienen dazu, dass die Endgeräte regelmäßig desinfiziert werden können, um so eine Verbreitung von pathogenem Material zu verhindern (Pramann, Graf & Albrecht, 2012). Auch Experte I trifft im Interview eine ähnliche Aussage: „[…] an die Endgeräte denkt, dass man da natürlich die entsprechenden Hygienevorgaben erfüllt, dass man eine abwischbare - jetzt habe ich einen Sprachfehler - desinfizierbare Oberfläche hat, um da eben die Hygienestandards zu halten“ (Interview I, Pos. 323–326). Daraus lässt sich für die Praxis ableiten, dass die Hardware und insbesondere die elektronischen Eingabegeräte eine abwischbare sowie desinfizierbare Oberfläche besitzen sollten, um so die Verbreitung von Krankheitserregern zu verhindern.

Besonders bei einem Ausfall der IT-Struktur spielt das Business Continuity Management (BCM) eine entscheidende Rolle. Das Grundkonzept besteht in der Geschäftsfortführung in Notfall-, Katastrophen- und Krisensituationen (RiskNET, o.J.). Auch hier liegt die Vermutung nahe, dass die elektronische Patientenakte eine wichtige Sicherheitsanforderung zu erfüllen hat. Das System muss wahrscheinlich so ausgelegt sein, dass die Mitarbeitenden bei einem Ausfall der IT-Struktur weiterhin Unterstützung durch das System erhalten, um reibungslos weiterarbeiten zu können. Dies sieht auch Experte B so: „[…] bei dem Thema mit dieser Verfügbarkeit. Da sind wir dann beim Thema mit der Geschäftsfortführung im Notfall. Das System muss mich unterstützen, möglichst reibungslos weiterzuarbeiten“ (Interview B, Pos. 284–286).

Es ist zu vermuten, dass die Systeme über unterschiedliche Mechanismen verfügen sollten, um die Sicherheitsanforderungen zu gewährleisten. Der Schutz mithilfe von Firewalls und Antivirenprogrammen stellt höchstwahrscheinlich eine Säule dar. Dies sieht auch Experte N ähnlich: „[…] ein Virenschutz oder Firewall vorhanden sein“ (Interview N, Pos. 200). Darüber hinaus müssen Sicherheitspatches ebenfalls unverzüglich in das System eingespielt werden und die Systeme auf dem aktuellen Stand gehalten werden. Diese Ansicht vertritt auch Experte K: „Die Software und die Hardware immer entsprechend aktuell zu halten, Sicherheitspatches relativ zügig einzuspielen“ (Interview K, Pos. 250–251).

Einen weiteren Sicherheitsaspekt stellt höchstwahrscheinlich das individuelle Einloggen in das System durch den Benutzer dar: „Man muss sich selber einloggen in alle Systeme, um was arbeiten zu können“ (Interview G, Pos. 150–151). Es liegt aber auch nahe, dass der automatische Logout infolge längerer Nichtbenutzung des Systems eine entscheidende Rolle bei der Sicherheit spielt: „Bildschirme regelmäßig gesperrt werden“ (Interview G, Pos. 150).

Es ist davon auszugehen, dass die Sicherheit der digitalen Patientenakte und der Systeme dadurch gewährleistet werden kann, dass Letztere regelmäßig überwacht werden. Dies bedingt vermutlich, dass die entsprechenden Ressourcen zur Verfügung gestellt werden, was auch Experte I ähnlich sieht:

> *„[…] intern überprüft werden, ob diese Systeme dem aktuellen Stand der Technik entsprechen. Und der verändert sich kontinuierlich. Das heißt: Wie werden Daten übertragen? Über welche Schnittstellen? Ist diese Kommunikation verschlüsselt oder nicht? Sind bekannte Schwachstellen in der Infrastruktur bekannt? Wie wird das System gemonitort, wie ist sozusagen der Security-Incident-Prozess dahinter, wenn man eben Anomalien feststellt oder wenn auch von Herstellerseite auf Schwachstellen oder Sicherheitsmängel aufmerksam gemacht wird. Aber damit einher geht auch die Verantwortung des Betreibers, also der Krankenhäuser, genügend Ressourcen für diese Systeme auch vorzuhalten, dass es eben auch genügend Systembetreuer gibt, um eben solche kritischen Systeme auch in der Stellvertreterregelung betreiben zu können“ (Interview I, Pos. 330–341).*

Die EDV-Abteilung steht für Hilfestellungen vermutlich auf verschiedenen Wegen zur Verfügung. Zum einen liegt die Vermutung nahe, dass über den Helpdesk telefonischer Support angefordert werden kann. Dieser Ansicht ist auch Experte J: „[…] direkte Nummer haben, die er im Schadensfall oder bei Problemen anrufen kann, wo er auch eine technische Hotline oder Ansprechpartner dahinter hat“ (Interview I, Pos. 350–352). Auch die Experten G, I, K, und L kommen zu der ähnlichen Meinung, dass sich Mitarbeitende an den telefonischen Helpdesk wenden können. Des Weiteren scheint die Möglichkeit zu bestehen, die EDV per E-Mail zu kontaktieren. Diese Meinung vertritt auch Experte L: „Da müsste auch irgendwo jemand entweder Bereitschaft haben oder per E-Mail zugeschaltet werden können“ (Interview L, Pos. 159–160).

Darüber hinaus ist anzunehmen, dass die im System oder im Intranet hinterlegten Handbücher benutzt werden können. Dies sieht auch Experte G ähnlich: „Auf der Startseite sind Handbücher hinterlegt, wo alles Mögliche beschrieben ist, was man machen kann, wie man es man es machen soll. Die sind aber sehr unübersichtlich bzw. sehr, sehr viele Seiten“ (Interview G, Pos. 164–167).

Zudem liegt es nahe, dass sich die Mitarbeitenden bei Fragen und Problemen an die Vorgesetzten wenden können (Interview H, Pos. 125–126). Des Weiteren stehen vermutlich auch die Mitarbeitenden der Anwendungsbetreuung zur Verfügung (Interview C, Pos. 434).

Die Einführung eines Frequently-Asked-Questions-Systems (FAQ) scheint eine Möglichkeit zu bieten, kleinere Probleme zu lösen – beispielsweise in den Nachtstunden. Diese Ansicht vertritt auch Experte D: „[…] FAQ-System zu etablieren“ (Interview D, Pos. 258). Die Experten I und B verweisen ebenfalls auf die Möglichkeit, ein FAQ-System zu etablieren.

Mithilfe von E-Learning kann den Mitarbeitenden vermutlich eine lösungsorientierte Hilfestellung angeboten werden. Auch Experte B sieht es als Möglichkeit der Problemlösung (Interview B, Pos. 321–322).

Die Eigeninitiative der Mitarbeitenden zur selbständigen Problemlösung muss gefördert werden. Es ist anzunehmen, dass dies mithilfe von Schulungsangeboten, E-Learning, Filmen und der Zuhilfenahme von künstlicher Intelligenz erfolgen kann. Diese Ansicht vertritt auch Experte B:

> *„Also da erwarte ich mir Eigeninitiative, nachdem vorher aber alle Register gezogen sind, wie wir es gehabt haben. E-Learning, Filme, was weiß ich. Sogar künstliche Intelligenz, dass das System mit dem Assistenten sagt, wenn er wo unterwegs ist, was er da machen könnte. Und dann die Bereitschaft, sich auch mit dem Zeug zu beschäftigen. Ich meine, ein Software-System ist jetzt kein Handy mit zwölf Tasten, wo man einfach mal rumdrückt wie früher. Ein bisschen Engagement muss auch vonseiten des Anwenders kommen“ (Interview B, Pos. 330–337).*

Auch die Experten K und I sehen die Schulung von Mitarbeitenden als notwendig an.

Ein weitere Problemlösungsansatz könnte darin liegen, dass sich die Kollegen untereinander Hilfestellung geben. Es ist davon auszugehen, dass Mitarbeitende gemeinsam versuchen können, Probleme selbst zu lösen und aus den Erfahrungen der anderen zu lernen. Dies sieht auch Experte D ähnlich: „[…] kollegial lösen“ (Interview D, Pos. 253).

Damit die Beschäftigten bei Fragen und Problemen bezüglich der elektronischen Patientenakte Hilfe einholen können, ist es vermutlich von Vorteil, Unterstützungstools (z.B. Hilfe-Popups) in das digitale System einzubauen. Es kann davon ausgegangen werden, dass dies gerade in den Nachtzeiten von Nutzen ist. Diese Ansicht vertritt Experte N ebenfalls in der Befragung: „[…] in der Software integriert man so Popups mit Erklärungen, wo draufsteht, wie jetzt gewisse Dinge einzugeben sind, wenn es Zahlen oder irgendwelche anderen Parameter sind“ (Interview N, Pos. 214–216).

Es besteht Grund zur Annahme, dass die Dokumentationssoftware von Anfang an benutzerfreundlich gestaltet sein sollte. Dadurch steigt wahrscheinlich die Akzeptanz gegenüber der elektronischen Patientenakte und infolgedessen wird die Arbeit der Mitarbeitenden erleichtert. Dies sieht auch Experte N ähnlich: „[…] wenn man diese Software entsprechend so gestaltet, dass die selbsterklärend ist“ (Interview N, Pos. 117-118).

Neben der Benutzerfreundlichkeit können den Mitarbeitenden bei Fragen und Problemen vermutlich Hilfetools Unterstützung bieten. Diese Meinung teilt auch Experte N: „[…] zusätzlich noch Tools installieren, die gewisse Schritte erklären“ (Interview N, Pos. 116).

6.16. Betreuung der elektronischen Patientenakte und ihrer Systeme

Die elektronische Patientenakte muss 24 Stunden am Tag, sieben Tage die Woche und 365 Tage im Jahr von Fachleuten betreut werden, da das Krankenhaus rund um die Uhr im Einsatz ist (Klinikum Ingolstadt GmbH, o.J.a). Diese Ansicht teilt auch Experte H: „[…] 24 Stunden rund um die Uhr, 365 Tage im Jahr“ (Interview H, Pos. 133). Die Experten O, N, M, L, K und A kommen zu einer ähnlichen Ansicht wie Experte H, dass die Betreuung der elektronischen Patientenakte ‚24/7‘ erfolgen muss.

Auch Experte B äußert den Wunsch eines ‚24/7‘-Supports, macht aber klar, dass dies nicht durchführbar ist. Hierbei spielt die Wirtschaftlichkeit wieder eine Rolle:

> *„Es kommt zwar immer der Wunsch auf nach "ich kann dann irgendwo anrufen", aber das werden wir nicht leisten können. Man kann tagsüber irgendwo schon anrufen, aber ich kann nicht nachts um zehn Uhr, weil einer nicht weiß, wie er einen Arztbrief freigibt, ein Helpdesk anbieten. Da gehen wir leider auf Seite der Anwender in so eine konsumorientierte Erwartungshaltung. "Wenn ich jetzt ein Problem habe, dann muss da einer für mich da sein." Andersrum: Da ist etwas da, was ich mir dann anschaue. Da muss ich also klar davor warnen. Es gibt keinen Anbieter, wo man 24 Stunden anruft und der einem lächelnd erzählt, wie man das Produkt bedient“ (Interview B, Pos. 322–330).*

Es ist davon auszugehen, dass die Betreuung der digitalen Patientenakte außerhalb der regulären Servicezeiten, in den Nachtstunden oder an Feiertagen mit einem Bereitschafts- oder Rufdienst bewältigt werden kann. Diese Ansicht vertritt auch Experte A: „[…] sowas wie ein Bereitschaftsdienst, der eben auch nachts angerufen werden kann, weil wir ja in einem Bereich arbeiten, in dem 24 Stunden gearbeitet wird und somit auch der Zugriff denjenigen gewährt werden muss, die nachts arbeiten“ (Interview A, Pos. 143–146). Auch hier sind die Experten C, E, J, K und N ähnlicher Meinung.

Dennoch liegt es auch hier nahe, dass die Inanspruchnahme der Fachkräfte in Rufbereitschaften und Bereitschaftsdiensten begrenzt sein sollte. Dies kann höchstwahrscheinlich dadurch ermöglicht werden, wenn bereits im Vorhinein die Zuständigkeiten der Mitarbeitenden festgelegt werden. Auch Experte E nimmt diesen Standpunkt ein: „Diese Zuständigkeiten müssen geklärt werden, sodass man im Falle eines Problems sofort den richtigen Mitarbeiter ansprechen kann“ (Interview E, Pos. 244–246).

Des Weiteren besteht die Vermutung, dass verschiedene Priorisierungsgruppen von Problemen definiert werden müssen. Dies sieht auch Experte I so: „[…] vorab definieren, welche Probleme bzw. welche Prioritäten an Problemen denn auftreten können“ (Interview I, Pos. 368–369). Es ist davon auszugehen, dass anhand dieser Gruppen das zu behandelnde Problem der Dringlichkeit eingestuft und bei Bedarf am nächsten Tag zu den regulären Servicezeiten bearbeitet werden kann. So können Probleme der Prioritätengruppe 3 (z.B. nicht-zeitkritische Probleme) durchaus am nächsten Morgen bearbeitet werden (Interview I, Pos. 370–372). Demgegenüber ist es naheliegend, dass Probleme die der Prioritätengruppe 1 angehören, sprich dringende und gefährdende Probleme, unverzüglich bearbeitet und den Mitarbeitenden Hilfe angeboten werden sollte. Experte I hat dazu eine ähnliche Meinung: „[…] ein Prio-1-Thema hat, dann sollte sichergestellt werden, dass es auch im Rahmen einer Hilfsbereitschaft zum Beispiel jemanden gibt, der auch Auskunft zu diesen Themen oder zu diesen Problemen geben kann“ (Interview I, Pos. 373–375).

Experte F äußert in seinem Interview die Ansicht, dass für kleine Probleme eine Wartezeit von ein bis drei Stunden in Ordnung ist, während prozessstörende Schwierigkeiten sofort oder spätestens nach einer halben Stunde behoben werden sollten (Interview F, Pos. 214–216).

Die Analyse hat auch gezeigt, dass der Prozess der Meldung (beispielsweise in einem Ticketsystem) möglichst einfach strukturiert sein sollte. Dieser Meinung ist auch Experte F:

> *„[…] darf kein Prozess sein, der auch recht aufwändig ist für die Berufsgruppen, sondern es muss irgendwie auch ein automatisierter Prozess sein, wo man sagt, ich habe jetzt hier ein Problem und dann kann ich das auch online übermitteln und dann kümmert sich auch jemand darum“ (Interview F, Pos. 204–207).*

Wenn Rufbereitschaften oder Bereitschaftsdienste zur Betreuung der digitalen Systeme zur Verfügung gestellt werden, müssen die Mitarbeitenden höchstwahrscheinlich auch entsprechend vergütet werden. Es ist davon auszugehen, dass eine gute Bezahlung deren Motivation fördert. Dies sieht auch Experte J so: „Also das ist ein ganz wichtiger Punkt, dass das auch entsprechend dann vergütet wird, um diese Mitarbeiter bei der Stange zu halten“ (Interview J, Pos. 266–268). Seine Erfahrung hat nämlich gezeigt, dass die internen IT-Mitarbeitenden Supportleistungen außerhalb der regulären Servicezeiten bereitwilliger als externe Dienstleister durchführen:

> *„Unsere Erfahrung ist, dass die Bereitschaft, sich auch in den Wochenenden und in den Nachtstunden um unsere Systeme zu kümmern, bei den eigenen Mitarbeitern um vielfaches höher ist, auch wenn sie nicht Bereitschaftsdienst haben und unklar ist, ob sie es jemals vergütet bekommen, als bei externen Anbietern. Also das muss man ganz klar sagen. Auch wenn wir zum Teil Verträge mit externen Anbietern über 24 Stunden, sieben Tage die Woche haben, ist die Bereitschaft, nachts sich wirklich eines Problems anzunehmen, bei den externen Anbietern dramatisch schlechter, und deswegen würde ich auch immer davor warnen, dass alles in fremde Hände zu geben“ (Interview J, Pos. 268–276).*

6.17. Vulnerabilität von elektronischen Patientenakten

Durch die Digitalisierung der Datensätze ist davon auszugehen, dass die elektronischen Patientenakten vulnerabler gegenüber Cyberangriffen sind als papiergebundene Akten. Diese Meinung vertritt auch Experte F: „Gründe dafür sind erst mal, dass sie elektronisch sind und nicht mehr auf Papier. Und alles, was elektronisch ist, kann irgendwie angegriffen werden“ (Interview F, Pos. 224–225). Zu einem ähnlichen Schluss kamen die Experten C, G und O.

Eine andere Ansicht haben die Experten N und J. Sie sind sich nicht sicher, ob elektronische Patientenakten tatsächlich vulnerabler gegenüber Cyberangriffen sind (Interview N, Pos. 235–236; Interview J, Pos. 283).

Hingegen sind sich die Experten B und K einig, dass digitale Patientenakten nicht anfälliger und verletzlicher gegenüber Cyberangriffen sind (Interview B, Pos. 344; Interview K, Pos. 305–306).

Dass auch Krankenhäuser nicht vor Hackerangriffen geschützt sind, beweist unter anderem der Vorfall von Düsseldorf im Jahr 2020 (Kucera, 2020). Auch Experte N

bestätigt ähnliche Vorfälle: „Das ist ein sehr schwieriges Thema, weil es gibt ja auch schon Hackerangriffe auf Krankenhäuser“ (Interview N, Pos. 196–197).

Die Analyse zeigt, dass die technische Entwicklung der digitalen Patientenakte nicht mit der zügigen technischen Computerentwicklung mithalten kann. Während sich Erstere auf einem niedrigen Niveau befindet, ist Letztere auf einer deutlich höheren Stufe. Dies macht das System vulnerabel, was auch Experte A so sieht:

> *„Ich denke, dadurch, dass diese Digitalisierung der Patientenakte noch gar nicht so weit fortgeschritten ist und noch nicht so lange vorhanden ist in dem Rahmen, in dem wir es haben, und in dieser sich immer schneller entwickelnden Zeit der Computerebene auf Internet und dergleichen“ (Interview A, Pos. 153–156).*

Dass Krankenhäuser vulnerabel sind, scheint zum einen an den mangelhaften Rahmenbedingungen zu liegen, unter denen sie arbeiten müssen. Ähnlich sieht dies auch Experte I in der Befragung: „[…] liegt an den Rahmenbedingungen, also grundsätzlich an den Rahmenbedingungen, in denen Krankenhäuser unterwegs sind“ (Interview I, Pos. 386–387).

So herrschen in deutschen Krankenhäusern zumeist schlechte finanzielle Rahmenbedingungen. Es wird bisher zu wenig Geld für die Sicherheit im Bereich der Digitalisierung ausgegeben (Sieger, 2021). Diese Ansicht teilt auch Experte J: „[…] für die IT-Sicherheit in Deutschland bisher zu wenig Geld ausgegeben worden ist, und zwar dramatisch zu wenig Geld ausgegeben wird“ (Interview J, Pos. 289–290).

Auch die Tatsache, dass Krankenhäuser aufgrund der in ihnen zu behandelnden vulnerablen Personengruppen erpressbar sind, lässt die Wahrscheinlichkeit für Cyberangriffe steigen (Perseus Technologies GmbH, 2020). Es ist davon auszugehen, dass ein Hackerangriff das Leben der Erkrankten gefährden kann oder sogar ein tödlicher Ausgang möglich ist. Dies sieht auch Experte D so:

> *„Und ich sage jetzt mal, die Auswirkungen, die so ein Angriff haben kann, möglicherweise auf Leib und Leben von Patienten, macht natürlich ein Krankenhaus besonders erpressbar. Da geht es nicht wie vielleicht bei anderen Firmen erstmal um Produktionsstopp oder um finanziellen Verlust, sondern auch möglicherweise direkt um Menschenleben, wie auch immer, weil die Betreuungs- und Versorgungsprozesse oder die Arbeitsprozesse natürlich dann gefährdet sind, die mit Patienten zusammenhängen“ (Interview D, Pos. 279–285).*

Die Verfügbarkeit vieler sensibler Daten macht das Krankenhaus ebenfalls zu einem potenziellen Angriffsziel (Perseus Technologies GmbH, 2020). Auch Experte K ist dieser Meinung: „Das heißt, es muss lukrativ sein. Patientendaten sind in dem Sinne lukrativ, weil es einfach viele sind, Bankdaten zum Beispiel sind lukrativ, weil ich eventuell Kohle abschöpfen kann oder auch wieder sensible Informationen“ (Interview K, Pos. 309–312).

Es ist auch anzunehmen, dass Cyberkriminelle in der heutigen Zeit wesentlich spezialisierter als in der Vergangenheit sind. Diesen Standpunkt vertritt auch Experte

N: „Klar, man weiß, Hacker sind jetzt immer sehr kreativ. Die finden wahrscheinlich irgendwo schon ihre Mittel und Wege“ (Interview N, Pos. 239–240). Sie suchen vermutlich immer neue und schwierigere Herausforderungen, meist ohne sich dabei Gedanken über die Konsequenzen zu machen. Experte A teilt diese Meinung: „Und eben auch Hacker sich, glaube ich, oftmals einen Spaß daraus machen, zu schauen, wie knacke ich ein System, ohne gar nicht darüber nachzudenken [sic], was damit passiert, was sie gerade tun“ (Interview A, Pos. 156–159).

Die Vermutung liegt nahe, dass die Vulnerabilität zunimmt, wenn die elektronische Patientenakte und deren Systeme nachlässig betreut werden. Dies sieht auch Experte N ähnlich: „Also ganz schlecht ist es, wenn das irgendwo nachlässig betreut wird. Also das ist undenkbar eigentlich, also das muss schon sichergestellt sein“ (Interview N, Pos. 242–244).

Zudem ist davon auszugehen, dass die Verletzlichkeit steigt, wenn veraltete Technik verwendet wird. Dies liegt daran, dass es zu Organisationsfehlern im Lifecycle-Management der digitalen Technologien kommt. Unter Lifecycle-Management versteht man die Betreuung eines Systems von der Konzeptionierung bis hin zur Stilllegung/Entsorgung (Pahl et al., 2007). Auch Mausa (2015) erwähnte in ihrer Arbeit zur Risikoanalyse von Tunnelleitzentralen ein mangelndes Lifecycle-Management.

Diese Aussage unterstreicht auch Experte I:

> *„[…] Stand der Technik oder der Stand der IT-Infrastruktur, der entspricht nicht dem Stand der freien Wirtschaft, sage ich jetzt mal. Das heißt, es werden sehr viele Systeme sehr lange in Betrieb gehalten, auch unter dem Punkt ‚never change a running system‘. Das heißt, es ist eine zum Teil sehr veraltete, auch schon End-of-Life- oder End-of-Service-betriebene IT-Infrastruktur vorhanden, die natürlich aus diesem Grund heraus schon sehr verwundbar ist“ (Interview I, Pos. 387–393).*

Deshalb ist es wichtig, die Technik auf dem aktuellen Stand zu halten und sie fachlich zu betreuen. Auch Experte N sieht dies ähnlich: „Also man sollte immer den Stand der neuesten Technik, was Patientendaten und Patientenakten und so weiter anbelangt, aufrechterhalten“ (Interview N, Pos. 237–238).

Ein nicht vorhandenes Risikobewusstsein bei Mitarbeitenden macht die elektronische Patientenakte verletzlicher (Brockhaus, 2021). So ist davon auszugehen, dass unbekannte E-Mailanhänge von Beschäftigten geöffnet werden, ohne dass sie sich der Gefahr bewusst sind. Eine ähnliche Meinung hat auch Experte O: „[…], dass mit den Daten einfach sehr vorsichtig umgegangen wird und vielleicht nicht alles, was interessant klingt, angeklickt wird“ (Interview O, Pos. 140–142). Experte I äußert vergleichbare Ansichten.

Auch die fehlenden Ressourcen zum Schutz vor cyberterroristischen Angriffen stellen einen vulnerabilitätssteigernden Faktor dar (Krüger-Brand, 2016). Dieser Ressourcenmangel macht sich unter anderem im personellen Bereich bemerkbar (Sieger, 2021). Dies sieht auch Experte I kritisch: „[…] Ressourcenausstattung in diesen Bereichen sehr stiefmütterlich behandelt wird. Das heißt, es gibt zu viele

Aufgaben für zu wenig Mitarbeiter. Das heißt, das verschleppt natürlich auch ein regelmäßiges Patchen von Systemen oder auch Schließen von Sicherheitslücken“ (Interview I, Pos. 394–397).

Es ist auch naheliegend, dass die mangelhafte oder fehlende Hard- und Software sich in Hinblick auf die Vulnerabilität negativ auswirkt. Diese Ansicht vertritt auch Experte H.

Durch die Vielzahl von elektronischen Endgeräten sowie von Mitarbeitenden steigt die Vulnerabilität ebenfalls (Perseus Technologies GmbH, 2020). Diese Aussage wird durch den Experten J unterstützt: „[…], dass ein Krankenhaus einfach extrem viele Mitarbeiter hat und extrem viele Endgeräte und dass nicht alles mit irgendwelchen Kontrollen abgesichert werden kann“ (Interview J, Pos. 292–294). Experte J gibt an, dass eine lückenlose Überwachung zum Schutz der elektronischen Patientenakte trotz aller Sicherheitsmechanismen nicht möglich ist. (Interview J, Pos. 294–295).

In der Vergangenheit kam es in Krankenhäusern immer wieder zu negativen Vorfällen im Bereich der Cybersicherheit (Kucera, 2020; Ludwig, 2016). Es ist aber davon auszugehen, dass nicht nur Krankenhäuser, sondern auch Unternehmen aus anderen Branchen, die mit sensiblen Daten arbeiten, bereits Opfer von Cyberkriminalität geworden sind. Dies sieht auch Experte M so: „Ich glaube, das ist ein großes Problem, aber ich weiß nicht, ob das ein größeres Risiko ist, dass man auf elektronische Patientenakten zugreifen kann. Es gibt andere Firmen, die arbeiten schon viel länger mit sensiblen Daten“ (Interview M, Pos. 167–169).

Nichtsdestotrotz kann angenommen werden, dass nur wenige Zwischenfälle in Verbindung mit der Cybersicherheit in Krankenhäusern an die Öffentlichkeit gelangt sind (Kucera, 2020). Diese Aussage bestätigt Experte B: „Es wird in der Branche ungern darüber geredet, was denn wirklich passiert ist. Das Thema mit Düsseldorf oder Lukas-Krankenhaus in Neuss, das sind alles die Dinge, die ans Licht der Öffentlichkeit gekommen sind, oder jetzt bei uns Fürth“ (Interview B, Pos. 344–347).

Die IT-Sicherheit ist ein eigenes spezielles Fachgebiet im Bereich der Informatik und bedarf eines spezialisierten IT-Technikers. Diese Meinung vertritt auch Experte B: „Faktisch muss man IT-Sicherheit als neues Themengebiet akzeptieren, Leute einstellen, die sich auch nur darum kümmern. Das ist was anderes als der klassische IT-Techniker. Ich glaube, nur dann werden wir den Krieg gewinnen“ (Interview B, Pos. 363–365). Es ist naheliegend, dass sich der IT-Techniker in der Sicherheitsabteilung um die sicherheitstechnischen Belange kümmert. Diese Aussage wird durch den Experten E unterstützt: „wir haben ja unsere IT-Sicherheitsabteilung. Also da gibt es einen Mitarbeiter, der sich ausschließlich um solche Sachen kümmert“ (Interview E, Pos. 267–269).

Die Schulung und Sensibilisierung der Mitarbeitenden kann die Vulnerabilität der elektronischen Patientenakte ebenfalls verringern (Brockhaus, 2021). Diese Ansicht vertritt auch Experte E: „[…] die Leute darauf zu sensibilisieren und zu schulen“ (Interview E, Pos. 270). Jeder einzelne Mitarbeitende ist Teil der Sicherheitsmaßnahmen und leistet seinen Beitrag: „[…] jeder Einzelne steht ja in der Verantwortung, einen Beitrag dazu zu leisten“ (Interview E, Pos. 274–275).

Es wirkt naheliegend, dass ein wesentlicher in der IT-Sicherheit zu verankernder Grundsatz darin besteht, dass Probleme lösungsorientiert behandelt werden müssen. Vermutlich ist es unabdingbar, dass die Mitarbeitenden wissen, wie sie im Falle eines IT-Ausfalls den Betrieb weiter aufrechterhalten können. Nur so scheinen sich die die Probleme auch lösen zu lassen. Dies sieht auch Experte B so:

> *„Und wir werden den Krieg auch gewinnen, wenn man einen Totalschaden endlich mal akzeptiert. Das tun wir nicht. Ich glaube, da haben wir eine falsche Denke. Wir glauben immer, wir schützen uns vor dem Schaden. Man muss das andersrum sehen. Ich sollte mal im Kopf durchdiskutieren: Ich habe einen Schaden. Wie kriege ich das Krankenhaus wieder hoch von null? Also das Thema grüne Wiese, Backup, Geschäftsvorfall, Fortsetzung, das wären so eher die Themen. Nicht immer nur hoffen, dass man sich verteidigt, sondern einen Schaden auch mal zulassen und im Kopf zu Ende zu denken“ (Interview B, Pos. 365–373).*

6.18. Weitere Gründe für den Ausfall der IT-Struktur

Neben Cyberangriffen gibt es eine Vielzahl von möglichen Gründen für den Ausfall der IT-Struktur. Die folgenden Antworten zeigen weitere Ursachen, die höchstwahrscheinlich für den Ausfall der IT-Struktur und damit der elektronischen Patientenakte verantwortlich sein können. Sie können aus Abbildung 6.4 entnommen werden.

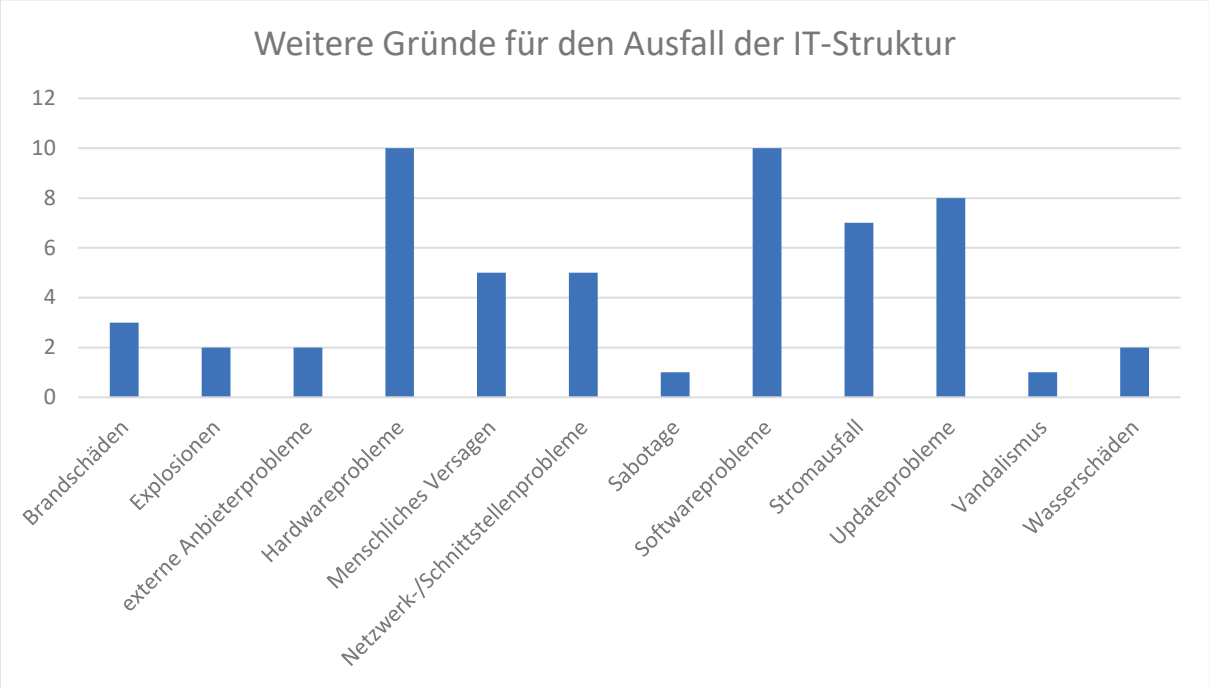


Abbildung 6.4: Weitere Gründe für Ausfälle der IT-Struktur

6.19. Auswirkungen bei Ausfall der IT-Struktur

Da ein digitalisiertes Krankenhaus stark von seiner IT-Struktur abhängig ist, kann deren Ausfall katastrophale Folgen für das Krankenhaus und dessen Betrieb haben (Perseus Technologies GmbH, 2020). Diese Aussage wird auch durch den Experten I unterstützt: „[…] prinzipiell ein Gesamtausfall der IT in einem Krankenhaus hat

natürlich massive Auswirkungen auf den gesamten Ablauf“ (Interview I, Pos. 450–451). Aber auch die Experten K, G, C, B und A sind ähnlicher Meinung wie Experte I.

Es ist davon auszugehen, dass die Auswirkungen eines Ausfalls der IT-Struktur so weit reichen können, dass der gesamte Betrieb und vor allem der Notfallbetrieb zum Erliegen kommen. Diese Ansicht hat auch Experte M: „Also unter Umständen kann das ein ganzes Krankenhaus lahmlegen“ (Interview M, Pos. 184). Die Experten O, N, L, E und C vertreten ebenfalls den Standpunkt, dass ein Ausfall der IT das Krankenhaus zum Stillstand bringt und eine Versorgung der Erkrankten nicht mehr gewährleistet werden kann.

Es liegt die Vermutung nahe, dass die Konsequenzen des IT-Ausfalls auch von dessen Ausmaß und den betroffenen Bereichen abhängig sind. Dies sieht auch Experte I so:

> *„[…] kommt auch ganz darauf an, ob es sich jetzt um einen Gesamtausfall handelt oder um einen Teilausfall. Wenn wir jetzt mal vom Worst-Case-Szenario ausgehen und es gibt einen Gesamtausfall der IT, dann kommt es sicherlich auch nochmal darauf an, in welchem medizinischen Bereich man gerade sich befindet oder der Patient sich befindet“ (Interview I, Pos. 437–441).*

Wichtig ist dabei zu erwähnen, dass das System nicht einsatzbereit und benutzbar ist, solange nicht mit hundertprozentiger Gewissheit ausgeschlossen werden kann, dass der Hacker noch im System ist. Auch Experte A hat diese Meinung:

> *„Ich denke, sobald eine Akte digitalisiert ist und ein solcher Cyberangriff stattgefunden hat, ist die Frage, in welchem Rahmen man die Daten noch schützen kann, ohne auch die interne Informationsverwaltung offenzulassen. Weil die Frage immer ist: Dieser Hackerangriff ist ja nicht nur eine Sache von fünf Minuten, sondern ob der noch auf dieses System geschalten ist und weiterhin Zugriff darauf hat. Und ich glaube, man sollte wirklich einen Riegel vorschieben und sagen, bis das Problem gelöst ist darf nichts mehr weiter dokumentiert oder getan werden, um eben zu vermeiden, dass weitere Daten rausgehen“ (Interview A, Pos. 165–172).*

Bei einem Ausfall der IT kann die Sicherheit des Erkrankten und seiner Gesundheit gefährdet werden (Deutsche Presseagentur, 2019). Es kann angenommen werden, dass dessen Versorgung durch den fehlenden Zugriff auf die digitale Patientenakte nicht mehr fortgeführt werden kann. Dies sieht auch Experte E so: „[…] sicherlich im ersten Moment führt es zu Problemen in der Patientenversorgung, kann sogar auch die Patienten gefährden“ (Interview E, Pos. 294–295). Ähnliche Meinungen werden von den Experten O, L, und B vertreten.

Es ist davon auszugehen, dass es bei einem Ausfall der IT-Struktur im schlimmsten Falle zu einer Falschbehandlung des Erkrankten kommen kann. So besteht vermutlich die Gefahr, dass durch den fehlenden Zugriff auf die Patientenakte Medikamente falsch verabreicht werden. Dies beurteilt auch Experte O sehr kritisch: „[…] einfach irgendwelche Veränderungen der Medikamente, die im System vom Arzt eingetragen

worden sind, der Pflege aber nicht weitergegeben wurden und dadurch falsche Medikamente verabreicht werden“ (Interview O, Pos. 173–175). Auch Experte H betont die Gefahr der Falschmedikation.

Eine weitere Annahme ist die Gefahr, dass Operationen falsch stattfinden, da eine Identifikation durch die fehlenden Daten aus der Patientenakte nicht mehr ohne Probleme möglich ist. Diese Gefahr sieht auch Experte O als realistisch: „[…] Operationen dramatischerweise falsch stattfinden“ (Interview O, Pos. 176).

Es ist darüber hinaus anzunehmen, dass die Gefahr besteht, einen anaphylaktischen Schock auszulösen, wenn dokumentierte Allergien nicht mehr einsehbar sind. Diese Aussage wird durch den Experten O unterstützt: „[…] Allergien, die im System eingetragen sind, bei Untersuchungen Kontrastmittel gegeben wird, wo nicht gewusst wird, dass eine Allergie besteht“ (Interview O, Pos. 177–179).

Im Falle einer Falschbehandlung kann der Betroffene gegenüber dem Krankenhaus vermutlich Haftungsansprüche geltend machen. Dies befürchtet auch Experte J: „[…] haftungsrechtliches Problem natürlich, wenn dadurch Patienten zu Schaden kommen“ (Interview J, Pos. 332–333). Experte J gibt zudem an, dass die Falschbehandlung ebenfalls weitere jurisitische Auswirkungen mit sich bringen kann (Interview J, Pos. 335–336).

Es ist anzunehmen, dass alle im Krankenhaus verwendeten elektronischen Endgeräte eine Software im Hintergrund benötigen, um arbeiten zu können. Naheliegend ist, dass bei einem Ausfall der IT die Gefahr besteht, dass die elektronischen Endgeräte nicht mehr genutzt werden können. Dies sieht auch Experte N so: „Oder vielleicht gibt es Softwares, die notwendig sind, um gewisse Medizingeräte zu betreiben, dann kann das natürlich schon eine Beeinträchtigung gerade in der Routine sein“ (Interview N, Pos. 260–262). So ist es möglich, dass Laborgeräte aufgrund des IT-Ausfalls nicht mehr funktionsfähig sind (Interview C, Pos. 495).

Bei einem Ausfall der IT-Struktur können außerdem Informationen verloren gehen, da diese nicht digital dokumentiert werden können. Dieses Problem sieht auch Experte G: „Aber natürlich gehen in der Zeit viele Informationen verloren bzw. kann nicht vernünftig weitergearbeitet werden“ (Interview G, Pos. 191–192).

Des Weiteren ist anzunehmen, dass ein IT-Ausfall dafür sorgt, dass sich die Prozesse verzögern. Dies bestätigt Experte F: „[…] dadurch die Prozesse verzögern“ (Interview F, Pos. 242). Dies liegt vermutlich daran, dass nicht mehr auf die Daten in der elektronischen Patientenakte zugegriffen und damit gearbeitet werden kann. Auch Experte K sieht dies ähnlich: „[…] auf die grundlegenden Daten, die ich zum Arbeiten brauche, nicht zugreifen kann, keine neuen Daten hinzufügen kann, keine Änderungen einpflegen kann, keine aktuellen Vitalparameter einlesen kann und wiederverwenden kann“ (Interview K, Pos. 338–341).

Es bleibt zu vermuten, dass bei einem fehlenden Zugriff auf die Patientenakte auch der Zugriff und die Sichtbarkeit der Station und deren Belegung nicht mehr möglich ist. Daraus lässt sich ableiten, dass im Falle eines internen Notfalls keine Meldung über

die aktuell im Haus liegenden Erkrankten mehr erfolgen kann. Dies sieht auch Experte I als problematisch:

> *„[…] nicht nur während des Ablaufs, sondern auch damit einher geht zum Beispiel, dass die Stationen keine Sichtbarkeit mehr haben: Welche Patienten sind denn gerade auf der Station anwesend? Welche Patienten werden verlegt? Das heißt, man wird auch blind im eigenen Haus“ (Interview I, Pos. 451–455).*

Es ist davon auszugehen, dass die Arbeitsbelastung bei einem IT-Ausfall zunimmt, da viele Tätigkeiten manuell durchgeführt werden müssen und die Mitarbeitenden darin nicht routiniert sind. Diese Ansicht vertritt auch Experte K:

> *„Und allein das sorgt ja auch schon eigentlich für Einschränkungen, weil A ich Dinge plötzlich wieder manuell tun muss, wenn ein System ausfällt, und ich B dafür aber vielleicht gar nicht mehr entsprechend qualifiziert bin, weil ich das das letzte Mal in meiner Ausbildung gemacht habe und seither nie wieder benötigt habe“ (Interview K, Pos. 347–351).*

Eine weitere Auswirkung eines IT-Ausfalls kann darin bestehen, dass die Kommunikation im Unternehmen eingeschränkt ist. Da die Telefonanlagen vermutlich über die IT-Struktur laufen, stehen sie bei einem Ausfall ebenfalls nicht zur Verfügung. Dies sieht auch Experte C: „[…] Kommunikationswege letztendlich dann sehr stark eingeschränkt sind“ (Interview C, Pos. 510–511).

Ein Ausfall der IT-Struktur kann einen Reputationsschaden für das Krankenhaus bedeuten. Dieser wird höchstwahrscheinlich schlimmer, wenn es infolge des Ausfalls zu einer Gefährdung oder Schädigung eines Erkrankten gekommen ist (Cohnen, o.J.). Eine ähnliche Meinung vertritt Experte J: „[…] Reputationsschaden natürlich. Wenn das in die Presse kommt, dass ein Krankenhaus wegen IT-Problemen nicht arbeiten kann, das ist immer unschön“ (Interview J, Pos. 328–329). Experte A sieht ebenfalls den Ruf der Klinik in Gefahr, wenn es zu einem Ausfall der IT kommt und dadurch der Betrieb beeinträchtigt wird.

Es kann ebenfalls von monetären Folgen ausgegangen werden, wenn Erkrankte durch einen Ausfall nicht mehr in das Krankenhaus aufgenommen werden können. Diese Gefahr sieht auch Experte I: „[…] direkt zu finanziellen Auswirkungen oder Budgetausfällen, wenn keine Patienten mehr aufgenommen werden können oder wenn zum Beispiel gewisse Sachen gar nicht mehr abgerechnet werden können oder gar nicht dokumentiert werden“ (Interview I, Pos. 460–463).

Die finanziellen Einbußen gelten vermutlich auch für die Behandlung von Notfallpatienten. Da das Krankenhaus bei einem Ausfall der IT-Struktur üblicherweise von der Notfallversorgung abgemeldet wird, können wahrscheinlich auch keine Notfallpatienten aufgenommen werden. Dies teilt auch Experte I: „[…] von der Notfallversorgung abmelden, bis man eben eine Einschätzung der aktuellen Lage hat, um dann auch die Patientenbetreuung und die Patientensicherheit auch gewährleisten zu können“ (Interview I, Pos. 447–449). Durch diese Abmeldung können

Notfallpatienten auch nicht mehr abgerechnet werden. Experte J betont dies ebenfalls und führt weitere Bereiche auf, in denen bei einer Krankenhausabmeldung finanzielle Nachteile entstehen: „[…] finanzielles Problem. Weil üblicherweise, wenn so ein Ausfall passiert, wird man das Krankenhaus abmelden von der Notfallversorgung, wird elektive Patienten abbestellen, wird nicht notfällige Operationen absagen müssen. Das heißt, das ist ein finanzieller Schaden, der entsteht“ (Interview J, Pos. 324–327).

Es sollten bereits vor einem Ausfall der IT-Struktur Vereinbarungen mit den Kostenträgern getroffen werden, wie die Abrechnung im Falle eines langfristigen Ausfalls stattfinden kann. Es muss angenommen werden, dass über einen längeren Zeitraum keine Dokumentationen mehr geführt werden können und die erbrachte Leistung auch nicht über das elektronische System abgerechnet werden kann. Dies würde für das Krankenhaus höchstwahrscheinlich einen immensen finanziellen Schaden bedeuten. Experte B teilt diese Meinung:

> *„Das muss man im Vorfeld besprechen und sagen: Was würde das bedeuten? Kann man so einem Krankenhaus, auch wenn es Patienten behandelt, ohne Abrechnung Geld geben? Aber alles ab 14 Tagen wird wirklich bedrohlich fürs Haus, weil A die Leistung gar nicht mehr erbracht wird, damit auch nicht mehr abgerechnet wird“ (Interview B, Pos. 391–394).*

Für die Praxis lässt sich daraus ableiten, dass es von Vorteil wäre, bei einem Ausfall der IT-Struktur und der infolgedessen fehlenden Abrechnung der erbrachten Leistung eine Pauschalvergütung mit den Kostenträgern zu vereinbaren.

Andere Krankenhäuser wurden bereits Opfer von Cyberattacken (Kucera, 2020). Dazu führt Experte J aus: „Umgekehrt muss man sagen, nachdem wir das von ganz vielen Häusern haben, würde man damit nicht mehr ganz alleine stehen. Also man ist nicht mehr der erste Dumme, der dann dieses Problem hat“ (Interview J, Pos. 329–332). Daraus kann für die Praxis geschlossen werden, dass ein Austausch mit den bereits betroffenen Krankenhäusern stattfinden sollte, um von deren Erfahrungen im Umgang mit Cyberattacken oder Ausfällen der IT-Struktur zu profitieren.

Wenn das Krankenhaus nach dem Ausfall der IT-Struktur wieder in Betrieb genommen wird, ist dies vermutlich mit viel Arbeitsaufwand verbunden. Unter anderem kann dies daran liegen, dass alle analogen Dokumentationen, die während des Ausfalls entstanden sind, aufwendig digitalisiert und den entsprechenden Erkrankten zugewiesen werden müssen. Auch Experte I sieht dies als Problem:

> *„Und auf der anderen Seite natürlich auch die Dokumentation, die währenddessen entsteht, die muss auch wieder digitalisiert werden. Das heißt, der Wiederanlauf nach so einem Gesamtausfall, der ist natürlich auch immens arbeitsintensiv, das auch wieder zu organisieren und zu gestalten“ (Interview I, Pos. 455–458).*

Ein Experte gibt zu bedenken, dass ein Krankenhaus ab dem sechsten Tag seines Stillstandes nicht wieder ohne Hilfe in den Normalzustand gebracht werden kann: „[…] gibt es sogar Studien, die sagen: Wenn ein Krankenhaus nach fünf Tagen nicht wieder

langsam hochkommt, dann wird es das aus eigener Kraft auch nicht mehr schaffen“ (Interview B, Pos. 385–387).

Jedem Mitarbeitenden muss bewusst sein und er muss auch dahingehend sensibilisiert werden, dass es immer zu einem Cyberangriff oder einem Ausfall der IT-Struktur kommen kann (Perseus Technologies GmbH, 2020). Damit können wahrscheinlich lebensbedrohliche Zustände bei den Erkrankten einhergehen. Es ist ratsam, bei den Mitarbeitenden und im gesamten Unternehmen ein Risikobewusstsein zu schaffen und vorzuleben. Experte B unterstützt diese Ansicht mit einer ähnlichen Meinung:

> *„Aber genauso gut weiß man: Wenn ein Flugzeug abstürzt, wird es auch keiner überleben. Deswegen fliegt man ja trotzdem. Also auch da wieder das Plädoyer, den Schaden zulassen und dann ehrlicherweise sagen: Ja, wir werden Opfer bringen müssen. Weil alles andere wäre verlogen und Augenwischerei, zu glauben, wir können uns vor sowas hundertprozentig schützen“ (Interview B, Pos. 401–405).*

6.20. Ausfallkonzepte

Bei der Implementierung und dem Betrieb einer elektronischen Patientenakte ist es vermutlich von Anfang an unumgänglich, ein entsprechendes Ausfallkonzept für den Fall zur Hand zu haben, dass die elektronische Patientenakte nicht verfügbar ist. Diese Ansicht vertritt auch Experte I: „Das heißt, man sollte sich auch frühzeitig mit der Rückfallebene, wenn das System nicht zur Verfügung steht, auseinandersetzen“ (Interview I, Pos. 196–198). Die Experten B, E, F, G, H, I, J und N sind ähnlicher Meinung und plädieren für ein Ausfallkonzept.

Es ist anzunehmen, dass die oberste Priorität bei einer Cyberattacke darin besteht, die Sicherheit der Erkrankten weiterhin zu gewährleisten. Dies sieht auch Experte O ähnlich: „wenigstens die Patientensicherheit im Falle eines Hackerangriffs, solange der stattfindet, gewährleistet ist“ (Interview O, Pos. 190–192).

Zudem ist es höchstwahrscheinlich unabdingbar, dass die Operabilität des Krankenhauses weiterhin gegeben ist. Auch Experte G betont dies: „Und dafür muss aber gesorgt werden, dass dann trotzdem weitergearbeitet werden kann, rund um die Uhr“ (Interview G, Pos. 198–199).

Es ist davon auszugehen, dass es im Falle einer Cyberattacke ausreichend ist, dass die Operabilität des Krankenhauses zumindest auf niedrigem Niveau garantiert ist, sodass die wichtigsten Behandlungen weitergeführt werden können. Diese Ansicht vertritt auch Experte L: „[…] auf jeden Fall so sicher sein, dass der Betrieb zumindest auf Sparflamme, also das Wichtigste, weiterlaufen kann“ (Interview L, Pos. 184–185).

Ein weiteres Ziel bei einem Ausfall der IT-Struktur besteht höchstwahrscheinlich darin, dass die Ursachen für den Ausfall schnellstmöglich behoben werden, damit die volle Operabilität des Krankenhauses wieder gewährleistet ist. Diese Aussage wird durch den Experten K unterstützt: „Es muss in jedem Fall schnellstmöglich jede Kraft dafür

eingesetzt werden, den Ausfall so schnell wie möglich zu beheben“ (Interview K, Pos. 362–363).

Damit das Ausfallkonzept von allen Mitarbeitenden verwendet werden kann, ist es notwendig, dass sie darin geschult werden und Übungsmöglichkeiten haben. Dabei liegt die Vermutung nahe, dass sowohl Vollzeitkräfte als auch Arbeitnehmer in Teilzeit in gleichem Maße an entsprechenden Fortbildungen teilnehmen müssen. Dies sieht auch Experte F:

> *„[…] jeder darüber Bescheid weiß, informiert ist und dass das auch mal eingeübt ist und nicht, dass zum Beispiel Teilzeitkräfte damit dann auch nicht umgehen können. Also das muss dann schon auch geübt sein und im Kopf auch sein von den Mitarbeitenden, dass es das gibt“ (Interview F, Pos. 254–257).*

Damit sollte jeder in der Lage sein, das Ausfallkonzept im Ernstfall zu benutzen. Diese Ansicht vertritt Experte H ebenfalls: „Das Ausfallkonzept sollte so sein, dass jeder in der Lage ist, damit umzugehen“ (Interview H, Pos. 158–159).

Es ist anzunehmen, dass bei den Mitarbeitenden nur durch eine regelmäßige Schulung eine Routine bei der Verwendung der Ausfallkonzepte entsteht. Deshalb scheint es unumgänglich, dass halbjährlich eine Pflichtveranstaltung zur Schulung und Übung des Konzeptes organisiert wird. Diese Ansicht teilt auch Experte H: „[…] und dass jeder in dieses Ausfallkonzept mindestens zweimal jährlich geschult ist, damit er weiß, wie das funktioniert“ (Interview H, Pos. 159–160). Diese Veranstaltungen sollten als Pflichtveranstaltungen durchgeführt werden, da die Mitarbeitenden im Ernstfall schnellstmöglich wissen müssen, was sie zu tun haben.

Bei der Erstellung von Ausfallkonzepten ist das Wissen darüber unerlässlich, welche Art von Konzepten benötigt werden und ob diese individualisiert oder generalisiert vorliegen müssen. So liegt die Annahme nahe, dass für Ausfälle der Labor-IT Ausfallmappen mit den wichtigsten Laboranforderungen und vorgefertigten Etiketten auf den Stationen vorgehalten werden. Ähnlicher Ansicht ist auch Experte K: „Was ich kenne, sind Ausfallmappen, die einfach viele Dinge, die man normalerweise am Bildschirm tun kann, in Papierform abbilden, sodass ich zumindest angeleitet werde“ (Interview K, Pos. 358–361).

Auch Experte F sieht das Ausfallkonzept in Papierform als Möglichkeit: „Digital wäre natürlich das Wichtigste dann vor Ausfällen. Da muss man natürlich wieder auf Papier- oder bestimmte Ausfallkonzepte zurückgreifen können. Wenn man digitalisiert, dann ist natürlich das Papier auch von Vorteil im Haus“ (Interview F, Pos. 66–68).

Es ist anzunehmen, dass das Vorhalten von Backups dem Krankenhaus dazu dienen kann, bei einem Ausfall der IT-Struktur weiterhin Daten im Backupsystem zu haben. Dies führt vermutlich dazu, dass das Krankenhaus weiterhin operabel bleibt. Eine vergleichbare Ansicht vertritt auch Experte J: „[…] zumindest Zusammenfassungen in regelmäßigen Abständen dann auch in anderen Systemen abgelegt werden, auf die ich dann zugreifen kann“ (Interview J, Pos. 141–143).

Es ist naheliegend, dass die Backups in regelmäßigen und sinnvollen Abständen gesichert werden müssen, um die aktuellen Daten zur Verfügung zu haben. Dies sieht auch Experte A so: „Also ich denke, es müsste in einem bestimmten Rhythmus, den man sich wirklich überlegen müsste, immer wieder wie ein Backup erfolgen von den kompletten Akten der Patienten“ (Interview A, Pos. 224–226).

Um besser für interne Schadensszenarien (z.B. einen Brand) gewappnet zu sein, kann es von Vorteil sein, wenn die Backupdaten zudem an einem externen Ort redundant gelagert werden. Diese Ansicht vertritt auch Experte A:

> *„Ich denke, wenn es diese Backups geben würde, eben auf einem externen Bereich, wäre das Ganze gar nicht so schwierig. Weil man ja jederzeit sagen könnte, keine Ahnung, diese Diskette ist nicht bei uns im Haus, wo es brennt, sondern ganz woanders, und ich kann jederzeit darauf zugreifen. Und somit interessiert mich dieser Brand bezugnehmend auf die Daten nicht, weil das Ganze ja woanders zwischengespeichert ist“ (Interview A, Pos. 246–251).*

Daraus lässt sich für die Praxis ableiten, dass die elektronische Patientenakte in regelmäßigen Abständen auf einem extern gelegenen Backupserver gesichert werden sollte – beispielsweise einmal am Tag. So kann auch garantiert werden, dass die Daten bei einem internen Zwischenfall weiterhin zur Verfügung stehen.

Auch die Vorhaltung eines Notstromaggregats für Stromausfälle kann höchstwahrscheinlich eine sinnvolle Ergänzung zum Ausfallkonzept darstellen. Dass die Notstromversorgung dabei eine bedeutsame Rolle spielt, sieht auch Experte N so (Interview N, Pos. 250).

Bei planbaren und kurzzeitigen Ausfällen der IT-Struktur (z.B. Wartungsarbeiten) ist es naheliegend, die Dokumentation nach der Wartung durchzuführen. Diese Meinung vertritt auch Experte I:

> *„[…] geplanten Wartungsfenstern, da reden wir über einen recht kurzen Zeitraum, dass diese Systeme dann nicht zur Verfügung stehen. Ich denke, da lässt sich in der Ablauf- und Arbeitsorganisation das gut abbilden, dass eben diese Dokumentation zu einem anderen Zeitpunkt oder später eben nachgeholt wird“ (Interview I, Pos. 473–477).*

Es muss allerdings beachtet werden, dass die Gefahr des Informationsverlustes bei der späteren Dokumentation hoch ist.

Trotz des Ausfalls der IT-Struktur oder des fehlenden Zugriffs auf das System ist anzunehmen, dass die datenschutz- und arbeitsrechtlichen Vorgaben weiterhin eingehalten werden. Auch hier sollten die Mitarbeitenden vermutlich intensiv dahingehend geschult werden, dass Verstöße gegen geltendes Recht oder arbeitsrechtliche Vorgaben Probleme mit sich bringen können. Diese Ansicht teilt auch Experte A: „Ich finde es schwierig. Wir wissen alle, wie es läuft, wenn es so ist, was datenschutzrechtlich und arbeitsrechtlich absolut nicht sein soll“ (Interview A, Pos. 234–235).

6.21. Ausfallkonzept: Notfallakte

Es liegt nahe, dass den Mitarbeitenden bei einem Ausfall die Informationen und Daten vorliegen sollten, die kurz davor verfügbar waren. Diese ‚eingefrorenen' Daten sollten höchstwahrscheinlich als eine Art Notfallakte dienen, um die Versorgung des Erkrankten weiterhin gewährleisten zu können. Diese Ansicht vertritt auch Experte A im Interview:

> *„Eine sehr schwierige Frage. Wenn nämlich nichts mehr in Papierform vorhanden ist, ist auch die Frage, wie weitläufig sich diese Auswirkungen zeigen. Kann man vorhandene Daten noch irgendwie in Papierform bringen, um damit arbeiten zu können mit einer Notfallakte, wie auch immer? Oder sind bestimmte Daten vorhanden, die immer wieder abgerufen werden können über Archiv, eine Cloud, was auch immer man nehmen will? Dass man sagt, man hat zumindest den Ist-Zustand bis kurz vor dem Ausfall, um mit Daten arbeiten zu können" (Interview A, Pos. 206–212).*

Auch Experte D ist ähnlicher Meinung.

Die Notfallakte sollte nur die wichtigsten Daten enthalten, die für die Notfallversorgung der Erkrankten erforderlich sind. Es ist anzunehmen, dass die Stammdaten des Erkrankten hinterlegt sein sollten, sodass seine Identifikation stattfinden und eine Verwechslung ausgeschlossen werden kann. Dies sieht Experte A im Interview ebenfalls so: „Definitiv müssen die kompletten Stammdaten des Patienten vorhanden sein, um eine Verwechslung zu vermeiden" (Interview A, Pos. 215–216). Vermutlich sollten auch die Diagnosen, die durchgeführten Untersuchungen und die bisherige bestehende Medikation des Erkrankten Bestandteil der Notfallakte werden und dort eine entscheidende Rolle spielen:

> *„Dann auch die Diagnosen. Nicht nur die Diagnosen, warum der Patient aktuell hier ist, sondern auch die alten Diagnosen, um eben bestimmte Dinge unterstützend bei der Therapie mit einbringen zu können. Die gelaufenen Untersuchungen, die Medikation auf jeden Fall gehört mit dazu, die aktuelle" (Interview A, Pos. 216–220).*

6.22. Ausfallkonzept im Falle einer Evakuierung

Es ist anzunehmen, dass die Evakuierung des Krankenhauses einen Spezialfall eines Ausfallkonzeptes darstellt. Hierbei ist dahingehend zu unterscheiden, aus welchem Grund evakuiert wird. Auch Experte I sieht dies so: „Evakuierung des Hauses? Ist natürlich jetzt auch die Frage aufgrund welchen Ereignisses" (Interview I, Pos. 502–503).

Die Planungen für die Evakuierung des Krankenhauses sollten bereits im Voraus durchgeführt werden. Es ist davon auszugehen, dass so überprüft werden kann, ob die benötige Hardware und Software in der Noteinrichtung vorhanden ist oder ob noch entsprechende technische Einrichtungen angeschafft werden müssen. Auch hier wird

die Aussage durch den Experten E unterstützt: „[…] es muss Hardware vorhanden sein“ (Interview E, Pos. 331).

Die Vorausplanung soll den Verantwortlichen höchstwahrscheinlich bei der Überprüfung helfen, ob die in der geplanten Noteinrichtung vorhandenen Systeme miteinander kompatibel sind. Dies sieht auch Experte H ähnlich:

> *„Aber in der Turnhalle weiß ich auch nicht, ob die Turnhalle über einen PC ausgestattet ist, und wenn die tatsächlich einen PC haben sollte, weiß ich ja nicht, ob die Hardware und die Software kompatibel ist mit unserer elektronischen Patientenakte“ (Interview H, Pos. 172–176).*

Zudem ist es naheliegend, bereits in der Vorplanung Zugänge und Zugriffsberechtigungen im Notfallsystem einzurichten. Eine vergleichbare Ansicht hat Experte E: „[…] Zugänge müssen eingerichtet werden, sodass man zurückgreifen kann“ (Interview E, Pos. 331–332).

Es ist des Weiteren anzunehmen, dass datenschutzrechtliche Fragestellungen im Voraus geklärt werden können, die dann spätestens bei einer Evakuierung aufkommen. Auch Experte H stellt sich die Frage nach dem Datenschutz: „Naja, die Frage ist doch: Darf ich dem Rettungsdienst die elektronische Patientenakte überhaupt mitgeben, ja oder nein?“ (Interview H, Pos. 171–172).

Es besteht Grund zur Annahme, dass eines der wichtigsten Ziele bei einer Evakuierung des Krankenhauses sein sollte, dass trotzdem weiterhin digital gearbeitet werden kann. Eine vergleichbare Meinung hat Experte F: „Also ich würde es auch weiter digital sehen dann auch, wenn es Turnhallen wären“ (Interview F, Pos. 288–289).

Bei einer Krankenhausevakuierung ist es höchstwahrscheinlich unumgänglich, dass die Erkrankten in Noteinrichtungen (z.B. in Turnhallen) weiter versorgt werden. Aus diesem Grund ist davon auszugehen, dass alle am Erkrankten tätigen Mitarbeitenden Zugriff auf sämtliche Daten der Erkrankten haben müssen. Dies sieht auch Experte L im Interview ähnlich: „[…] auch Zugriff eigentlich auf die gesamte Akte haben. Weil du kannst sonst einen Patienten nicht richtig versorgen“ (Interview L, Pos. 192–193).

Im Falle einer Evakuierung scheint es sinnvoll zu sein, dass die Pflegekräfte erweiterten Zugriff auf alle Erkrankten bekommen, um deren Versorgung gewährleisten zu können. Auch Experte O vertritt diese Meinung:

> *„[…] sollten vor allem Pflegekräfte bzw. das gesamte Personal einen erweiterten Zugriff auf eigentlich alle möglichen Daten bekommen, um einfach hier ... gut, ‚was auszudrucken‘ ist immer schwierig gesagt bei so einem Fall. Aber einfach darauf zugreifen zu können. Weil mir bringt es nichts, wenn ich nur auf das Pflegerische zugreifen kann, den Patienten aber komplett versorgen soll, sei es auch mit Medikamenten, ich aber keinen Zugriff darauf habe“ (Interview O, Pos. 235–240).*

Vermutlich ist die Unterscheidung relevant, ob es sich um eine kurzzeitige oder längerfristige Versorgung der Erkrankten in Noteinrichtungen handelt. Bei einer kurzzeitigen Versorgung der Erkrankten unter 24 Stunden ist es mit großer Wahrscheinlichkeit ausreichend, dass die Mitarbeitenden Informationen über Diagnosen und Therapien erhalten. Dies sieht auch Experte L im Interview ähnlich: „Wenn es sich um eine kurzfristige Evakuierung handelt, 24 Stunden, dann reicht das, wenn sie die Diagnose, die Therapie und wie es halt weitergeht wissen“ (Interview L, Pos. 193–195). Bei längerfristigen Versorgungen über 24 Stunden sollten den Mitarbeitenden höchstwahrscheinlich alle relevanten und benötigten Daten zur Verfügung gestellt werden. Diese Aussage unterstützt auch Experte L in seiner Befragung: „wenn es sich um eine langfristige Versorgung handelt, dann müssten die entweder Zugriff auf die Patienten kriegen oder sie müssten die Patientendaten übermittelt kriegen, die für sie notwendig sind“ (Interview L, Pos. 195–198).

Bei einer Evakuierung in umliegende Noteinrichtungen und der damit möglichen Gefährdung der Erkrankten spielt der Datenschutz vermutlich eine untergeordnete Rolle. Es ist anzunehmen, dass das Wohl des Patientenlebens in diesem Fall höher angesiedelt ist als die datenschutzrechtlichen Anforderungen. Dies sieht Experte K ähnlich: „Rechtlich ist es tatsächlich so, dass in dem Fall das Patientenwohl den Datenschutz überlagert“ (Interview K, Pos. 375–376).

Eine der entscheidendsten Maßnahmen im Evakuierungsfall ist wahrscheinlich die Entlassung von Erkrankten, die aus medizinischer Sicht nicht mehr im Krankenhaus behandelt werden müssen, eine der entscheidendsten Maßnahmen ist. Damit soll vermutlich erreicht werden, dass nur die wirklich notwendigen Erkrankten und die am schwersten Erkrankten in der Klinik liegen. Diese Meinung vertritt auch Experte J: „Da wird man ohnehin die Patienten, die halbwegs kraksen können, nach Hause schicken. Es wird sicherlich nur noch um die schwerstkranken Patienten gehen“ (Interview J, Pos. 348–350).

Es liegt nahe, dass bei einer Evakuierung das Vorhalten von dezentralen Backups eine wichtige Rolle spielt. Diese sollten vermutlich an einem anderen bzw. weiteren dezentralen Ort vorhanden sein und überall abgerufen werden können. Dies sieht auch Experte J ähnlich:

> *„Wir haben allerdings unsere Informationen an unterschiedlichen Orten gespeichert. Das heißt also, wenn jetzt unser zentraler Serverraum durch was auch immer, Anschlag oder keine Ahnung, was auch immer, Naturkatastrophen betroffen sein sollte, dann hieße das, dass wir aber noch an einem zweiten Ort die Daten haben, um auf diese zuzugreifen“ (Interview J, Pos. 353–357).*

Auch die Experten N und M haben vergleichbare Ansichten.

Besonders bei einer Evakuierung liegt die Vermutung nahe, dass die Verwendung einer cloud- oder webbasierten Technologie eine Möglichkeit sein kann, um das Ausfallkonzept zu verbessern. Dies sieht auch Experte J:

> *„Tatsächlich verfolgen wir aber noch einen weiteren Aspekt, der im Augenblick geprüft wird und wo uns der Datenschutz allerdings im Augenblick noch Schwierigkeiten macht, das ist das Auslagern in die Cloud. Also tatsächlich beabsichtigen wir durchaus, Daten des Krankenhauses außerhalb des Klinikums und der Stadt Ingolstadt abzulegen, eben um genau für solche Dinge gewappnet zu sein, weil diese noch natürlich mit ihren Ressourcen deutlich besser Daten wiederherstellen können, wenn es Probleme hardware- oder softwaremäßig gab“ (Interview J, Pos. 361–368).*

Es ist davon auszugehen, dass das Cloudsystem im Gegensatz zum bereits bestehenden Krankenhaussystem den Vorteil hat, dass es aus technischer Sicht anders aufgebaut ist. Diese Aussage wird durch den Experten B unterstützt: „Wären wir in der Cloud - und in der Regel sind Cloudstrukturen technologisch komplett anders aufgebaut“ (Interview B, Pos. 436–438). Durch die neue Technologie scheint es möglich, ortsunabhängig auf das Krankenhausinformationssystem zuzugreifen. Der Vorteil liegt nahe, dass die Erkrankten in virtualisierten Organisationseinheiten zugeordnet werden können, zu denen die verantwortlichen Mitarbeitenden Zugang haben. Eine ähnliche Ansicht äußert Experte B:

> *„Aber dann könnte ich sagen, mir ist egal, wo diese Patienten später liegen. Jedes Krankenhaus kriegt den Zugriff auf das nach wie vor vorhandene virtuelle Krankenhausinformationssystem. Und da könnte man sogar überlegen, wenn es in der Cloud läuft, dass ich diesen Patienten verlege, indem ich in meinem KIS eine Org-Einheit mache, nämlich das andere Krankenhaus. Dann führt man faktisch diesen Patienten bei uns weiter oder man gibt denen Zugriff bis zu dem Moment der Akte, wo der Patient das Haus verlassen hat, weil er jetzt woanders liegt“ (Interview B, Pos. 440–447).*

Auch Experte E vertritt eine vergleichbare Meinung.

Wenn es trotz aller Bemühungen dazu kommt, dass die elektronische Patientenakte nicht mehr verfügbar und nutzbar ist oder noch genügend Zeit bis zur Evakuierung vorhanden ist, ist es vermutlich unumgänglich, ein papiergebundenes Ausfallkonzept für die Möglichkeit einer Evakuierung vorzuhalten. Eine ähnliche Meinung hat auch Experte I:

> *„[…] planbares Ereignis ist, also Fliegerbombe wird gefunden, dann hätte man womöglich tatsächlich noch ein paar Tage Zeit, die Dokumentation den Patienten mitzugeben und eben sozusagen in Papierform zumindest einen gewissen Datenbestand zu haben. Und die schwierigsten Patienten, die würde man ja verlegen und dann würden die auch in den Krankenhausinformationssystemen sozusagen der anderen Einrichtungen wieder aufgenommen werden“ (Interview I, Pos. 504–510).*

Experte D plädiert ebenfalls für ein zusätzliches papiergebundenes Ausfallkonzept.

Eine weitere Idee für ein Ausfallkonzept im Rahmen der Evakuierung stellt vermutlich die Verwendung eines QR-Codes mit den wichtigsten Patientendaten dar. Es ist anzunehmen, dass dieser unter anderem an einem Patientenarmband angebracht werden könnte. Mit entsprechenden Endgeräten und einer speziellen Software können die am Erkrankten tätigen Mitarbeitenden einen ersten Zugang zu den wichtigsten Patientendaten haben. Experte F ist ähnlicher Meinung:

> *„[…], dass immer Patientenarmbänder getragen werden und dass darauf vielleicht auch so ein Notfall mit den QR-Codes ist, dass da die wichtigsten Sachen auch darauf vermerkt sind. Also würde ich jetzt mal selber so Zukunft spinnen gerade, dass man so einen QR-Code dann hat, wo dann das Wichtigste dann drauf wäre im Falle des Notfalls, wo dann auch Rettungskräfte von außen darauf mit einem Programm Zugriff hätten“ (Interview F, Pos. 292–297).*

Trotz aller vorbereitender Maßnahmen gilt es auch hier, die Mitarbeitenden dahingehend zu sensibilisieren und darauf vorzubereiten, dass bei einem Ausfall der digitalen Patientenakte im Rahmen einer Evakuierungsmaßnahme im ersten Moment vermutlich keinerlei Patienteninformationen zur Verfügung stehen. Dieses Problem sieht auch Experte F in der Befragung: „Schwieriger wird es dann wahrscheinlich, wenn die Infrastruktur auch nicht zur Verfügung steht und das ist dann keine Cloudlösung. Dann hat man natürlich erstmal keine Informationen über den Gesundheitszustand, das Behandlungsregime und Ähnliches“ (Interview I, Pos. 521–524).

6.23. Nutzung von innovativen Techniken und Konzepten

Ein innovativer Faktor für die Zukunft wird höchstwahrscheinlich die benutzerfreundliche Bedienung der Systeme werden. Dies sieht auch Experte B in der Befragung ähnlich:

> *„[…] User-Experience-Design haben Sie jetzt nicht angesprochen. Sie kommen über das Thema Sicherheit, Verfügbarkeit und wie führt man sowas ein. Man könnte mal trefflich darüber diskutieren - da habe ich eine Bachelorarbeit gemacht dazu: Wie muss denn so eine Oberfläche ausschauen, damit ein Mensch sie bedienen kann? Also wir haben uns über andere Sehgewohnheiten unterhalten, der Lernvideos statt dem Buch. Vielleicht unterhalten wir uns auch mal über eine neue Oberflächenart, wo Menschen sagen, ich verstehe das jetzt“ (Interview B, Pos. 460–466).*

Es liegt nahe, die Oberfläche der Dokumentationssysteme so zu gestalten, dass sie Betriebssystemen von Smartphones oder Tablets (z.B. Apple oder Microsoft) ähneln. Experte B vertritt in der Befragung ebenfalls die Meinung, dass die Oberfläche benutzerfreundlich gestaltet werden soll, da dadurch die Lust an der Verwendung der Systeme steigt:

> *„Das war eine Revolution, wie Software ausschaut. Auch das könnte man überlegen. Ist das interessant? Nicht umsonst gibt es ja von großen Anbietern, von Microsoft bis SAP, sogenannte Style-Guides, wo steht: Wenn du eine Software schreibst für mein Ökosystem, haben wir eine gewisse Erwartung an Form und Farbe. Könnte man mal machen. Also Software, die einem gefällt, bedient man in jedem Falle angenehmer“ (Interview B, Pos. 507–512).*

Experte B macht einen weiteren Vorschlag für die Gestaltung einer Oberfläche für Krankenhausinformationssysteme: „Muss man das vielleicht mal in Einklang bringen, also muss man mal den Mut haben, zu sagen, wir machen Oberflächen in einem KIS in der Pflegeplanung, als ob die von Apple wären“ (Interview B, Pos. 473–475).

Zudem ist es naheliegend, Icons in das Dokumentationssystem zu implementieren, um eine intuitive Bedienung des Systems zu ermöglichen. Es ist davon auszugehen, dass davon besonders nichtmuttersprachliche Mitarbeitende profitieren und der Umgang mit dem System erleichtert wird. Diese Meinung vertritt auch Experte B:

> *„Oder auch Fremdsprachlichkeit. Nehmen Sie mal gängige Oberflächen an, die sind alle in Deutsch. Und habe ich deutsche Mitarbeiter, die wirklich jeden Fachbegriff verstehen? Kann ich das nicht mit einer Symbolik? In der Bachelorarbeit ging es um eine Bildsprache. Kann ich nicht Software bedienen, wo eigentlich jeder aus einem westlichen Kulturkreis versteht: Ah, das ist das Symbol Mann, Frau oder das ist das Symbol Exit oder was auch immer. Ich meine, es gibt ja Handyprogramme, die bedienen Sie intuitiv, wenn Sie zehn der gleichen Art mal genommen haben“ (Interview B, Pos. 493–501).*

Einen anderen Ansatz stellt vermutlich die Verwendung von Gesichtserkennung und Fingerabdrücken in Kombination mit Passwörtern dar. Hierbei könnte aber die Gefahr bestehen, dass ein Fingerabdruck kompromittiert wird. Dies stellte auch Experte B fest: „Gesichtserkennung, Fingerabdruck, das sind alles Dinge, wo ich sage: Ja, dann mach doch. Dann musst du wenigstens kein Kennwort mehr verwenden. Nachteil, wenn mal ein Fingerabdruck kompromittiert ist, dann kann ich mir keinen neuen besorgen“ (Interview B, Pos. 482–485).

Zudem ist es naheliegend, dass der Zugang zur elektronischen Patientenakte vereinfacht werden kann, indem der Dienstausweis aufgelegt und das System mit einer PIN zusätzlich erleichtert freigeschaltet wird. Die Lust an der Anwendung von Technologie spielt auch für den Experten B eine entscheidende Rolle: „Dann bin ich beim Lustprinzip, sage: ‚Leg dein Dienstausweis auf‘ Kannst du machen. Und dann brauchst du bloß noch eine vierstellige PIN-Nummer. Das ist vielleicht einfacher als immer länger werdende Passworte. Also das Thema Lust zur Anwendung sollte man mal thematisieren“ (Interview B, Pos. 490–493). Durch die Kombination mehrerer Verfahren besteht die Vermutung, dass eine Multi-Faktor-Authentifizierung erreicht werden kann.

Auch die Anwendung von Virtual- oder Augmented-Reality-Konzepten in der Pflege könnte vermutlich einen innovativen Ansatz darstellen, um die Digitalisierung und den

Spaß an der Pflege weiterzuentwickeln. Es ist beispielsweise anzunehmen, dass VR- oder AR-Technologie die Pflegefachkraft bei der Medikamentengabe unterstützen kann. Dies sieht auch Experte B so:

> *„Wir müssen uns beschäftigen mit Virtual Reality. Was kann ich alles machen mit solchen Brillen? Ich habe nicht zu Ende gedacht, aber warum kann eine Krankenschwester nicht eine Augmented-Reality-Brille aufhaben und wenn sie dem Patienten die Tabletten hinlegt, wird im Display eingespielt, in welcher Dosierung der Patient die eigentlich nehmen müsste. Dann hat sie alles im Blick“ (Interview B, Pos. 512–517).*

7. Diskussion der Ergebnisse

Die Experten haben eine Vielzahl von Aussagen zur elektronischen Patientenakte getroffen. Im nachfolgenden werden diese mit dem bekannten Stand der Technik verglichen.

Bei der Implementierung und dem Betrieb der elektronischen Patientenakte gaben die Experten an, dass gesetzliche Vorgaben zu berücksichtigen sind. Ihrer Ansicht nach spielt beispielsweise die Europäische Datenschutzgrundverordnung eine Rolle, da mit Hilfe der elektronischen Patientenakte personenbezogene Daten verarbeitet werden. Diese Aussage deckt sich mit Artikel 1 Abs. 1 der Europäische Datenschutzgrundverordnung: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten“ (EUR-OP, 2016, : 2). Neben den datenschutzrechtlichen Belangen spielt nach Expertenmeinung auch die Pflicht zur elektronischen Dokumentation eine entscheidende Rolle. So verpflichtet §630f Abs. 1 BGB zur Dokumentation der Behandlung:

> *„Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen“ (BMJV & BfJ, 2021, : 170).*

Neben der Anschaffung der Softwareprodukte muss auch die benötigten Hardwareprodukte angeschafft werden. Dies führt nach Meinung der Experten dazu, dass bei der Implementierung einer elektronischen Patientenakte mit hohen Investitionskosten gerechnet werden muss. Eine Studie des DKI und BDO (2019) kam ebenfalls zu der Ansicht, dass die hohen Investitionskosten zu einem Problem für die Krankenhäuser wird (DKI & BDO, 2019).

Die Experten gaben in ihren Befragungen an, dass die heutige technische Ausstattung in deutschen Krankenhäusern nicht ausreichend ist (z.B. Datensicherheit). Neben den bestehenden unzureichenden Ausstattungen bringt nach Pohlmann (2019) die fortschrittliche Entwicklung der Digitalisierung im Pflegebereich und in den Krankenhäusern auch Probleme mit sich. Pohlmann sieht die Probleme der Datensicherheit vor allem in den Schwachstellen der Softwareprodukten:

> *„Die Fehlerdichte – die Anzahl der Softwarefehler pro 1 000 Zeilen Code – liegt bei qualitativ hochwertiger Software heute im Schnitt bei 0,3. Da gängige Betriebssysteme und größere Anwendungen mehr als zehn Millionen Zeilen Code haben, sind hier im Schnitt 3 000 Software-Fehler zu finden“ (Pohlmann, 2019, : 56).*

Eine weitere Herausforderung besteht nach Ansicht der Experten in der Schulung der Mitarbeitenden. Die Unterschiede zwischen der elektronischen Patientenakte und der heutigen verwendeten Papierakte ist enorm. Zudem muss auf Grund der Komplexität der elektronischen Patientenakte eine umfangreiche und mehrmalige Benutzerschulung, da diese anders als Papierakten nicht mehr intuitiv erlernt werden können. Fiedler und Kaeding (2021) identifizierten bereits Schulungsprobleme im Bereich der elektronischen Patientenakte und bieten verschiedene Schulungsmöglichkeiten für unterschiedliche Zielgruppen an (Fiedler & Kaeding, 2021).

Die Zuweisung von Benutzer- und Rollenprofile sehen die Experten als Notwendig an, um den unberechtigten Datenzugriff auf Patientenakten zu unterbinden und den Schutz der personenbezogenen Patientendaten zu gewährleisten. Auch Kropp (2016) vertritt die Meinung, dass ein Berechtigungskonzept sinnvoll ist:

> *„Allerdings birgt das gleichzeitig auch ein hohes Risiko in puncto Datenschutz und stellt hohe Anforderungen an das Berechtigungskonzept des Krankenhausinformationssystems (KIS). Über dieses System erfolgen in der Regel alle Zugriffe auf die Patientendaten. Ein solches Berechtigungskonzept gewährt oder verweigert den einzelnen Nutzern des KIS spezifische Zugriffsrechte auf bestimmte Daten“ (Kropp, 2016, : 4).*

Neben den Benutzer- und Rollenprofilen ist es nach Meinung der Experten auch sinnvoll, dass die Mitarbeitenden von jedem Ort im Krankenhaus auf die Daten zugreifen. Diese Ansicht vertritt ebenfalls Kropp (2016):

> *„So können Patientendaten jederzeit und an jedem beliebigen Ort innerhalb des Krankenhauses abgerufen werden. Diese hohe Verfügbarkeit der Patientendaten bringt einen immensen Mehrwert und ist vor allem die Grundlage für effiziente Behandlungsentscheidungen in der unmittelbaren medizinischen Versorgung von Patienten“ (Kropp, 2016, : 4).*

Die Mehrheit der Befragten gab in den Interviews an, dass eine 24/7/365 technische Betreuung für den Betrieb der elektronischen Patientenakte notwendig ist. Es ist jedoch nicht belegbar, dass eine 24/7/365 technische Betreuung zu einer besseren Systemperformance führt. Es ist jedoch davon auszugehen, dass bei einer 24/7/365 Betreuung, Probleme frühzeitiger detektiert werden und somit schneller behoben werden. Dies kann dazu führen, dass sich die Systemperformance verbessert.

Auf die Frage wie sich der Zugriff auf die Patientendaten durch den Rettungsdienst und die Pflegekräfte im Falle einer Evakuierung des Krankenhauses mit anschli8eßender Versorgung der Patienten in umliegenden Noteinrichtungen (z.B. Turnhallen) gestaltet, kam es durch die Experten zu keiner eindeutigen Aussagen. Die heutigen Krankenhausalarm- und Einsatzpläne berücksichtigen den Einsatz elektronischer Patientenakten im Ernstfall (z.B. Evakuierungsfall) nicht und bieten

keine Handlungsempfehlung an (Deutsche Gesellschaft für KatastrophenMedizin e.V., 2006).

Die elektronische Patientenakte lösen nach heutigem Stand der Technik die aktuell verwendete papiergebundene Patientenakte noch nicht ab. So macht es nach Ansicht der Experten durchaus Sinn, die papiergebundene Patientenakten als Ausfallkonzept zu Verfügung zu haben, wenn die elektronischen Redundanzen versagen. Dies ist vor allem im Falle eines Hackerangriffs von Vorteil, wenn die elektronische Patientenakte kompromittiert ist. Diese Erfahrung musste das Universitätsklinikum Düsseldorf im September 2020, nachdem ein Hacker die gesamte Krankenhaus-IT zum Ausfall brachte und dadurch der Betrieb des Krankenhauses massiv beeinträchtigt wurde (Kucera, 2020).

8. Empfehlungen für die Praxis und die Forschung

Das Ziel dieser Arbeit sollte darin bestehen, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert zu erarbeiten und daraus Handlungsempfehlungen ableiten zu können. Dieses IT-gestützte Dokumentationssystem soll dazu dienen, die Bearbeitung elektronischer Patientenakten im Pflegealltag unter Beachtung gesetzlicher, operativer, wirtschaftlicher Aspekte zu ermöglichen. Die Erwartung an solch ein System besteht darin, sowohl die Verfügbarkeit als auch die Anfälligkeit gegenüber natürlichen und menschlichen Ereignissen zu verbessern.

Das Ziel sollte mit Hilfe eines qualitativen Forschungsdesigns erreicht werden. Im Rahmen dieses Forschungsdesigns wurden 15 Interviews mit Experten aus dem Klinikum Ingolstadt geführt. Die Interviews fanden leitfadenbasiert statt. Die Aufnahme der Interviews fand tontechnisch statt und welche anschließend transkribiert wurden. Die Transkripte wurden einer qualitativen Inhaltsanalyse nach (Mayring, 2002) unterzogen.

Auf Basis der Ergebnisse aus Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**, können folgende Implikationen abgeleitet werden:

- **Notwendigkeit:** die Digitalisierung ist Notwendig, um eine bessere Versorgung des Patienten zu gewährleisten.
- **Die ganzheitliche Entwicklung elektronischer Patientenakten ist eine Herausforderung,** da ein Krankenhaus ein vulnerables Umfeld darstellt.
- **Testläufe sind empfehlenswert**, um frühzeitig eventuelle Schwachstellen zu identifizieren.
- **Die Ernennung einer Stabstelle IT-Sicherheit** sorgt für eine reibungslose und dedizierte Gesamtbetreuung des Systems.
- **Die Entwicklung soll Multidisziplinär erfolgen:** alle Berufsgruppen im Krankenhaus sollen mitinvolviert werden.
- **Die Implementierung soll interdisziplinär erfolgen:** die drei großen Bereiche ‚System', ‚Technik', und ‚Finanzen' sollen gemeinsam erarbeitet werden.
- **Die aktive Beteiligung der Mitarbeiter ist erforderlich**, dadurch wird die Akzeptanz und Qualität gesteigert.
- **Die Rechtslage ist komplex**, spezialisierte Fachanwälte müssen in der Entwicklung und im Betrieb miteingebunden werden.
- **Datenschutzbestimmungen müssen gesetzkonform angewendet werden**, dafür muss hinterfragt werden, welche Datenkategorien rollenabhängig bearbeitet werden dürfen.
- **Auch externe Kooperationspartner sollen miteingebunden werden**, um eine reibungslose Mitarbeit gewährleisten zu können.

- **Die Eignung von externen Mitarbeitenden** muss sorgfältig beurteilt werden.
- **Die Implementierungsdauer darf nicht unterschätzt werden**, da diese von zahlreichen und vielfältigen Faktoren beeinflusst wird.
- **Durch elektronische Patientenakten wird für Transparenz gesorgt:** diese kann zu eine positive Fehlerkultur im Unternehmen führen.
- **Die benutzerfreundliche Anordnung der Daten** kann die Arbeit der Mitarbeitenden in schwierigen Situationen ermöglichen.
- **Krankenhäuser müssen eigene finanzielle Mitteln bereitstellen:** Investitionskosten lassen sich nicht über das heutige DRG-System refinanzieren.
- **Kosten können optimiert werden**, indem man die vorhandenen Systeme wartet und die aktuell zu beschaffenden Systemen auf die Eignung für die elektronische Patientenakten überprüft. Auch die Skalierbarkeit muss bedacht werden.
- **Schulungen der Endanwender sind erforderlich** und sollen vom Personal mit besonderer didaktischer Eignung durchgeführt werden.
- **Ein ausgereifter Schulungskonzept muss entwickelt werden**, damit die Mitarbeiter sowohl bei der Einführung als auch langfristig das System optimal bedienen können.
- **Mitarbeitende müssen im Thema Datensicherheit sensibilisiert werden**, da sie ein Teil des Sicherheitskonzepts sind.
- **Daten müssen ununterbrochen verfügbar sein**, da ein Krankenhaus ein vulnerabler Dauerbetrieb ist.
- **Dafür muss für Redundanz gesorgt werden**, da technische Systeme ausfallen oder gewartet werden können. Dennoch ist immer ein Restrisiko vorhanden.
- **Relevante Datenkategorien sind dennoch für die Behandlung wichtig**, obwohl dies eventuell heutige Datenschutzbestimmungen widersprechen kann.
- **Über ein Mindestmaß an Daten für Notfallsituationen** muss entschieden werden.
- **Relevante Prozesse müssen erarbeitet werden**, um die sichere Versorgung der Patienten in Notfallsituationen gewährleisten zu können.
- **Ein adäquates Datensicherheitskonzept ist notwendig**, um die gesetzlichen Anforderungen erfüllen zu können.
- **Genügend Endgeräte sind erforderlich**, damit jeder Mitarbeitende die Möglichkeit hat, mit elektronischen Patientenakten zu arbeiten.

- **Durch eine hohe Integration der Systeme**, kann die Zuverlässigkeit des Endprodukts erhöht werden.
- **Eine gute drahtlose Netzwerkverbindung ist von Nöten**, damit Informationsverluste verhindert werden können.
- **Die Netzwerkverbindung muss gesichert werden**, um die Sicherheit sensibler Daten zu gewährleisten.
- **Turnusmäßige Systemaktualisierungen und -wartungen** sorgen für eine hohe Verfügbarkeit des Systems durch den gesamten Lebenszyklus.
- **Rollen und individualisierte Zugänge müssen implementiert werden,** damit sorgt man für eine transparente und rechtsichere Dokumentation.
- **Eine 24/7/365 Betreuung muss gewährleistet sein**, damit die Aufrechterhaltung des Systems reibungslos läuft.
- **Durch den Einsatz von Key-User** auf den Stationen können Probleme zeit- und kosteneffizient gelöst werden.
- **Die Akkulaufzeit** muss bei der Entscheidung über die Endgeräte besonders berücksichtigt werden.
- **Hygienebestimmungen** müssen bei der Auswahl von Elektronische Endgeräte berücksichtigt werden.
- **Die Vernachlässigung von geeigneten Sicherheitsvorkehrungen**, kann die Lebensqualität der Patienten beeinträchtigen.
- **Zivil- und Strafrechtliche Konsequenzen können erwartet werden,** bei Missachtung etablierter Sicherheitsstandards. Dazu kommen auch Imageschäden.
- **Lange Systemstillstände** können zu erheblichen Konsequenzen führen.
- **Ausfallkonzepte müssen erarbeitet und gelebt werden**, da die Datenverarbeitung im Krankenhausumfeld ein kritischer Prozess darstellt.
- **Papierakten haben noch einen Vorteil**, vor allem für Ausfallkonzepte.
- **Neue Technologieszenarien können entstehen**: das eröffnet zukünftiges Forschungspotential.

Die Limitation dieser Arbeit besteht darin, dass das Untersuchungssetting und die Stichprobe auf die Klinikum Ingolstadt GmbH begrenzt waren. Die Befragung der Experten des Klinikum Ingolstadts stellt nur eine Momentaufnahme dar, welche von den Erfahrungen aus diesem Krankenhaus geprägt sind. Die Ergebnisse können nicht eins zu eins auf andere Krankenhäuser übertragen und verallgemeinert werden.

Diese vorliegende Thematik bietet Möglichkeit für weitere Forschungsvorhaben. So sollten weitere Untersuchungen mit weiteren Krankenhäusern und mehreren Experten durchgeführt werden. So können die Erfahrungen von verschiedenen Krankenhäusern und einer Vielzahl von Experten zusammengetragen werden.

Nach den in dieser Arbeit erarbeiteten Ergebnisse, sollen weiterführende Forschungsarbeiten folgende Aspekte beinhalten:

- **Im Bereich Pflegepädagogik** sollte erarbeitet werden, wie die Mitarbeitenden zu diesem Thema sensibilisiert werden können. Dazu gehören beispielsweise die Erstellung von geeignete Schulungskonzepte.
  Wie die Untersuchung gezeigt hat, spielt die Schulung und Sensibilisierung der Mitarbeitenden eine entscheidende Rolle für die Implementierung und den Betrieb der elektronischen Patientenakte.
- **Die heutigen Krankenhausprozesse** müssen auch für die Einführung der elektronischen Patientenakte angepasst werden.
  Die elektronische Patientenakte bietet zwar eine Unterstützung der heutigen Prozesse, aber es ist unabdingbar, dass diese Prozesse auch modernisiert werden müssen. Die Einführung neuer Technologien kann ein Rahmen bieten, in dem die heutigen Prozesse nochmals evaluiert werden können und gegebenenfalls vorangetrieben werden können.

9. Literaturverzeichnis

Amt für Veröffentlichungen der Europäischen Union. (2016). *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*. Zugriff am 30.11.2020. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02016R0679-20160504

Axel Springer SE. (2020). *Welche Laptop-Größen gibt es? Ein Überblick*. Zugriff am 19.07.2021. Verfügbar unter: https://tipps.computerbild.de/hardware/notebook/welche-laptop-groessen-gibt-es-ein-ueberblick-918837.html

Bayerische Landesärztekammer. (o.J.). *Aufbewahrungspflicht*. Zugriff am 19.07.2021. Verfügbar unter: https://www.blaek.de/arzt-und-recht/aufbewahrung

Bayerische Staatskanzlei. (2007). *Bayerisches Krankenhausgesetz (BayKrG) in der Fassung der Bekanntmachung vom 28. März 2007 (GVBl. S. 288, BayRS 2126-8-G), das zuletzt durch § 1 Abs. 149 der Verordnung vom 26. März 2019 (GVBl. S. 98) geändert worden isz*. Zugriff am 19.07.2021. Verfügbar unter: https://www.gesetze-bayern.de/Content/Document/BayKrG?fontsize=large

Bayerisches Staatsministerium für Gesundheit und Pflege. (o.J.). *Krankenhäuser in Bayern*. Zugriff am 13.03.2021. Verfügbar unter: https://www.stmgp.bayern.de/gesundheitsversorgung/krankenhaeuser/krankenhaeuser-in-bayern/

Brandenburg, H., Panfil, E.-M., Mayer, H., Manzei, A., Schnell, M. W., Schnepp, W. et al. (Hrsg.). (2013). *Pflegewissenschaft 2. Lehr- und Arbeitsbuch zur Einführung in die Methoden der Pflegeforschung* (Pflegeforschung, 2., vollständig überarbeitete Auflage). Bern: Verlag Hans Huber. Verfügbar unter: http://elibrary.hogrefe.de/9783456951607/A

Braun, S. (2017). Arbeiten im Krankenhaus: Wie Sie dem Datenschutz gerecht werden. *Deutsches Ärzteblatt*, *114*(1-2).

Breinich-Schilly, A. (2021). *Digitalisierung ist oft ein großer Kostentreiber*. Zugriff am 19.07.2021. Verfügbar unter: https://www.springerprofessional.de/kostenmanagement/business-analytics/digitalisierung-ist-oft-ein-grosser-kostentreiber/18756574

Brockhaus, A. (2019). *Was ist Informationssicherheit?,* isits AG International School of IT Security. Zugriff am 31.05.2021. Verfügbar unter: https://www.is-its.org/it-security-blog/it-sicherheit-informationssicherheit-cyber-sicherheit-unterschiede

Brockhaus, A. (2021). *Wie Unternehmen trotz Fachkräftemangel die IT-Sicherheit erhöhen*. Zugriff am 20.07.2021. Verfügbar unter: https://www.is-its.org/it-security-blog/fachkraeftemangel-it-sicherheit

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe & Bundesamt für Sicherheit in der Informationstechnik. (2009). *Sektoren und Branchen Kritischer Infrastrukturen*. Verfügbar unter: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html

Bundesamt für Sicherheit in der Informationstechnik. (o.J.a). *Gesetze zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG)*. Zugriff am 23.07.2021. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/it_sig_node.html

Bundesamt für Sicherheit in der Informationstechnik. (o.J.b). *Zwei-Faktor-Authentisierung*. Zugriff am 20.07.2021. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2013). *Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT*. Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2020). *KRITIS-Sektor Gesundheit: Informationssicherheit in der stationären medizinischen Versorgung Rahmenbedingungen, Status Quo, Handlungsfelder. Ergebnisse einer qualitativen Studie*. Bonn. Zugriff am 20.07.2021. Verfügbar unter:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_stationaere_med_Versorgung.pdf?__blob=publicationFile&v=3

Bundesgesundheitsministerium. (2019a). *Gesetzes für mehr Sicherheit in der Arzneimittelversorgung (GSAV)*. Zugriff am 01.11.2020. Verfügbar unter: https://www.bundesgesundheitsministerium.de/gsav.html

Bundesgesundheitsministerium (Bundesgesundheitsministerium, Hrsg.). (2019b). *Terminservice- und Versorgungsgesetz (TSVG)*. Zugriff am 01.11.2020. Verfügbar unter: https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html

Bundesgesundheitsministerium. (2020a). *Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG)*. Zugriff am 01.11.2020. Verfügbar unter: https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html

Bundesgesundheitsministerium. (2020b). *Krankenhauszukunftsgesetz für die Digitalisierung von Krankenhäusern*. Zugriff am 01.11.2020. Verfügbar unter: https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html

Bundesgesundheitsministerium. (2020c). *Patientendaten-Schutz-Gesetz*. Zugriff am 01.11.2020. Verfügbar unter: https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html

Bundeskriminalamt. (o.J.). *Biometrie*. Zugriff am 16.07.2021. Verfügbar unter: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/Biometrie/biometrie_node.html;jsessionid=B8522F65CB44A70C3FFFA4BFEF41DD06.live2302

Bundesministerium der Justiz und für Verbraucherschutz & Bundesamt für Justiz (Bundesamt für Justiz, Bundesministerium der Justiz und für Verbraucherschutz, Hrsg.). (2009). *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG),* Bundesamt für Justiz, Bundesministerium der Justiz und für Verbraucherschutz. Zugriff am 01.11.2020. Verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Bundesministerium der Justiz und für Verbraucherschutz & Bundesamt für Justiz. (2021). *Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S.738), das zuletzt durch Artikel 1 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2133) geändert worden ist,* Bundesministerium der Justiz und für Verbraucherschutz, Bundesamt für Justiz. Zugriff am 16.07.2021. Verfügbar unter: https://www.gesetze-im-internet.de/bgb/BGB.pdf

Bundesministerium des Innern. (2016). *Cyber-Sicherheitsstrategie für Deutschland 2016*. Berlin. Zugriff am 31.05.2021.

Bundesministerium für Wirtschaft und Energie. (2017). *Monitoring-Report Kompakt. Wirtschaft DIGITAL 2017*. Berlin.

Bundesministeriums der Justiz und für Verbraucherschutz & Bundesamts für Justiz. (1871). *Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletztdurch Artikel 29 des Gesetzes vom 7. Juli 2021 (BGBl. I S. 2363) geändert worden ist*. Zugriff am 19.07.2021. Verfügbar unter: https://www.gesetze-im-internet.de/stgb/StGB.pdf

Bundesministeriums der Justiz und für Verbraucherschutz & Bundesamts für Justiz. (1988). *Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20.Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 4 des Gesetzes vom 23. Juni 2021 (BGBl. I S.1982) geändert worden ist*. Zugriff am 19.07.2021. Verfügbar unter: https://www.gesetze-im-internet.de/sgb_5/SGB_5.pdf

Bundesministeriums der Justiz und für Verbraucherschutz & Bundesamts für Justiz. (1998). *Transfusionsgesetz in der Fassung der Bekanntmachung vom 28. August 2007 (BGBl. I S. 2169), das zuletztdurch Artikel 11 des Gesetzes vom 19. Mai 2020 (BGBl. I S. 1018) geändert worden ist*. Zugriff am 19.07.2021. Verfügbar unter: https://www.gesetze-im-internet.de/tfg/TFG.pdf

Bundesministeriums der Justiz und für Verbraucherschutz & juris GmbH. (1987). *Röntgenverordnung in der Fassung der Bekanntmachung vom 30. April 2003 (BGBl. I S. 604), die zuletzt durchArtikel 6 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010) geändert worden ist*. Zugriff am 19.07.2021. Verfügbar unter: https://www4.uni-jena.de/unijenamedia/Bilder/einrichtungen/strahlenschutz/R%C3%B6V+12_14.pdf

Bursig, H.-P. (2019). Cybersicherheit vernetzter Medizinprodukte: Neue Herausforderungen. *Klinik Management aktuell*, *24*(6), 76–77. Zugriff am 13.10.2020.

Cohnen, M. (o.J.). IT-Ausfall im Krankenhaus. *E-Health-Compass*, 4–7. Zugriff am 20.07.2021. Verfügbar unter: https://e-health-com.de/fileadmin/user_upload/dateien/Compass/Compass_IT-Sicherheit_gesamt.pdf

Cwojdzinski, D., Decher, J., Giraud, H., John-Koch, M., Juditzki, I., Kowalzik, B. et al. (2012). *Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus*. Bonn.

Deutsche Gesellschaft für KatastrophenMedizin e.V. (2006). *Hinweise für das Anlegen von Krankenhaus-Alarm- und Einsatzplänen*. Zugriff am 14.08.2021. Verfügbar unter: http://www.dgkm.org/files/downloads/krankenhaus_notfallplanung/Bayerisches_Staatsministerium_des_Innern__Hinweise_fuer_das_Anlegen_von_Krankenhaus-Alarm-_und_Einsatzplaenen.pdf

Deutsche Presseagentur. (2019). *Cyberattacken auf Krankenhäuser: Wenn der Klinikrechner zum Angriffsziel wird*. Verfügbar unter: https://www.handelsblatt.com/technik/it-internet/cyberattacken-auf-krankenhaeuser-wenn-der-klinikrechner-zum-angriffsziel-wird/23945496.html

Deutscher Bundestag. (2015). *Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen,* Deutscher Bundestag. Teil I Nr. 54. Zugriff am 14.10.2020. Verfügbar unter: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27635488%27%5D&skin=pdf&tlevel=-2&nohist=1

Deutsches Institut für Normung. (2011). *Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010); Deutsche Fassung EN 80001-1:2011*. Zugriff am 20.07.2021.

Deutsches Instiut für Normung. (2020). *DIN EN ISO/IEC 27000*. Zugriff am 30.03.2021.

Deutsches Krankenhausinstitut & BDO. (2019). *Das Digitale Krankenhaus*. Zugriff am 16.07.2021.

Dolle, J., Boeske, M., Franz, H., Goetz, C., Haibach, S., Hensel, F.-J. et al. (2004). *Managementpapier "Elektronische Patientenakte"*. Köln. Zugriff am 06.03.2021.

Dörries, M., Gensorowsky, D. & Greiner, W. (2017). Digitalisierung im Gesundheitswesen - hochwertige und effizientere Versorgung. In T. Lux, B. Breil, M. Dörries, D. Gensorowsky, W. Greiner, D. Pfeiffer et al. (Hrsg.), *Digitalisierung im Gesundheitswesen — zwischen Datenschutz und moderner Medizinversorgung* (Bd. 97, S. 692–696). Berlin/Heidelberg: Springer.

Dresing, T. & Pehl, T. (Hrsg.). (2011). *Praxisbuch Transkription. Regelsysteme, Software und praktische Anleitungen für qualitative ForscherInnen* (1. Auflage). Marburg: Eigenverlag.

Dresing, T. & Pehl, T. (Hrsg.). (2018). *Praxisbuch Interview, Transkription & Analyse. Anleitungen und Regelsysteme für qualitativ Forschende* (8. Auflage). Marburg.

Duden. (o.J.). *Vulnerabilität*. Zugriff am 31.01.2021. Verfügbar unter: https://www.duden.de/rechtschreibung/Vulnerabilitaet

Dujat, C. (2014). *Patientenakten sicher langzeit-archivieren*. Zugriff am 17.06.2021. Verfügbar unter: https://www.management-krankenhaus.de/topstories/it-kommunikation/patientenakten-sicher-langzeit-archivieren-0

Ebert, K., Hahn, P., Happe, K., Hetze, P., Hoeftmann, R., Meyer, M. et al. (Gemeinsam für unsere Gesundheit, Hrsg.). (o.J.). *Wie Vernetzung im Gesundheitsbereich gelingen kann. Integration - Kooperation - Digitalisierung*. Zugriff am 17.07.2021. Verfügbar unter: https://www.leopoldina.org/uploads/tx_leopublication/2017_11_Studie_Gesundheitsinitiative.pdf

Elsner, C. & Koch, A. (o.J.). *Künstliche Intelligenz in der Pflege: Anästze und Anwendungsgebiete,* Hochschule der Medien. Zugriff am 16.07.2021. Verfügbar unter: https://ai.hdm-stuttgart.de/downloads/student-white-paper/Winter-1819/KI_in_der_Pflege.pdf

E-mergency AG. (2020). *Risikomanagement verstehen*. Zugriff am 20.07.2021. Verfügbar unter: https://www.e-mergency.ch/de/blog/risikomanagement-verstehen

Engel jun., H. (2018). Digitalisierung in der Medizin: Praxismanagement und Datenschutz. *Journal für Ästhetische Chirurgie*, *11*(3), 146–150. Zugriff am 14.10.2020.

Erwig, B. (2019). IT-Sicherheit: Datenschutz, KRITIS und E-Health-Gesetz. *Klinik Management aktuell*, *24*(4), 42–44. Zugriff am 01.11.2020.

Europäische Union. (2008). *RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern*. Zugriff am 01.11.2020. Verfügbar unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:DE:PDF

European Commission. (2010). *Risk Assessment and Mapping Guidelines for Disaster Management - COMMISSION STAFF WORKING PAPER*. Brüssel. Zugriff am 07.02.2021.

Fekete, A., Hufschmidt, G. & Kruse, S. (2014). Benefits and Challenges of Resilience and Vulnerability for Disaster Risk Management. *International Journal of Disaster Risk Science*, *5*(1), 3–20. https://doi.org/10.1007/s13753-014-0008-3

Fiedler, M. & Kaeding, A. (2021). *Online-Schulungen zur elektronischen Patientenakte (ePA)*. Zugriff am 14.08.2021. Verfügbar unter: https://digitales-gesundheitswesen.de/online-schulungen-zur-elektronischen-patientenakte-epa/

Fracis, R. & Maier, F. (2017). *IT Security studieren - Zeitverschwendung?* Zugriff am 20.07.2021. Verfügbar unter: https://www.computerwoche.de/a/it-security-studieren-zeitverschwendung,3330599

Gesellschaft für Telematikanwendungender Gesundheitskarte mbH. (2019). *ePA - Elektronische Patientenakte*. Zugriff am 01.11.2020. Verfügbar unter: https://www.gematik.de/fileadmin/user_upload/gematik/files/Faktenblaetter/Faktenblatt_ePA_web.pdf

Gläser, J. & Laudel, G. (2006). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* (2., durchges. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Hauser, U. (2014). *Zugriffskontrolle*. Zugriff am 19.07.2021. Verfügbar unter: https://www.scope-and-focus.com/datenschutzberatung/faq/faq-begriffserklaerungen-faq-bdsg/zugriffskontrolle-gem-anlage-zu-9-satz-1-bdsg-erlaeuterung/

Helfferich, C. (2011). *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews* (4. Auflage). Wiesbaden: VS Verlag für Sozialwissenschaften / Springer Fachmedien Wiesbaden GmbH Wiesbaden.

Hieber, M. (2018). Pflegeübergabe: Die Informationsweitergabe muss geübt werden. *Heilberufe*, *70*(7-8), 22. https://doi.org/10.1007/s00058-018-3566-8

Hillienhof, A. (2019). *Krankenhäuser wollen eine Milliarde Euro pro Jahr für Digitalisierung*. Zugriff am 19.07.2021. Verfügbar unter: https://www.aerzteblatt.de/nachrichten/103175/Krankenhaeuser-wollen-eine-Milliarde-Euro-pro-Jahr-fuer-Digitalisierung

Höhl, R. (2020). *Organisierte Angebote GBA beschließt elektronische Dokumentation der Krebs-Früherkennung,* Ärztezeitung. Zugriff am 19.07.2021. Verfügbar unter: https://www.aerztezeitung.de/Politik/GBA-beschliesst-elektronische-Dokumentation-der-Krebs-Frueherkennung-410442.html

Höhne, C. & Lenz, K. (2019). *Versorgungssicherung: Was tun bei einem Stromausfall im Krankenhaus.* 44. Zugriff am 30.10.2020. Verfügbar unter: https://www.aerzteblatt.de/archiv/210611/Versorgungssicherung-Was-tun-bei-einem-Stromausfall-im-Krankenhaus

Holling, C. S. (1973). *Resilience and stability of ecological systems* (Research report / International Institute for Applied Systems Analysis). Laxenburg: IIASA. Accessed 21.02.2021.

International Telecommunication Union, the World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation & NATO Cooperative Cyber Defence Centre of Excellence. (2018). *Guide to Developing a National Cybersecurity Strategy. Strategic engagement in cybersecurity*. Genf.

Kaiser, R. (2014). *Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung* (Lehrbuch). Wiesbaden: Springer VS.

Kebede, M. M. & Pischke, C. R. (2019). Popular Diabetes Apps and the Impact of Diabetes App Use on Self-Care Behaviour: A Survey Among the Digital Community of Persons With Diabetes on Social Media. *Frontiers in Endocrinology*, *10*, 1–14. Accessed 30.11.2020.

Klinikum Ingolstadt GmbH. (o.J.a). *EinBlick*. Zugriff am 16.07.2021. Verfügbar unter: https://www.klinikum-ingolstadt.de/klinik/medizinische-klinik-ii/einblick/

Klinikum Ingolstadt GmbH. (o.J.b). *Fakten*. Zugriff am 13.03.2021. Verfügbar unter: https://www.klinikum-ingolstadt.de/ueber-uns/fakten/

Klinikum Ingolstadt GmbH. (o.J.c). *Stellenangebote*. Zugriff am 13.03.2021. Verfügbar unter: https://www.klinikum-ingolstadt.de/karriere/stellenangebote/

Kropp, H. (2016). *Digitalisierung: Sicherer Schutz von Patientendaten*. Zugriff am 19.07.2021. Verfügbar unter: https://www.aerzteblatt.de/archiv/182630/Digitalisierung-Sicherer-Schutz-von-Patientendaten

Krüger-Brand, H. E. (2016). Medizinische IT-Netzwerke: Cybersicherheit als Herausforderung. *Deutsche Ärzteblatt*, *113*(9), A364-A369. Zugriff am 20.07.2021.

Krüger-Brand, H. E. (Ärzteblätt, Hrsg.). (2018). *Ethische Fragen werden bei der Digitalisierung wichtiger*. Zugriff am 19.07.2021. Verfügbar unter:

https://www.aerzteblatt.de/nachrichten/88774/Ethische-Fragen-werden-bei-der-Digitalisierung-wichtiger

Kruse, S., Abeling, T., Deeming, H., Fordham, M., Forrester, J., Jülich, S. et al. (2019). The emBRACE Resilience Framework. In H. Deeming, M. Fordham, C. Kuhlicke, L. Pedoth, S. Schneiderbauer & C. Shreve (Hrsg.), *Framing Community Disaster Resilience* (S. 79–96). Chichester, UK: John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119166047.ch6

Kucera, M. (2020). Uniklinik Düsseldorf: Cyberangriff verursacht Todesfall. *Klinik Management aktuell*, *25*(10), 6. Zugriff am 13.10.2020.

Lamnek, S. & Krell, C. (2016). *Qualitative Sozialforschung* (6., überarbeitete Auflage). Weinheim, Basel: Beltz.

Lettau, A. & Breuer, F. (Westfälische Wilhelms-Universität Münster, Hrsg.). (o.J.). *Kurze Einführung in den qualitativ-sozialwissenschaftlichen Forschungsstil*. Zugriff am 30.11.2020. Verfügbar unter: https://www.uni-muenster.de/imperia/md/content/psyifp/aebreuer/alfb.pdf

Ludwig, K. (Süddeutsche Zeitung, Hrsg.). (2016). *Wenn Cyberkriminelle ein Krankenhaus lahmlegen,* Süddeutsche Zeitung. Zugriff am 27.10.2020. Verfügbar unter: https://www.sueddeutsche.de/digital/angriff-auf-klinik-das-comeback-des-klemmbretts-1.2912255

Lux, T. & Breil, B. (2017). Digitalisierung im Gesundheitswesen: bessere Versorgungsqualität trotz Kosteneinsparung. In T. Lux, B. Breil, M. Dörries, D. Gensorowsky, W. Greiner, D. Pfeiffer et al. (Hrsg.), *Digitalisierung im Gesundheitswesen — zwischen Datenschutz und moderner Medizinversorgung* (Bd. 97, S. 687–692). Berlin/Heidelberg: Springer.

Mausa, I. (2015). *Risikoanalyse Tunnelleitzentrale. Empfehlungen für eine einrichtungsbezogene Risikoanalyse*. Zugriff am 20.07.2021. Verfügbar unter: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Risikoanalyse_Tunnelleitzentrale.pdf?__blob=publicationFile

Mayer, H. (2018). *Pflegeforschung kennenlernen. Elemente und Basiswissen* (7., überarbeitete Auflage). Wien: Facultas.

Mayring, P. (2002). *Einführung in die Qualitative Sozialforschung*. Weinheim, Basel: Beltz Verlagsgruppe.

Mayring, P. (2015). *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (Beltz Pädagogik, 12., überarb. Aufl.). Weinheim: Beltz. Verfügbar unter: http://content-select.com/index.php?id=bib_view&ean=9783407293930

Mayring, P. (2016). *Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (6., überarbeitete Auflage). Weinheim, Basel: Beltz. Verfügbar unter: http://content-select.com/index.php?id=bib_view&ean=9783407294524

Meuser, M. & Nagel, U. (1991). ExpertInneninterviews - vielfach erprobt, wenig bedacht: ein Beitrag zur qualitativen Methodendiskussion. In D. Garz & K. Kraimer (Hrsg.), *Qualitativ-empirische Sozialforschung. Konzepte, Methoden, Analysen* (S. 441–471). Wiesbaden: VS Verlag für Sozialwissenschaften.

Microsoft. (2020). *So funktioniert's: Azure AD Multi-Factor Authentication*. Zugriff am 20.07.2021. Verfügbar unter: https://www.microsoft.com/de-de/security/business/identity-access-management/mfa-multi-factor-authentication

Pahl, G., Beitz, W., Blessing, L., Feldhusen, J., Grote, K.-H. & Wallace, K. (2007). *Engineering Design. A Systematic Approach* (Third Edition). London: Springer-Verlag London Limited. https://doi.org/10.1007/978-1-84628-319-2

Perseus Technologies GmbH. (2020). *Krankenhäuser im Visier von Cyberkriminellen*. Zugriff am 20.07.2021. Verfügbar unter: https://www.perseus.de/wissen/blog/news/cyberangriffe-aus-krankenhaeuser/

Pohlmann, N. (o.J.). *Authentifikation*. Zugriff am 20.07.2021. Verfügbar unter: https://norbert-pohlmann.com/glossar-cyber-sicherheit/authentifikation/

Pohlmann, N. (2019). IT-Sicherheit im Krankenhaus. Ohne Cybersicherheit gelingt keine nachhaltige Digitalisierung. *Klinik Management aktuell*, *24*(10), 55–59. Zugriff am 13.10.2020.

Pramann, O., Graf, K. & Albrecht, U.-V. (2012). Tablet-PC im Krankenhaus: Hygienische Aspekte beachten. *Deutsche Ärzteblatt*, *109*(14), A706-A707. Zugriff am 20.07.2021. Verfügbar unter: https://www.researchgate.net/publication/234007393_Tablet-PC_im_Krankenhaus_Hygienische_Aspekte_beachten

Rahmati-Georges, A. & Groves, C. (2018). *Datenintegrität : Was ist das und wie ist sie aufrecht zu erhalten?* Zugriff am 20.07.2021. Verfügbar unter: https://blog.varonis.de/datenintegritat-was-ist-das-und-wie-ist-sie-aufrecht-zu-erhalten/

Reichardt, C. & Gastmeier, P. (2013). *„Patient Empowerment“.* 03. Zugriff am 20.11.2020. Verfügbar unter: https://www.thieme.de/statics/dokumente/thieme/final/de/dokumente/tw_neurologie/patient_empowerment.pdf

RiskNET. (o.J.). *BCM*. Zugriff am 16.07.2021. Verfügbar unter: https://www.risknet.de/wissen/glossar-eintrag/bcm/

Rudolf-Miklau, F. (2009). *Naturgefahren-Management in Österreich. Vorsorge, Bewältigung, Information* (Orac kompakt). Wien: LexisNexis.

SAP SE. (o.J.). *Leitfaden für Power-User*. Zugriff am 06.03.2021. Verfügbar unter: https://help.sap.com/viewer/108f985b6c531014b00cfa8dbff3d28f/7.0.37/de-DE

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. *Yearbook of Medical Informatics*, (1), 130–137.

Schneiderbauer, S., Kruse, S., Kuhlicke, C. & Abeling, T. (2016). Resilienz als Konzept in Wissenschaft und Praxis. In A. Fekete & G. Hufschmidt (Hrsg.), *Atlas Verwundbarkeit und Resilienz. Pilotausgabe zu Deutschland, Österreich, Liechtenstein und Schweiz = Atlas vulnerability and resilience : Pilot version for Germany, Austria, Liechtenstein and Switzerland* (S. 22–23). Spangenberg: Werbedruck GmbH Horst Schreckhase.

Schnell, M. W. & Dunger, C. (2018). *Forschungsethik. Informieren – reflektieren – anwenden* (2. vollständig überarbeitete und erweiterte Auflage). Bern: Hogrefe. Verfügbar unter: http://elibrary.hogrefe.de/9783456958507

Schnell, M. W. & Heinritz, C. (2006). *Forschungsethik: ein Grundlagen- und Arbeitsbuch mit Beispielen aus der Gesundheits- und Pflegewissenschaft* (1. Aufl.). Bern: Huber.

Schnell, R. (2019). *Survey-Interviews*. Wiesbaden: Springer Fachmedien Wiesbaden.

Semler, S. C. (2000). Medizinische Dokumentation: Rechtliche Aspekte der digitalen Archivierung. *Deutsche Ärzteblatt*, *97*(36), 8–10.

Sieger, H. (2021). *Kein Fördergeld für IT-Sicherheit: Eine absurde Situation in Krankenhäusern*. Zugriff am 20.07.2021. Verfügbar unter: https://digitales-gesundheitswesen.de/kein-foerdergeld-fuer-it-sicherheit-eine-absurde-situation-in-krankenhaeusern/

Simon, M. (2013). Literaturrecherche. In H. Brandenburg, E.-M. Panfil, H. Mayer, A. Manzei, M. W. Schnell, W. Schnepp et al. (Hrsg.), *Pflegewissenschaft 2. Lehr- und Arbeitsbuch zur Einführung in die Methoden der Pflegeforschung* (Pflegeforschung, 2., vollständig überarbeitete Auflage, S. 43–66). Bern: Verlag Hans Huber.

Solms, R. von & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Studiengemeinschaft Werner Kamprath Darmstadt GmbH. (o.J.). *Lernen für Erwachsene*. Zugriff am 19.07.2021. Verfügbar unter: https://www.sgd.de/magazin/leben-lernen/ratgeber/effektives-lernen/lernen-fuer-erwachsene.html

Suda, J., Holub, M., Hübl, J., Jaritz, W., Starl, H. & Rudolf-Miklau, F. (2012). Gefährdungs- und Schadensbilder für Gebäude. In J. Suda & F. Rudolf-Miklau (Hrsg.), *Bauen und Naturgefahren. Handbuch für konstruktiven Gebäudeschutz* (SpringerLink Bücher, S. 71–118). Wien: Springer Vienna.

Telekom Deutschland GmbH. (o.J.). *Managed IT-Service*. Zugriff am 19.07.2021. Verfügbar unter: https://cloud.telekom.de/de/infrastruktur/managed-it-services

Thranberend, T., Knöppler, K. & Neisecke, T. (2016). *Gesundheits-Apps. Bedeutender Hebel für Patient Empowerment - Potenziale jedoch bislang kaum genutzt.* 2. Zugriff am 20.11.2020. Verfügbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/SpotGes_Gesundheits-Apps_dt_final_web.pdf

Tschersich, T. (o.J.). *Security by Design: von Grunf auf Sicher*. Zugriff am 28.07.2021. Verfügbar unter: https://www.t-systems.com/de/blickwinkel/security/architecture/security-by-design-546112

United Nations International Strategy for Disaster Reduction. (2009). *2009 - UNISDR Terminology on Disaster Risk Reduction*. Genf.

United Nations Office for Disaster Risk Reduction. (o.J.a). *Resilience*. Zugriff am 21.02.2021. Verfügbar unter: https://www.undrr.org/terminology/resilience

United Nations Office for Disaster Risk Reduction. (o.J.b). *Terminology*. Zugriff am 07.02.2021. Verfügbar unter: https://www.undrr.org/terminology/vulnerability

Weichselgartner, J. (2016). Verwundbarkeit als Konzept in Wissenschaft und Praxis. In A. Fekete & G. Hufschmidt (Hrsg.), *Atlas Verwundbarkeit und Resilienz. Pilotausgabe zu Deutschland, Österreich, Liechtenstein und Schweiz = Atlas vulnerability and resilience : Pilot version for Germany, Austria, Liechtenstein and Switzerland* (S. 18–19). Spangenberg: Werbedruck GmbH Horst Schreckhase.

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne Hilfe Dritter verfasst habe. Bei der Arbeit wurden keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Alle den angegebenen Quellen entnommenen wörtlichen oder sinngemäßen Inhalte wurden von mir entsprechend kenntlich gemacht.

_____

Ort, Datum Unterschrift

A. Interviewleitfaden zum Experteninterview

Interviewleitfaden zur Masterarbeit

Digitalisierung in der Pflege

Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag

Interviewer: Kunze Florian

Interviewter: _____

Interviewkürzel: _____

Datum: _____

Uhrzeit: _____

Ort: _____

Einführung

Herr/ Frau […], ich darf Sie herzlich zu unserem heutigem Interviewtermin begrüßen.

Vielen Dank, dass Sie sich die Zeit genommen haben für unser Gespräch und mich damit bei meiner Masterarbeit unterstützen. In meiner Masterarbeit beschäftige ich mich mit dem Thema „Digitalisierung in der Pflege – Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag“. Das Ziel dieser Arbeit besteht darin, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert zu erarbeiten und daraus Handlungsempfehlungen ableiten zu können. Dieses IT-gestützte Dokumentationssystem soll dazu dienen, die Bearbeitung elektronischer Patientenakten im Pflegealltag unter Beachtung gesetzlicher, operativer, wirtschaftlicher Aspekte zu ermöglichen. Die Erwartung an solch ein System besteht darin, sowohl die Verfügbarkeit als auch die Anfälligkeit gegenüber natürlichen und menschlichen Ereignissen zu verbessern.

Wie besprochen wird unser Gespräch tontechnisch aufgezeichnet. Sie bleiben dabei selbstverständlich anonym. Die Formalitäten der Einwilligungserklärung und des Datenschutzes haben wir bereits im Vorfeld erledigt. Herr/Frau […], haben Sie noch Fragen bevor wir beginnen?

♪♪♪ START TONAUFNAME ♪♪♪

Einstiegsfrage

Die Digitalisierung in der Pflege schreitet immer weiter voran. Welche Rolle spielt die Digitalisierung in der Pflege, beispielsweise die digitale Pflegedokumentation im Krankenhaus, für Sie?

Leitfrage (Erzählaufforderung)	Checkliste	Konkrete Fragen	Aufrechterhaltungs- und Steuerungsfragen
Notwendigkeit, Vor- und Nachteile elektronischer und papiergestützter Patientenakten			
Die papiergestützte Patientenakte wird immer mehr von der digitalen Patientenakte abgelöst. Wie bewerten Sie diese Entwicklung in deutschen Krankenhäusern?	• Vorteile Papierakte • Nachteile Papierakte • Vorteile elektronische Akte • Nachteile elektronische Akte	Welche Vorteile hat in Ihren Augen die Verwendung elektronischer Patientenakten? Welche Nachteile hat in Ihren Augen die Verwendung elektronischer Patientenakten?	Können Sie dazu noch etwas mehr erzählen? Sie haben gerade erwähnte, dass …… Können Sie mir mehr darüber erzählen?
Implementierung elektronischer Patientenakten im Krankenhaus			
Ich stelle mir vor, dass die Implementierung einer elektronischen Patientenakte im Krankenhaus ein großes Projekt ist. Wie sieht in Ihren Augen eine erfolgreiche Implementierung einer elektronischen Patientenakte aus?	• Finanzielle Rahmenbedingungen • Technische Rahmenbedingungen • Gesetzliche Rahmenbedingungen • Beteiligte Akteure • Benutzereinweisungen • Keyuser	Wieviel Zeit sollte man für eine erfolgreiche Implementierung einer elektronischen Patientenakte einplanen?	Welche weiteren Gesetzte müssen bei der Implementierung elektronischer Patientenakten berücksichtigt werden? Können Sie das noch näher erläutern?

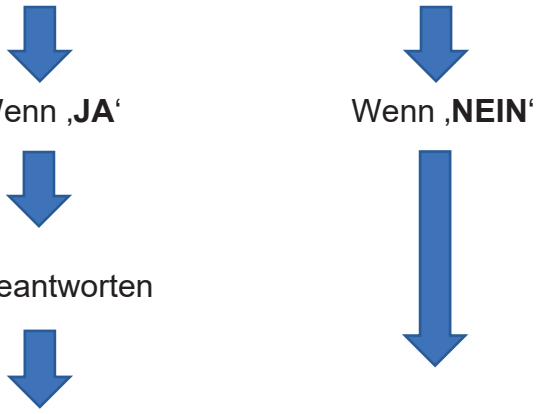
Leitfrage (Erzählaufforderung)	Checkliste	Konkrete Fragen	Aufrechterhaltungs- und Steuerungsfragen
Anforderungen elektronischer Patientenakten (Datenverfügbarkeit, Datenschutz und Sicherheit)			
Wenn die elektronische Patienten- akte im Krankenhaus implementiert wurde, welche Anforderungen werden an diese bezüglich der Datenverfügbarkeit gestellt?	• Datenverfügbarkeit • Verfügbarkeit elektronischer Endgeräte zum Datenabruf • Benötigte IT-Struktur	Welche technischen Anforderungen müssen erfüllt werden, um die Datenverfügbarkeit gewährleisten zu können?	Wie kann …… Ihrer Meinung nach aussehen? Können Sie mir bezüglich […] bitte mehr erzählen?
Der Zugriff auf Patientendaten spielt eine grundlegende Rolle im Krankenhaus und im Pflegealltag. Welche Patientendaten müssen Ihrer Meinung nach den am Patienten tätigen Personen zur Verfügung stehen, um den Patienten versorgen zu können?	• Genereller Patientendatenzugriff im täglichen Routinegeschäft • Patientendatenzugriff bei fehlenden Datenzugriff/Datenverlust	Welches Mindestmaß an Patientendaten benötigen Ihrer Meinung nach Pflegende bei einem Ausfall der IT-Struktur, um den Patienten in dieser Situation weiter versorgen zu können?	Können Sie das […] weiter erläutern? Verstehe ich sie richtig, dass […] Wie sieht es mit […] aus?
Das Thema Datenschutz ist großes Thema in Krankenhäusern. Welche datenschutzrechtliche Anforderung muss eine elektronische Patientenakte haben?	• Durchsetzung des Datenschutzes • Kontrollinstanzen • Speicherung der Datensätze • Datenzugriff	Welche Berufsgruppen haben eine Berechtigung um auf sensible Patienten-daten, welche in der elektronische Patienten-dokumentation hinterlegt sind, zugreifen zu können und in welchem Umfang? Wie werden die Datenzugriffe überwacht?	Verstehe ich Sie richtig, dass […]?
Neben dem Datenschutz müssen sich Krankenhäuser aber auch mit der Sicherheitsthematik elektronischer Patientenakten auseinandersetzten. Welche Sicherheitsanforderungen müssen elektronische Patientenakten erfüllen?	• Software • Hardware • Netzwerke • Schnittstellen • Betreuung der elektronischen Patientenakte	Welche Möglichkeiten haben Mitarbeitende, wenn hinsichtlich der elektronischen Patientendokumentation Probleme oder Fragen aufkommen? Welche Unterstützungsangebote seitens der IT-Abteilung/IT-Hotline existieren in Ihrer Einrichtung, wenn es zu Problemen außerhalb der Bürozeiten (z.B. in den Abend- oder Nachtstunden) kommt?	Wie gestaltet sich die […]? Können Sie bitte den Zusammenhang zwischen […] und […] erklären?

Leitfrage (Erzählaufforderung)	Checkliste	Konkrete Fragen	Aufrechterhaltungs- und Steuerungsfragen
Vulnerabilität von elektronischen Patientenakten			
Man hört in den Medien immer wieder von Cyberangriffen bzw. Hackerangriffen auf Krankenhäuser. So musste sich das Universitätsklinikum Düsseldorf im September 2019 von der Notfallversorgung abmelden, da ein Hacker das IT-System des Klinikums verschlüsselte. Welche Gründe sind Ihrer Meinung nach verantwortlich, dass elektronische Patientenakten anfälliger gegenüber Cyberangriffen (z.B. Hackerangriffe) sind?	• Auswirkungen • Gründe warum elektronische Patientenakten anfälliger/vulnerabler sind • Cyberangriffe • Gründe für den Ausfall der IT-Struktur	Welche Auswirkungen können Angriffe auf IT-Infrastruktur (z.B. Computervirus) auf das Krankenhaus selbst bzw. auf den täglichen Krankenhausbetrieb haben?	Verstehe ich, dass […] Können Sie zu der Thematik […] noch was sagen?
Ausfallkonzept			
Wir haben gerade über die Anfälligkeit von elektronischen Patientenakten geredet. Im Fall eines Ausfalles der elektronischen Patientenakte (z.B. Hackerangriff, Stromausfall), wie sollte Ihrer Meinung nach das Ausfallkonzept gestaltet sein?	• Ausfallkonzept ‚Wartung' • Ausfallkonzept ‚kurzzeitiger Stromausfall' • Ausfallkonzept ‚langfristiger Stromausfall' • Ausfallkonzept ‚fehlende Datensicherheit' • Ausfallkonzept ‚hausinterne Notfälle' • Ausfallkonzept ‚Evakuierung' • Ausfallkonzept ‚fehlende Zugangsdaten'	Im Fall einer Evakuierung des gesamten Krankenhauses in umliegende Noteinrichtungen. Wie gestaltet sich in Ihrer Einrichtung der Zugriff auf die Patientendaten durch den Rettungsdienst und die Pflegekräfte, wenn diese die Patienten in Noteinrichtungen beispielsweiser einer Turnhalle über einen längeren Zeitraum versorgen müssen?	Was ist, wenn […]? Können Sie sich vorstellen, wie ein […] gestaltet sein sollte, damit die Versorgung weiter gewährleistet werden kann? Können Sie dazu noch etwas mehr erzählen? Habe ich Sie richtig verstanden, dass […]?

Rückblick:

Herr/Frau […], wir sind jetzt am Ende des Interviews angelangt. Wir haben jetzt über die Vor- und Nachteile elektronischer und papiergestützter Patientenakten sowie die Implementierung elektronischer Patientenakten gesprochen. Zudem haben wir über die Anforderungen elektronischer Patientenakten bezüglich Datenverfügbarkeit, Datenschutz und Sicherheit, über die Anfälligkeiten elektronischer Patientenakten sowie über Ausfallkonzepte gesprochen.

Haben Sie abschließend noch weitere Themen dazu, die ich nicht angesprochen habe, die Ihnen aber wichtig sind?



Ich danke Ihnen nochmals, dass Sie sich Zeit für unser Gespräch genommen haben und mich bei meiner Masterarbeit unterstützen.

♪♪♪ ENDE TONAUFNAME ♪♪♪

B. Informationsschreiben und Datenschutzerklärung zum Experteninterview

Informationsschreiben

Sehr geehrte/r _____,

herzlichen Dank für Ihr Interesse an diesem Forschungsvorhaben.

Forschungsprojekt:	Masterarbeit „Digitalisierung in der Pflege – Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag“
Institution:	Universität Wien
Projektleitung:	Florian Kunze B.Sc. (kunze.thesis@gmail.com)
Interviewer:	Florian Kunze B.Sc.
Interviewdatum:	_____

Im Rahmen meiner Masterarbeit will ich mit Ihrer Hilfe Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert erarbeiten und Handlungsempfehlungen daraus ableiten. Das IT-gestütztes Dokumentationssystem soll dazu dienen, die Bearbeitung elektronischer Patientenakten im Pflegealltag unter Beachtung gesetzlicher, operativer, wirtschaftlicher Aspekte zu ermöglichen. Die Erwartung an solch ein System besteht darin, sowohl die Verfügbarkeit aller patientenrelevanter Daten als auch die Anfälligkeit des Systems gegenüber natürlichen und menschlichen Ereignissen zu verbessern.

Um dieses Ziel erreichen zu können, will ich mit Ihnen ein Interview führen.

Die Teilnahme an dem Interview ist freiwillig. Sie haben zu jedem Zeitpunkt die Möglichkeit, das Interview abzubrechen, Ihre Einverständniserklärung in die Aufzeichnung und die verschriftliche Interviewniederschrift zurückzunehmen, ohne das Ihnen daraus Nachteile entstehen.

Datenschutzhinweis

Die Daten werden von Florian Kunze, B.Sc. im Rahmen seiner Masterarbeit

„**Digitalisierung in der Pflege**

Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag“

erhoben.

Die Daten werden ausschließlich für Lehr- und wissenschaftliche Zwecke genutzt. Das Gespräch wird tontechnisch aufgezeichnet und anschließend verschriftlicht. Dieses Interviewtranskript wird anonymisiert, sodass kein Rückschluss auf Ihre Person möglich ist. Die anonymisierten Interviewtranskripte werden inhaltsanalytisch bearbeitet. In anonymisierter Form können die Daten auch öffentlich zum Download zur Verfügung gestellt werden.

Die personenbezogene Kontaktdaten und die generierten Interviewdaten werden getrennt voneinander für Dritte unzugänglich gespeichert. Nach Beendigung der Masterarbeit werden Ihre Kontaktdaten gelöscht. Sie haben am Ende die Möglichkeit die Speicherung Ihrer Kontaktdaten ausdrücklich zuzustimmen, wenn Sie für weitere Forschungsprojekten in diesem Themengebiet angeschrieben werden wollen. Sie können einer längeren Speicherung zu jeder Zeit widersprechen.

Zugang zu den Daten haben ausschließlich Mitglieder des Projektteams. Die anonymisierten Daten werden an weitere Dritte ausschließlich zu wissenschaftlichen Zwecken weitergegeben, die ebenfalls an die vorgegebenen datenschutzrechtlichen Bestimmungen gebunden sind. Des Weiteren werden die anonymisierten Datensätze zur Verarbeitung in wissenschaftlichen Arbeiten an einem sicheren Ort aufbewahrt und gesichert. Die erhobenen Daten werden auf einem passwortgeschützten Server gespeichert und gelagert.

Abschlussarbeiten müssen laut Universitätsgesetz veröffentlicht werden (durch Aufstellen in der National- und Universitätsbibliothek), sie sind üblicherweise auch online zugänglich.

Weiters besteht das Recht auf Auskunft durch den Verantwortlichen dieser Studie über die erhobenen personenbezogenen Daten sowie das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung der Daten sowie ein Widerspruchsrecht gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit.

Wenn Sie Fragen zu dieser Erhebung haben, wenden Sie sich bitte per E-Mail an den Verantwortlichen dieser Untersuchung, Florian Kunze B.Sc. (kunze.thesis@gmail.com).

Für grundsätzliche juristische Fragen im Zusammenhang mit der DSGVO und studentischer Forschung wenden Sie sich bitte per Mail an den Datenschutzbeauftragen der Universität Wien, Dr. Daniel Stanonik, LL.M. (verarbeitungsverzeichnis@univie.ac.at).

C. Einverständniserklärung zum Experteninterview

Forschungsprojekt:	Masterarbeit „Digitalisierung in der Pflege – Vulnerabilität und Resilienz von elektronischen Patientenakten im Pflegealltag“
Institution:	Universität Wien
Projektleitung:	Florian Kunze B.Sc. (kunze.thesis@gmail.com)
Interviewer:	Florian Kunze B.Sc.
Interviewdatum:	_____

Das Informationsschreiben und den Datenschutzhinweis habe ich gelesen und verstanden. Ich bin damit ausdrücklich einverstanden, im Rahmen des genannten Forschungsprojekts freiwillig an einem Interview teilzunehmen.

Ich wurde ausführlich über den Zweck und die Vorgehensweise der Studie informiert. Des Weiteren hatte ich ausreichend Zeit, mich zur Teilnahme zu entscheiden. Ich weiß, dass die Teilnahme freiwillig ist und ich die Zustimmung zur Teilnahme ohne Nennung von Gründen jederzeit widerrufen kann und mir daraus keine Nachteile entstehen. Der Widerruf kann mündlich erfolgen und bedarf ausdrücklich nicht der schriftlichen Form.

Der vertrauliche und anonyme Umgang mit den erhobenen Daten wurde mir zugesichert. Ich bin mit der Erhebung und Verwendung persönlicher Daten nach Maßgabe des Informationsschreibens einverstanden. Ebenso stimme ich einer anonymen Speicherung, Auswertung und Veröffentlichung der Daten zu.

Ort, Datum	**Name in Druckschrift**	**Unterschrift**

Ich bin damit einverstanden, für weitere Forschungsprojekte in diesem Themengebiet kontaktiert zu werden. Hierfür werden meine Kontaktdaten über das Ende der Masterarbeit hinaus gespeichert.

Ort, Datum	**Name in Druckschrift**	**Unterschrift**

D. Kodierleitfaden

	Kategorie	Definition	Ankerbeispiel	Kodierregel
OK 1	Rolle und Notwendigkeit der Digitalisierung in der Pflege	Informationen, die die Wichtigkeit und Erfordernis für die Digitalisierung in der Pflege enthalten	„Eine essenzielle Rolle. Letztlich führt da kein Weg mehr daran vorbei, wenn wir mitgehen wollen mit dem, was andere Berufsgruppen in unserem Haus ja auch als notwendig ansehen. Und wenn wir im Rahmen der schnellen Schlagzahl, die wir zu bewältigen haben, eine - wie soll ich sagen? - eine verbesserte Gleichzeitigkeitssituation herstellen wollen, was man mit einem Papierdokument niemals erreichen können wird.“ (Interview D, Pos. 24-29)	
OK 2	Abwägungen zur papiergebundenen Patientenakte	Informationen, die Aspekte der papiergebundenen Patientenakte enthalten		
UK 2.1	Vorteile der papiergebundene Patientenakte	Informationen, die positive Aspekte in Hinblick auf die Verwendung der papiergebundenen Patientenakte enthalten	„Die Vorteile sind in der Papierakte, dass, wenn du einen Stromausfall hast, du trotzdem die Daten hast von den Patienten.“ (Interview H, Pos. 39-40)	
UK 2.2	Nachteile der papiergebundenen Patientenakte	Informationen, die negative Aspekte in Hinblick auf die Verwendung der papiergebundenen Patientenakte enthalten	„Allein schon, wenn man bedenkt, wie die Handschrift von manchen ist, dass es nicht leserlich ist, dass man es nicht identifizieren kann, ausgeschrieben wurde, wer geschrieben hat (...) Da ist natürlich die digitale Akte besser.“ (Interview G, Pos. 50-53)	
OK 3	Abwägungen zur elektronischen Patientenakte	Informationen, die Aspekte der elektronischen		

		Patientenakte enthalten		
UK 3.1	Vorteile der elektronischen Patientenakte	Informationen, die positive Aspekte in Hinblick auf die Verwendung der elektronischen Patientenakte enthalten	„Ich glaube, Vorteile gibt es viele, da man einfach eine bessere Übersicht hat, eine einheitliche Dokumentation, keine handschriftlichen Sachen, die man nicht lesen kann, zum Beispiel.“ (Interview G, Pos. 36-38)	
UK 3.2	Nachteile der elektronischen Patientenakte	Informationen, die negative Aspekte in Hinblick auf die Verwendung der elektronischen Patientenakte enthalten	„Aber natürlich digital kann auch alles immer wieder mal irgendwie ausfallen wegen Servern oder - keine Ahnung - technischen Problemen einfach. Und dann braucht man halt ein gutes Ausfallsystem.“ (Interview G, Pos. 38-40)	
OK 4	Implementierung elektronische Patientenakte im Krankenhaus	Informationen, die mit der Einführung bzw. Implementierung einer elektronischer Patientenakten im Krankenhaus in Zusammenhang stehen		
UK 4.1	Finanzielle Rahmenbedingungen	Informationen, die monetäre Aspekte zur Einführung elektronischer Patientenakten enthalten	„Also was finanziell betrifft, es ist wichtig, dass da nicht gespart werden soll. Finanziell und technisch muss man dann in Einklang bringen. Das heißt, wenn ich eine digitale Akte einführe, dann muss mir auch bewusst sein als Geschäftsführer, dass wir entsprechende Hardware auch benötigen. Also als Beispiel, wenn ich eine digitale Pflegedokumentation einführe, kann es ja nicht sein, dass wir nur mit den kleinen Geräten ausgestattet sind, wie	

			zum Beispiel Tablets, weil da kann ich nicht die gesamte Dokumentation abbilden, aber wohl einen bestimmten Teil, zum Beispiel Wundversorgung.“ (Interview E, Pos. 108-115)	
UK 4.2	Technische Rahmenbedingungen	Informationen, die technische Aspekte zur Einführung elektronischer Patientenakten enthalten	„Naja, da sind wir bei dem Punkt: Bitte keine Kompromisse. Also ich würde bei der Technik heute noch weniger Kompromisse eingehen als in der Vergangenheit. Weil es zeigt sich, wenn ich kein vernünftiges WLAN habe - und vernünftiges WLAN heißt ausgeleuchtet in jeder Ecke einer Station -, das sind Dinge, da investiert man auf Jahrzehnte, zum Teil. Die Fehler, die man da macht, die muss man immer wieder aufs Neue bereuen. Also bei der Technik relativ kompromissfrei. Die Technik muss skalierbar sein. Das heißt, einmal hinsichtlich der Datenmengen, [...].“ (Interview B, Pos. 137-145)	
UK 4.3	Gesetzliche Rahmenbedingungen	Informationen, die gesetzliche Aspekte zur Einführung elektronischer Patientenakten enthalten	„Ja, da haben wir eine ganze Menge. Da geht es los von Datenschutzgrundverordnung, die wir einhalten müssen, von Security by Design, von Löschvorgaben. Also das wird zukünftig meines Erachtens noch mehr.“ (Interview B, Pos. 163-165) „Dann haben wir Medizinproduktgesetz oder jetzt neu diese Medical Device	

			Regulation.“ (Interview B, Pos. 169-170)	
UK 4.4	Beteiligte Akteure	Informationen, welche Akteure und Berufsgruppen für die Implementierung einer elektronischen Patientenakte miteinbezogen werden müssen	„Ja, in erster Linie die IT-Leute. Die Leute, die in der Lage sind, Software zu programmieren. Die Firmen, die die Produkte, die als Dokumentationsprodukte erstellt wurden, hergestellt haben bzw. betreuen und aktualisieren. Die darf man sicherlich nicht vergessen. Und alle beteiligten Berufsgruppen. Natürlich nicht in der Masse und dauernd alle auf einen Haufen, aber sicherlich Vertreter der jeweiligen Berufsgruppen, die in einer Patientenakte Dokumentationsverpflichtungen haben [...].“ (Interview D, Pos. 81-88)	
UK 4.5	Benutzereinweisung/Key-User	Informationen, die Aspekte zur Einweisung von Benutzern in die elektronischen Patientenakte oder Aspekte bezüglich Key-Usern enthalten	„Zum einen, wie gesagt, im Voraus das Grundverständnis der Pflege zu klären dann im direkten Handling eventuell im Voraus schon E-Learning-Angebote zu machen, in denen schrittweise die einzelnen Bedienelemente dargestellt werden, wo man auch nochmal nachschauen kann, wo man sich nochmal draufklinken kann. Und aber auch persönliche Schulungselemente, wo man konkret jemanden fragen kann, der sich damit auskennt, wo man einen Ansprechpartner hat. Da sind wir auch ganz schnell dabei, dass wir aktiv auf den Stationen Begleitung brauchen, die die	

			Kollegen auf der Station mit dem ganzen System jederzeit ansprechbar haben, damit sie Fragen klären, dass man Veränderungen mit einbauen kann.“ (Interview C, Pos. 114-123)	
UK 4.6	Dauer der Implementierung	Informationen, die Aspekte zur zeitlichen Dauer der Implementierung einer elektronischen Patientenakte enthalten	„Persönlich sage ich mal, alles unter sechs Monaten ist irgendwie falsch aufgesetzt oder in die Tasche gelogen. Alles ab 18 Monaten kommt so in die Gefahr, die Leute langeweilen sich in Richtung "Werden wir jetzt irgendwann fertig?". Also persönlich würde ich sagen, zwischen sechs und zwölf Monaten sollte man solche Module dann entsprechend umsetzen. Im ganzen KIS müsste man es neu betrachten, aber wie gesagt, aus meiner Erfahrung, sechs Monate ist ein guter Sprint.“ (Interview B, Pos. 183-189)	
OK 5	Anforderungen an die elektronische Patientenakte	Informationen, die verschiedene Rahmenbedingungen zur Implementierung einer elektronischen Patientenakte enthalten	„Die normalen Stammdaten immer. Also immer bezogen auf denjenigen, der auch in diesem Bereich arbeitet und mit dem Patienten arbeitet. Auch die Diagnosen, die erfolgten Untersuchungen. Dann beispielsweise bezugnehmend auf die Entlass-Planung, die Dokumentation derjenigen, die das ganze machen. Und ansonsten müsste man dann wirklich individuell entscheiden, in welchem Rahmen man noch was bräuchte.	

			Gerade diese Pflegeplanungssachen, also alles, wo der Mitarbeiter direkten Zugriff haben muss, weil er gerade am Patienten arbeitet, um an ihm arbeiten zu können, müssen vorhanden sein.“ (Interview A, Pos. 104-111)	
UK 5.1	Datenverfügbarkeit	Informationen, die Aspekte bezüglich der Datenverfügbarkeit oder den Zugriff auf Patientendaten enthalten		
UK 5.2	Datenschutz	Informationen, die Aspekte zu den datenschutzrechtlichen Anforderungen an eine elektronische Patientenakte enthalten	„Also den Mitarbeitern ist ja von Anfang an klar, dass es den Datenschutz gibt, dass sie sich daran halten müssen, dass das ansonsten arbeitsrechtliche Folgen für ihn haben kann. Der Patient muss bei Aufnahme oder oft schon vor Aufnahme darüber informiert werden, was eben bei den Datenschutzvereinbarungen vorhanden ist, an wen diese Daten weitergegeben dürfen in welchem Rahmen. Das auch gegen Unterschrift.“ (Interview A, Pos. 122-127)	Diese Kodierung nur anwenden, wenn die Thematik des Datenschutzes weiter erläutert wird. Wenn nur das Schlagwort ‚Datenschutz‘, ‚Datenschutzgrundverordnung‘ oder ‚Datenschutzgrundgesetz‘ verwendet wird als Hinweis, dass diese Rahmenbedingung erfüllt werden muss → UK 4.3
UK 5.3	Sicherheit	Informationen, die Aspekte zu sicherheitstechnischen Anforderungen an die elektronische	„Also wenn man jetzt an die Endgeräte denkt, dass man da natürlich die entsprechenden Hygienevorgaben erfüllt, dass man eine abwischbare - jetzt habe ich einen Sprachfehler -	

		Patientenakte enthalten	desinfizierbare Oberfläche hat, um da eben die Hygienestandards zu halten. Punkt 1. Dann muss müssen solche Systeme natürlich auch, ich sage jetzt mal, den Vertraulichkeits-, Verfügbarkeits- und Integritätsanforderungen der IT-Sicherheit irgendwo Rechnung tragen. Das heißt, es müssen zuverlässige Hersteller oder Produzenten sein, die diese Produkte anbieten, vertreiben. Es muss aber gleichzeitig auch intern überprüft werden, ob diese Systeme dem aktuellen Stand der Technik entsprechen.“ (I, Z. 323-331)	
OK 6	Vulnerabilität von elektronischen Patientenakten	Vulnerabilität von elektronischen Patientenakten		
UK 6.1	Vulnerabilität gegenüber Cyberangriffen	Informationen, die Aspekte bezüglich der Verletzlichkeit und Angreifbarkeit von elektronischen Patientenakten gegenüber Cyberangriffen enthalten	„Das heißt, es ist eine zum Teil sehr veraltete, auch schon End-of-Life oder End-of-Service betriebene IT-Infrastruktur vorhanden, die natürlich aus diesem Grund heraus schon sehr verwundbar ist. Dazu kommt, dass meiner Erfahrung nach das Thema IT-Abteilung und auch Ressourcenausstattung in diesen Bereichen sehr stiefmütterlich behandelt wird. Das heißt, es gibt zu viele Aufgaben für zu wenig Mitarbeiter. Das heißt, das verschleppt natürlich auch ein regelmäßiges Patchen von Systemen oder auch Schließen von Sicherheitslücken.“	

			(Interview I, Pos. 391-397)	
UK 6.2	Weitere Gründe für den Ausfall der IT-Struktur	Informationen, die Aspekte bezüglich der Ursachen für den Ausfall der IT-Struktur enthalten	„Ja, da gibt es ganz vielfältige Gründe. Also wir können natürlich an elementare Gefährdungen denken, zum Beispiel Hochwasser oder ein Brand in einem Rechenzentrum oder auch Vandalismus oder Sabotage, dass jemand bewusst auch Infrastrukturen zerstört, oder Explosion dazu führt, dass eben auch ein Serverschrank mit wichtigen Switchen oder eben Rückfallebenen ausfällt. Das ist eine Möglichkeit, warum die Infrastruktur ausfällt.“ (Interview I, Pos. 419-424)	Diese Kodierung kann verwendet werden, wenn außer den Ausfall der IT-Struktur durch Cyberangriffe andere Gründe für Ausfälle genannt werden.
UK 6.3	Auswirkungen bei Ausfall der IT-Struktur	Informationen, die Aspekte bezüglich der Auswirkungen bei einem IT-Ausfall enthalten	„Da gibt es sogar Studien, die sagen: Wenn ein Krankenhaus nach fünf Tagen nicht wieder langsam hochkommt, dann wird es aus eigener Kraft auch nicht mehr schaffen. Also das kann ganz fatale Auswirkungen haben.“ (Interview B, Pos. 385-387)	
OK 7	Ausfallkonzepte	Informationen, die Aspekte bezüglich allgemeiner Konzepte bei Ausfällen der IT-Struktur enthalten		
UK 7.1	Allgemeines Ausfallkonzept	Informationen, die allgemeine Aspekte über	„Wir hatten es vorhin schonmal gesagt. Vielleicht gibt es	

		Ausfallkonzepte enthalten	irgendwo PCs, die stundengenau PDF-Dateien haben, und davon dann aber 20 Stück übers Haus verteilt“ (Interview B, Pos. 422-424)	
UK 7.2	Ausfallkonzept im Falle einer Evakuierung	Informationen, die Aspekte bezüglich eines Ausfallkonzeptes im Falle einer Evakuierung oder Räumung des gesamten Krankenhauses enthalten	„Nein, also spätestens da sind wir genau an dem Punkt, dass ich sage, jetzt wären wir beim Cloud-Konzept im Idealzustand. Wenn man mal sagt, bislang ist es ja so: Ein Krankenhaus, ein KIS, eine EDV, ein Rechenzentrum oder zwei. Jetzt machen wir mal die Annahme, wir haben einen Totalausfall. Blöd gelaufen. Wären wir in der Cloud - und in der Regel sind Cloudstrukturen technologisch komplett anders aufgebaut. [...] Aber dann könnte ich sagen, mir ist egal, wo diese Patienten später liegen. Jedes Krankenhaus kriegt den Zugriff auf das nach wie vor vorhandene virtuelle Krankenhausinformations system.“ (Interview B, Pos. 433-442)	Kodierung kann verwendet werden, wenn es ausdrücklich um ein Ausfallkonzept im Zusammenhang mit der Evakuierung oder Räumung des Krankenhauses geht. Ansonsten Kodierung mit OK 7.1

E. Kurzfassung

Die Digitalisierung in der Pflege bringt eine Vielzahl von Vorteilen mit sich. Es müssen aber auch eine Reihe von Herausforderungen bewältigt werden. Dies wird vor allem im Bereich der elektronischen Patientenakte in Krankenhäusern deutlich.

Das Ziel dieser Masterthesis besteht darin, Anforderungen für die pflegerische Dokumentation in der IT-gestützten Patientenakte wissenschaftlich fundiert erarbeiten und Handlungsempfehlungen daraus ableiten zu können.

Um dieses Ziel zu erreichen, wurden sechs Forschungsfragen festgelegt:

- Was sind die Vorteile von digitalen Dokumentationssystemen gegenüber papiergestützter Dokumentation im akutstationären Setting?
- Welche Patientendaten müssen im Falle eines Ausfalls der IT-Struktur im akutstationären Setting den am Patienten tätigen Personen zur Verfügung stehen, wenn der Zugriff auf die elektronische Patientenakte nicht mehr möglich ist oder Datensätze verloren gegangen sind?
- Sind elektronische Patientenakten im Klinikalltag vulnerabler gegen Cyberangriffe als papiergebundene Patientenakten?
- Welche Anforderungen muss eine elektronische Patientenakte im akutstationären Setting in Hinblick an die Datenverfügbarkeit, den Datenschutz und die Sicherheit erfüllen?
- Welche Rahmenbedingungen müssen erfüllt sein, damit die elektronische Patientenakte im Klinikalltag implementiert werden kann?
- Welche Akteure im Krankenhaus müssen bei der Implementierung der elektronischen Patientenakte miteinbezogen werden, um eine gelungene Einführung der elektronischen Patientenakte zu erreichen?

Zur Beantwortung der Forschungsfragen wurden im Rahmen eines qualitativen Forschungsdesigns 15 Experteninterviews geführt und anschließend inhaltsanalytisch ausgewertet.

Die Ergebnisse zeigen, dass die Implementierung und der Betrieb einer digitalen Patientenakte im Krankenhaus komplex sind. Neben der Sicherheit der Systeme, spielen gesetzliche, operative und wirtschaftliche Aspekte eine entscheidende Rolle.

Die Digitalisierung in der Pflege bietet Raum für weitere Forschungsvorhaben, beispielsweise die Entwicklung von Schulungskonzepten.

Abstract

Digitization in nursing care brings with it a host of benefits. However, a number of challenges must also be overcome. This is particularly evident in the area of electronic patient records in hospitals.

The aim of this master's thesis is to develop requirements for nursing documentation in the IT-supported patient file in a scientifically sound manner and to be able to derive recommendations for action.

To achieve this goal, six research questions were defined:

- What are the advantages of digital documentation systems over paper-based documentation in the acute inpatient setting?
- In the event of a failure of the IT structure in the acute inpatient setting, what patient data must be available to those working on the patient if access to the electronic patient record is no longer possible or data records have been lost?
- Are electronic patient records in the hospital setting more vulnerable to cyberattacks than paper-based patient records?
- What requirements must an electronic patient record meet in the acute inpatient setting with regard to data availability, data protection and security?
- What framework conditions must be met for the electronic patient record to be implemented in the hospital setting?
- Which hospital stakeholders need to be involved in the implementation of the electronic health record in order to achieve a successful introduction of the electronic health record?

To answer the research questions, 15 expert interviews were conducted as part of a qualitative research design and then evaluated using content analysis.

The results show that the implementation and operation of a digital patient record in hospitals is complex. In addition to the security of the systems, legal, operational and economic aspects play a decisive role.

Digitization in nursing care offers scope for further research projects, such as the development of training concepts.