UniversitätsKlinikum Heidelberg

„Surveillance der Gesundheit und primärmedizinischen Versorgung von Asylsuchenden in Erstaufnahmeeinrichtungen und Gemeinschaftsunterkünften in Deutschland“

DATENSCHUTZKONZEPT

Version 2.0 vom 03.09.2020

Herausgeber:
Abteilung Allgemeinmedizin und Versorgungsforschung
Universitätsklinikum Heidelberg
INF 130.3, Marsilius Arkaden, Turm West
69120 Heidelberg

Projektleitung:
Prof. Dr. Kayvan Bozorgmehr
Tel.: +49 6221 56-38581
Fax: +49 6221 56-1972
E-Mail: kayvan.bozorgmehr@med.uni-heidelberg.de

Projektkoordination:
Rosa Jahn
Tel.: +49 6221 56-34137
E-Mail: rosa.jahn@med.uni-heidelberg.de

1 Inhaltsverzeichnis

Dokumenteninformation

Status

Beschreibung	Verantwortliche
Initiierung	Kayvan Bozorgmehr
Erstellung Version 1.0	Frank Aluttis Kayvan Bozorgmehr Johannes Drepper Valérie Gläß Stefan Nöst Markus Qreini Ronny Repp Irene Schluender Jonas Steinmann
Erstellung Version 2.0	Frank Aluttis Kayvan Bozorgmehr Johannes Drepper Rosa Jahn Markus Qreini Ronny Repp Knut Kaulke Sophie Rybczak
Laufende Koordination v. a. des Umsetzungs- und Fortschreitungsprozesses:	Rosa Jahn

2 Einleitung

Über die gesundheitliche Situation von Asylsuchenden und ihre medizinische Versorgung ist bisher sehr wenig bekannt. Dies ist unter anderem auf eine unzureichende Datensituation zur medizinischen Versorgung in Erstaufnahmeeinrichtungen und in großen Gemeinschaftsunterkünften zurückzuführen[1].

Mit dem Ausmaß der Immigration nach Deutschland gehen weitreichende Anforderungen an die individualmedizinische sowie die bevölkerungsmedizinische Versorgung einher. Daher besteht ein großes öffentliches Interesse an Daten zum Gesundheitszustand der Asylsuchenden und geflüchteten Menschen sowie an der Sicherstellung der medizinischen Versorgung. Die Versorgungsangebote in den einzelnen Unterkünften sind allerdings sehr unterschiedlich gestaltet. Sowohl die Intensität, die Varianz sowie die Qualität der Versorgungsangebote unterscheiden sich, meist in Abhängigkeit von materiellen und personellen Ressourcen, von Einrichtung zu Einrichtung. Sowohl die gesetzlichen Grundlagen zum eingeschränkten Umfang der medizinischen Behandlung im Asylbewerberleistungsgesetz (§ 4 und §6 AsylbLG) sowie die gesetzlich festgelegte Sicherstellung medizinischer Versorgung durch die Aufnahmebehörden setzen Rahmenbedingungen, die regional und situativ sehr unterschiedlich ausgelegt werden. Dies führt zu einer großen Heterogenität und vielen regionalen Insellösungen.

Dies spiegelt sich auch in der Umsetzung der Dokumentationspflicht nach § 630f BGB wider: während in einigen Einrichtungen keine Dokumentation medizinischer Behandlungen stattfindet und der Dokumentationspflicht somit nicht nachgekommen wird, führen andere Einrichtungen ausschließlich eine papierbasierte Dokumentation zu meist ohne standardisierte Klassifikationen durch. Diese Problemlage wurde von der Universitätsklinik Heidelberg in einer bundesweiten Analyse der Versorgungssituation Asylsuchender empirisch nachgewiesen [2]. Die unzureichende Dokumentation medizinischer Behandlungsmaßnahmen birgt nicht nur Probleme für die Wissenschaft. Sie führt auch dazu, dass bei Wiederholungsbesuchen die Krankenhistorie mehrfach erhoben werden muss und es zu Über-, Unter- und Fehlversorgung kommen kann.

Verglichen mit der Regelversorgung fehlen in diesem Setting Normsetzungsverfahren wie die gesetzlichen Rahmenbedingungen zur Qualitätssicherung oder die Regelungen der gesetzlichen Krankenversicherungen nach SGB V, die eine verbindliche Basis für Dokumentation, Bedarfsplanung, Transparenz und schlussendlich Qualität der gesundheitlichen Versorgung darstellen. Die Bedingungen für die Akteure, die für Bedarfsplanung und Gestaltung der Versorgungsangebote verantwortlichen sind, sind daher innerhalb und zwischen Regionen und Bundesländern sehr unterschiedlich. Folglich fehlen sowohl regional als auch überregional die

[1] Razum O, Bunte A, Gilsdorf A, Ziese T, Bozorgmehr K. Gesundheitsversorgung von Geflüchteten: Zu gesicherten Daten kommen. Dtsch Arztebl 2016;113:A130-A133

[2] Bozorgmehr K, Noest S, Thaiss MH, Razum O. Die gesundheitliche Versorgungssituation von Asylsuchenden Bundesweite Bestandsaufnahme über die Gesundheitsämter. Bundesgesundheitsblatt 2016;59:545-55.

notwendigen Daten, die für die Bedarfs- und Angebotsplanung sowie für die Entwicklung von übergreifenden Versorgungsstandards erforderlich sind.

Vereinzelt gibt es nicht-repräsentative Fallserien, die auf Datenquellen in Erstaufnahmeeinrichtungen basieren [1]. Deren Aussagekraft ist jedoch durch die Heterogenität der Datenquellen sowie der ausschließlich deskriptiven und von Standort zu Standort unterschiedlichen Analyseansätze sehr begrenzt. Nicht zuletzt gibt es eine große zeitliche Latenz zwischen der Erhebung von Daten sowie deren Auswertung und Berichterstattung.

Daher besteht ein großer Bedarf bei medizinischen Leistungserbringern und Leistungsträgern an einer verlässlichen Datenbasis zum Gesundheitszustand und davon ausgehend zur Planung der medizinischen Versorgungssituation von Asylsuchenden. Nicht zu Letzt steht eine adäquate Datenbasis zur Planung- und bedarfsgerechten Ausgestaltung von Versorgungsangeboten sowie zur Qualitätssicherung der Angebote im Interesse von Asylsuchenden selbst.

Aus diesem Grund hat sich im Rahmen der Dateninitiative „Gesundheit und medizinische Versorgung von Asylsuchenden und Geflüchteten“ ein Netzwerk aus Wissenschaft, Praxis, Öffentlichem Gesundheitsdienst (ÖGD) und Fachabteilungen des Robert Koch-Instituts (RKI) gebildet, um dem Problem der unzureichenden Datensituation sowie der heterogenen und punktuellen Analyse entsprechender Daten nachhaltig zu begegnen. Mit Förderung des Bundesministeriums für Gesundheit (BMG) entstand aus der Initiative das Vorhaben „Surveillance der Gesundheit und primärmedizinischen Versorgung von Asylsuchenden in Erstaufnahmeeinrichtungen und Gemeinschaftsunterkünften in Deutschland“ (Laufzeit: 01.10.2016 - 31.12.2020).

Das Ziel des Vorhabens ist die Verbesserung der Datenlage zur Gesundheit und primärmedizinischen Versorgung von Asylsuchenden in Erstaufnahmeeinrichtungen und Gemeinschaftsunterkünften in Deutschland. Das Vorhaben fokussiert dabei vier Schwerpunkte:

1. Erarbeiten eines einheitlichen Indikatorensatzes zur Gesundheit und zur medizinischen Versorgung von Asylsuchenden in Erstaufnahmeeinrichtungen/Gemeinschaftsunterkünften in Deutschland
2. Etablierung von „Surveillance Sites“ in Erstaufnahmeeinrichtungen/Gemeinschaftsunterkünften verschiedener Bundesländer durch Implementierung einer medizinischen Dokumentationssoftware (RefCare©) und unter Anwendung des einheitlichen Indikatorensatzes.
3. Entwicklung und Implementierung einer geeigneten Infrastruktur zur dezentralen, automatisierten Analyse und einrichtungsübergreifenden Zusammenführung der anonymen Ergebnisse zu Zwecken der Statistik (Surveillance) und Forschung.
4. Zeitnahe und regelmäßige Dissemination von relevanten Ergebnissen der Surveillance (Statistiken) über eine Reporting-Plattform.

Um die Ziele des Projektes zu erreichen, wurde in einem nutzerorientierten, iterativen Prozess zunächst eine Dokumentationssoftware (RefCare©) zur Nutzung in Ambulanzen in Aufnahmeeinrichtungen entwickelt. Nach erfolgreicher Testung in drei Pilotstandorten ist die Software

aktuell (Stand Januar 2020) in insgesamt 22 Standorten in drei Bundesländern (Baden-Württemberg, Bayern und Hamburg) im Regelbetrieb im Einsatz. Die Funktionen der Software beinhalten neben der medizinischen Versorgungsdokumentation im Sinne einer Patientenakte auch administrative Funktionen zur Ambulanzorganisation und die Möglichkeit, Patientenakten mit Einwilligung der Patient*in zwischen mit RefCare© arbeitenden Einrichtungen zu versenden.

Es wurde außerdem eine Infrastruktur zur regelmäßigen statistischen Auswertung (Surveillance) der in RefCare© dokumentierten Behandlungsdaten entwickelt und in den beteiligten Einrichtungen implementiert. Dies erfolgt durch den Ansatz des verteilten Rechnen im Verbund mit dem Ergebnis einer anonymisierten Kennzahl. Gemeinsam mit den beteiligten Einrichtungen wurde ein **Forschungsverbund (PriCare*net*)** gegründet, in dem die Inhalte der Surveillance (Indikatoren) gemeinsam diskutiert und konsentiert werden. Die konsentierten Indikatoren der routinemäßigen Surveillance wurden anschließend in einem Analyseskript umgesetzt und über RefCare© den Einrichtungen zur Verfügung gestellt. Die durch Auslösen dieses Analyseskripts lokal generierten, anonymen Ergebnisse (Kennzahlen) können zunächst lokal in den Einrichtungen eingesehen werden und anschließend aggregiert und ohne jeglichen Personenbezug zusammengeführt, in regelmäßigen Abständen meta-analytisch ausgewertet und berichtet werden. Das Reporting erfolgt in aggregierter Form sowie in einrichtungsspezifischen Feedbackberichten. Im Rahmen der bisherigen Laufzeit des Vorhabens (Stand: Februar 2020) wurde die Machbarkeit des Ansatzes nachgewiesen[2], sodass nun die nachhaltige Nutzung und Verstetigung des Surveillance-Ansatzes sowie die Ausweitung auf weitere Bundesländer im Vordergrund steht.

2.1 Nutzen des Vorhabens

Das Vorhaben verfolgt - auch nach Auslaufen der Bundesförderung zum 31.12.2020 - gemeinsam mit den Beteiligten und relevanten Akteuren aus dem Feld gezielten Infrastrukturaufbau, indem sowohl eine verlässliche Dokumentation der medizinischen Behandlung ermöglicht und diese auch über Einrichtungen hinweg harmonisiert wird. Die Implementierung der dafür erforderlichen Dokumentationssoftware und des Surveillance-Konzeptes erlaubt darüber hinaus eine deutliche Verbesserung der Daten- und Versorgungssituation. Von einer besseren Dokumentation ihrer gesundheitsbezogenen Daten profitieren Asylsuchende, da sie bei Folgebesuchen bei den medizinischen Leistungserbringern nicht wiederholt ihre gesamte Krankengeschichte berichten müssen und somit das Risiko von Unter-, Über- und Fehlversorgung reduziert wird.

Durch die anonyme Surveillance können Häufungen wichtiger Entitäten z.B. von Infektionen bzw. Infektionsausbrüchen, Unfällen, entgleiste chronischen Erkrankungen oder akut-

[2] Nöst S, Jahn R, Aluttis F, Preussler S, Qreini M, Bozorgmehr K. Surveillance der Gesundheit und primärmedizinischen Versorgung von Asylsuchenden in Aufnahmeeinrichtungen: Konzept, Entwicklung und Implementierung. *Bundesgesundheitsblatt. 2019* **62**:881-892

psychiatrischen Erkrankungen quantifiziert und zu Behandlungs- oder Entscheidungszwecken auf lokaler oder überregionaler Ebene berichtet sowie an die Leistungserbringer der behandelnden Einrichtungen als Feedback und Planungsgrundlage zurückgespiegelt werden.

Durch die harmonisierte, dezentrale Sekundärnutzung klinischer Routinedaten im Verbund wird die Vergleichbarkeit lokaler Analysen im Sinne einer synergistischen Forschung und somit eine aktive Surveillance wichtiger Gesundheits- und Versorgungsparameter ermöglicht. Die Notwendigkeit synergistischer Forschungsansätze, die einen Konsens über relevante Fragestellungen erzielen und diese regionenübergreifend beantworten wurde bereits in einer systematischen Übersichtsarbeit der empirischen Literatur der Gesundheit und medizinischen Versorgung Geflüchteter (1990 – 2014) festgestellt[3].

Durch den harmonisierten und synergistischen Forschungsansatz stehen Informationen zu gesundheitlichen Bedarfen der Population der Asylsuchenden sowie zu ihrer Versorgungssituation Versorgern sowie Entscheidungsträgern zeitnah zur Verfügung und ermöglichen es, die Planung gesundheitspolitischer Maßnahmen und Entscheidungen auf einer transparenten Datenbasis zu treffen. Von einer datenbasierten Qualitätssicherung im Rahmen der Surveillance profitieren auch Asylsuchende, da auf dieser Grundlage getroffene überregionale oder lokale Maßnahmen zur Verbesserung der Versorgung in erster Linien auch Ihnen zu Gute kommen.

3 Datenschutz-Folgenabschätzung

In dem vorliegenden Datenschutzkonzept wurde eine Datenschutz-Folgenabschätzung (DSFA) der Verarbeitung von Daten der medizinischen Versorgung von Asylsuchenden und geflüchteten Menschen sowie von Daten zur Sicherstellung der medizinischen Versorgung integriert vorgenommen. Dafür wurden gemäß DS-GVO (DS-GVO Art. 35 Abs.7 lit a-d) die erforderlichen Inhalte der DSFA in den Kapiteln 10 - 12 dargestellt.

Dabei gilt es zu beachten, dass obwohl bei dem Vorgang der Anonymisierung (Anwendungsfall 2) der Personenbezug der personenbezogenen Daten entfernt wird, eine DSFA gemäß Art. 35 Abs. 1 DSGVO durchgeführt werden sollte, „wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.“(Positionspapier vom 29.06.2020 zur Anonymisierung unter der

[3] Bozorgmehr K, Mohsenpour A, Saure D, Stock C, Loerbroeks A, Joos S et al. [Systematic review and evidence mapping of empirical studies on health status and medical care among refugees and asylum seekers in Germany (1990-2014)]. *Bundesgesundheitsblatt* 2016;**59**:599-620.

DSGVO des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) [4]) Auf der Grundlage des Positionspapiers kann weiterhin bei der Anonymisierung angenommen werden, dass ein hohes Risiko besteht, weil zum einen oft „neue Technologien“ zum Einsatz kommen und zum anderen der Aufbau eines anonymen Datenbestandes eine komplexe Aufgabe des Verantwortlichen darstellt und viele Fehlerquellen in sich trägt.

4 Skizzierung des Versorgungssettings und des Vorhabens

Asylsuchende und geflüchtete Menschen werden nach Ihrer Einreise in Deutschland für einen begrenzten Zeitraum (max. 6 Monate) in einer Erstaufnahmeeinrichtung eines Bundeslandes untergebracht. Nach Aufnahme des Asylverfahrens verlassen Asylsuchende meist die Erstaufnahmeeinrichtung und werden dezentral in Wohnungen oder Gemeinschaftsunterkünften in kommunaler Trägerschaft untergebracht[5]. Für die Sicherstellung der medizinischen Versorgung sind im Falle der Unterbringung in einer Erstaufnahmeeinrichtung die oberen Aufnahmebehörden (Landesbehörde bzw. die Behörde des Regierungsbezirks; z.B. Regierungspräsidien) und im Falle der anschließenden kommunalen Unterbringung die unteren Aufnahmebehörden (meist Sozialbehörde/-amt) zuständig.

Dieser Sicherstellungsauftrag (vgl. §4 Abs. 3 AsylbLG) wird nicht nur als finanzielle Sicherstellung gesehen, sondern bedeutet im Falle der Erstaufnahmeeinrichtungen und im Falle von großen Gemeinschaftsunterkünften meist auch das Vorhalten einer angemessenen Anlaufstelle für medizinische Belange bzw. einer medizinischen Versorgungseinrichtung vor Ort. Meist werden hierfür ein oder mehrere Räume in der Unterkunft als medizinische Behandlungsräume ausgestattet oder eigens dafür ausgestattete Behandlungscontainer genutzt.

Zwischen diesen zuständigen Behörden und den medizinischen Leistungserbringern werden zum Zwecke der Sicherstellung der medizinischen Versorgung Kooperationen oder andere Vertragsvereinbarungen getroffen. Die Ausgestaltung der Versorgungsangebote ist bundesweit sehr heterogen. Zwei Szenarien der ärztlichen Tätigkeit zur Leistungserbringung in medizinischen Versorgungseinrichtungen innerhalb von Erstaufnahmeeinrichtungen sind weit verbreitet:

1. Einzelne Ärzte werden entweder im Rahmen Ihrer Niederlassung tätig oder bieten private Leistungen gegen Rechnung bzw. Honorar (Szenario 1)

[4]Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand: 29.Juli 2020, https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2 .

2. Angestellte Ärzte werden tätig im Zuge eines Arbeitsvertrages mit einem Krankenhaus, einem Universitätsklinikum, einem medizinischen Dienstleister, oder einem Gesundheitsamt (Szenario 2)

Kostenträger ist die jeweils zuständige Behörde mit Sicherstellungsauftrag und die Vergütung der Behandlungskosten erfolgt entweder mit den einzelnen Ärzten (Szenario 1) oder den institutionellen Leistungserbringern wie z.B. Krankenhäusern (Szenario 2).

5 Anwendungsfälle und Zweckbestimmung

Ausgehend von den Zielen des Projektes wird auf Grundlage einer elektronischen Dokumentationssoftware („RefCare©“) die ärztliche Primärdokumentation der medizinischen Behandlung von Asylsuchenden und Geflüchteten ermöglicht und die erforderliche technische Infrastruktur installiert. Ausgehend von einem im Verbund der teilnehmenden Leistungserbringer konsentierten Indikatorensatz erfolgen automatisiert harmonisierte Sekundärdatenanalysen lokaler Behandlungsdaten. Aus den lokalen Analysen wird eine einrichtungsübergreifende Statistik zur Surveillance der Gesundheit und medizinischen Versorgung dieser Zielgruppe im Setting von großen Gemeinschaftsunterkünften und Landeserstaufnahmestellen erstellt. Anhand des konsentierten Indikatorensatzes werden lokale Daten aus der Primärdokumentation der Leistungserbringer unterschiedlicher Erstaufnahmeeinrichtungen (sog. Surveillance Sites) in regelmäßigen Abständen lokal seitens der behandelnden Ärzte durch ein automatisiertes Verfahren ausgewertet. Die hierdurch generierten anonymen Kennzahlen werden zu statistischen Zwecken (Surveillance) zusammengeführt, um in der dynamischen Population der Asylsuchenden Trends und Änderungen der Morbiditäts- sowie Versorgungsmuster monitorisieren zu können (z.B. Diabetesprävalenz im zeitlichen Verlauf). Die Ergebnisse dieser deskriptiv-epidemiologischen Analysen können weitere, spezifische Fragestellungen aufwerfen, die über eine reine Statistik bzw. Surveillance hinausgehen (z.B. Zusammenhang zwischen Herkunftsregionen, Body-Mass-Index und Diabetesprävalenz). Auf Grundlage eines Konsortialvertrages mit klaren Konsensfindungs- und Autorisierungsverfahren werden, zu anlassbezogenen Forschungszwecken ein automatisierte harmonisierte Sekundärdatenanalysen lokaler Behandlungsdaten ermöglicht, die wiederum anonyme Kennzahlen generiert und meta-analytisch – ohne Weitergabe personenbezogener Daten an Dritte –über Leistungserbringer und Standorte gepoolt werden kann. Ausgehend von diesen Vorhaben können daher drei Anwendungsfälle unterschieden werden:

5.1 Fall 1: Ärztliche Primärdokumentation (Software RefCare©)

<u>Ärztliche Dokumentation der primärmedizinischen, individuellen Behandlung durch medizinische Leistungserbringer.</u>

(Primärnutzung medizinischer Daten zum Behandlungszweck)

Beteiligte Leistungserbringer nutzen die Software RefCare© („Refugee Care Manager“) zur Primärdokumentation der medizinischen Behandlung und können auf diesem Wege der Dokumentation ihrer Behandlung nach § 630f BGB nachkommen. Die Software RefCare© ermöglicht eine auf Dauer gestellte, zielgruppen- und settingspezifische Behandlungsdokumentation der wesentlichen Inhalte einer ärztlichen Dokumentation unter Berücksichtigung der dafür erforderlichen Software-Funktionalität. Durch die Fokussierung auf das Wesentliche und die settingspezifisch relevanten Funktionalitäten ist die Anwendung als datensparsam zu bezeichnen und berücksichtigt damit eine zentrale Anforderung des Datenschutzes. Die Entwicklung der Software folgt somit bereits bei der Entwicklung und Architektur dem Konzept des „Privacy by design“. Wesentliche Elemente einer Primärdokumentation der medizinischen Behandlung sind (vgl. § 630f BGB):

- die medizinische Anamnese,
- der Behandlungsanlass,
- die medizinischen Befunde,
- die durchgeführten Untersuchungen und die Untersuchungsergebnisse,
- die Diagnosen,
- die Therapien und ihre Wirkungen,
- Eingriffe und ihre Wirkungen,
- Einwilligungen und Aufklärungen,
- Arztbriefe,
- der weitere Behandlungsverlauf.

5.2 Fall 2: Statistik (Surveillance) und Forschung

Sekundärnutzung medizinischer Behandlungsdaten der Leistungserbringer aus Erstaufnahmeeinrichtungen und großen Gemeinschaftsunterkünften zu Zwecken der (1.) Statistik (Surveillance) und (2.) Forschung: Automatisierte, dezentrale Analyse mit dem Ergebnis anonymer Kennzahlen

Das Ziel dieses Anwendungsfalles ist das regelmäßige Generieren von Statistiken zur Abbildung des Gesundheitszustandes Asylsuchender auf Populationsebene und der Qualitätssicherung der Versorgung in Erstaufnahmeeinrichtungen und großen Gemeinschaftsunterkünften (Surveillance). Aufgrund der Dynamiken der Fluchtmigration ist diese Regelmäßigkeit eines Surveillance-Ansatzes von sehr hoher Relevanz, da einmal generierte versorgungsepidemiologische Erkenntnisse nur eine geringe Halbwertszeit haben. Das Einholen einer informierten, persönlichen Einwilligung ist wünschenswert, für ein solches Vorhaben aus mehreren Gründen jedoch nicht umsetzbar:

1. Für eine möglichst unverzerrte Surveillance ist eine Vollerhebung notwendig, eine lediglich punktuelle Erhebung von Daten einer Selektivpopulation unter Ausschluss von Nichtteilnehmenden Individuen kann zu erheblichen Verzerrungen führen.
2. Durch die dafür meist unzureichende Personalausstattung in den Versorgungseinrichtungen ist eine routinemäßige Aufklärung mit Einholen einer schriftlichen Einwilligung

bei allen Patienten unrealistisch und kann zu Lasten der knappen zeitlichen und personellen Ressourcen für medizinische Behandlungszwecke gehen.

3. Bereits bei der medizinischen Behandlung existieren teils massive Sprachhürden, deren Überwindung hinsichtlich einer routinemäßigen angemessenen Information finanziell, strukturell, und personell nicht machbar erscheinen

Zur Erstellung der Surveillance werden daher die Daten aus der primären Behandlungsdokumentation (Elektronische Patientenakte RefCare©) innerhalb der eigenen Server-Strukturen der datenschutzrechtlich verantwortlichen Stelle anonymisiert: Die Daten werden automatisiert verarbeitet (d.h. ohne Weitergabe personenbezogener Daten an Dritte), mit dem Ergebnis einer anonymen Kennzahl (anonymer Output, z.B. aufsummierte Fallzahlen, Prävalenz, aggregierter Qualitätsindikator). Um diese Zweckänderung zur Sekundärdatennutzung datenschutzkonform zu gestalten, erfolgt lokal, durch die Leistungserbringer selbst ausgelöst, eine automatisierte Analyse und in diesem Zuge eine Anonymisierung der medizinischen Behandlungsdaten. Aus den dadurch generierten Kennzahlen ist kein Personenbezug mehr ableitbar (Anonymisierung). Die anonymen Kennzahlen werden im folgenden Schritt einrichtungsübergreifend auf einem Surveillance-Server zentral zusammengeführt, metaanalytisch ausgewertet und aus den Analyseergebnissen Statistiken erstellt. Die Statistiken können zur Bedarfsplanung, Qualitätssicherung sowie zu weiteren Planungs- und Entscheidungszwecken der medizinischen Leistungserbringung in Erstaufnahmeeinrichtungen genutzt werden. Analog zu diesem Vorgehen und auf Grundlage eines Konsortialvertrages mit klaren Konsensfindungs- und Autorisierungsverfahren werden die medizinischen Behandlungsdaten im Rahmen einer Sekundärnutzung auch für anlassbezogene Forschungszwecke verwendet. Der Konsortialvertrag regelt die Bedingungen der Datennutzung (data use) sowie die Anforderungen an das Einbringen von Forschungsvorschlägen sowie die Bereitstellung der anonymisierten Ergebnisse im Verbund der teilnehmenden Leistungserbringer und Kooperationspartner (data access).

Ein Data Use and Access Committee, dem u.a. beteiligte Ärztinnen und Ärzte aus Versorgungseinrichtungen (Leistungserbringer) angehören, prüft eingehende Vorschläge für Analysen zu wissenschaftlichen oder statistischen Zwecken seitens der Verbundpartner (vgl. 10.2.1) und spricht eine Empfehlung für oder gegen die Durchführung der Analysen aus. Basierend auf dieser Empfehlung entscheiden die einzelnen Leistungserbringer auf Grundlage des eigenen Planungsbedarfs und der eigenen Forschungsinteressen über die Teilnahme an einer Analyse. Zur Umsetzung der automatisierten Analyse wird durch das Universitätsklinikum Heidelberg ein Skript (Algorithmus) auf Basis der freien Programmiersprache R programmiert. Das Skript führt bei aktivem Initiieren eines autorisierten Arztes (push-Verfahren) innerhalb der Server-Strukturen der datenschutzrechtlich verantwortlichen Stelle (1.) den lokalen Export der erforderlichen Behandlungsdaten aus der elektronischen Patientenakte RefCare, (2.) die statistischen Berechnungen, (3.) die automatisierte Löschung temporär gespeicherter Daten sowie (4.) die lokale Speicherung der anonymen Kennzahlen durch. Die Differenzierung von Statistik und Forschung wird in Tab. 1 verdeutlicht.

Tab. 1: Unterschiede zwischen Statistik (Surveillance) und Forschung

	Statistik	Forschung
Maßnahme	Surveillance	Versorgungsforschung
Zweck	• lokale Bedarfsplanung und Entscheidungsgrundlage • Qualitätssicherung	• Beschreibung von Assoziationen • Erklärung von Kausalzusammenhängen
Dimensionen	Morbidität, Versorgungsprozesse, Versorgungsqualität, Frühwarnsystem	Outcome hinsichtlich dezidierter Fragestellungen
Auswertung	Deskriptiv	Analytisch
Berichterstattung	• Feedbackbericht an Leistungserbringer (tailored) • Einrichtungsübergreifendes Reporting	• Wissenschaftliche Publikation
Frequenz (lokale Analysen)	Regelmäßige Zeitintervalle	Anlassbezogen/Punktuell
Einholen eines Ethikvotums	Einmalig	Anlassbezogen (Für jede Forschungsfrage)

5.3 Fall 3: Einrichtungsübergreifender Informationsaustausch

Einrichtungsübergreifender Informationsaustausch zwischen medizinischen Leistungserbringern zum Zweck individueller Behandlung

(Primärnutzung medizinischer Daten zum Behandlungszweck)

Zum Zweck der medizinischen Weiterbehandlung werden Behandlungsdaten zwischen den an der Versorgung beteiligten Leistungserbringern auf informationstechnologischem Wege einrichtungsübergreifend ausgetauscht. Dies ist nur bei expliziter Einwilligung des Patienten möglich („privacy by default“).

6 Grundsätze des Artikel 5 DSGVO

Die Grundsätze des Art. 5 DSGVO sind ausgesprochen allgemein gehalten und konkretisierungsbedürftig. Es handelt sich aber keineswegs nur um Programmsätze oder

Optimierungsgebote sondern um verbindliche Regelungen. [6] Dementsprechend hebt auch der EuGH in seiner ständigen Rechtsprechung hervor, jede Datenverarbeitung müsse sowohl den Grundsätzen hinsichtlich der Qualität der Verarbeitung gem. Art. 5 DSGVO als auch den Grundsätzen zur Zulässigkeit der Verarbeitung gem. Art. 6 DSGVO genügen, also auf Basis einer dort genannten Rechtsgrundlage erfolgen (EuGH ZD 2020, ZD Jahr 2020 Seite 36 Rn. ZD Jahr 2020 Seite 36 Randnummer 64 – Google France mwN). Die Grundsätze gelten für jede Datenverarbeitung personenbezogener Daten. Verstöße gegen die Grundsätze des Art. 5 DSGVO sind *bußgeldbewehrt* (Art. 83 Abs. 5 lit. a), was angesichts ihrer Allgemeinheit vor dem Hintergrund des Bestimmtheitsgrundsatzes nicht in allen Fällen unproblematisch ist.[7]

6.1 Rechtmäßigkeit, Abs. 1 lit.a) DSGVO

Gemäß Artikel 5 Absatz 1 lit. a müssen personenbezogene Daten auf rechtmäßige Weise verarbeitet werden. Dies entspricht der Vorgabe von Artikel 8 Abs. 2 S. 1 GRC, wonach personenbezogene Daten nur mit Einwilligung der betroffenen Person oder auf Basis sonstiger gesetzlich geregelter legitimer Grundlagen verarbeitet werden dürfen. Zu den Rechtsgrundlagen, vgl. Kapitel8.

6.2 Zweckbindung, Abs. 1 lit.b) DSGVO

Personenbezogene Daten dürfen nach Abs. 1 lit. b nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden,vgl. Kapitel 5.

6.3 Datenminimierung, Abs. 1 lit. c) DSGVO

Nach Abs. 1 lit. c muss jede Datenverarbeitung dem Zweck angemessen und erheblich sein, zudem muss sie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein *(„Datenminimierung"),* vgl. Kapitel 10.

6.4 Richtigkeit, Abs. 1 lit. d) DSGVO

Nach Abs. 1 lit. d müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle *angemessenen Maßnahmen* zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden, vgl. Kapitel 10.1.1.**Fehler! Verweisquelle konnte nicht gefunden werden.**

[6] BeckOK DatenschutzR/Schantz, 32. Ed. 1.5.2020, DS-GVO Art. 5 Rn. 2

[7] Paal/Pauly/Frenzel, Artikel 5 Randnummer 2; Schantz/Wolff DatenschutzR/Wolff Rn. 1118.

6.5 Speicherbegrenzung, Abs. 1 lit. e) DSGVO

Nach Abs. 1 lit. e müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Durch den Grundsatz der Speicherbegrenzung wird der Grundsatz der *Zweckbindung* und das Verhältnismäßigkeitsprinzip *in zeitlicher Hinsicht konkretisiert* . Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen (Erwägungsgrund 39), vgl. Kapitel 10.

6.6 Vertraulichkeit und Integrität, Abs. 1 lit.f) DSGVO

Nach Abs. 1 lit. f müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Es geht also nicht um eine zusätzliche materielle Schutzdimension, wie sie das BVerfG mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt hat, sondern eher um allgemeine *formelle Vorgaben* hinsichtlich der *Datensicherheit.*[8] Zu den erforderlichen technisch-organisatorischen Maßnahmen, vgl. Kapitel 10 und 12.

6.7 Nachweispflicht, Abs. 2 DSGVO

Der für die Verarbeitung Verantwortliche ist nach Abs. 2 für die Einhaltung der Prinzipien des Art. 5 Abs. 1 verantwortlich und muss deren Einhaltung nachweisen können. Dieser sog. Grundsatz der Rechenschaftspflicht wird durch die Regelung des Art. 24 Abs. 1 S. 1 konkretisiert. Danach sind es in erster Linie „geeignete technische und organisatorische Maßnahmen“, durch die sichergestellt werden soll, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt. Dabei gilt ein sog. risikobasierter Ansatz, der Verantwortliche muss bei den technischen und organisatorischen Maßnahmen Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen.[9] Alle diese Anforderungen werden in diesem Datenschutzkonzept umgesetzt.

[8] Gola DS-GVO/Pötters, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 28

[9] Gola DS-GVO/Pötters, 2. Aufl. 2018, DS-GVO Art. 5 Rn. 30, 31

7 Verantwortlichkeiten

Der Begriff der Verantwortlichkeit wird in Art. 4 Nr. 7 DSGVO definiert. Verantwortlicher ist demnach die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hierbei lässt sich schon erkennen, dass sich der Begriff des Verantwortlichen nicht auf eine einzige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezieht. Verantwortlicher im Sinne der DSGVO können auch mehrere Stellen sein, wenn sie gemeinsam über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Weitere Regelungen zur gemeinsamen Verantwortlichkeit finden sich in Art. 26 DSGVO. Gemeinsame Verantwortlichkeit ist gegeben, wenn eine Verarbeitung selbständige Entscheidungen verschiedener Stellen voraussetzen, d.h. wenn eine Verarbeitung ohne die aktive Beteiligung jeder Stelle nicht denkbar ist, also ein kumulatives Zusammenwirken erfolgt.[10] Das Prinzip der gemeinsamen Verantwortlichkeit war schon in Art. 2 Buchst. d) der Richtlinie 95/46/EG angelegt. Allerdings hatte die Rechtsfigur vor Geltung der DSGVO wenig praktische Relevanz. Stattdessen wurde in diesen Fällen häufig eine Auftragsverarbeitung angenommen und der (Mit-)Verantwortliche zum vermeintlichen Auftragsverarbeiter erklärt. Durch die jüngere Rechtsprechung des EuGH und das Inkrafttreten der DSGVO hat das Thema neue Bedeutung erlangt und wirft in der Praxis noch viele offene Fragen auf.

7.1 Verantwortlichkeiten im Anwendungsfall 1 und 3

Nach aktuellem Recht kann prinzipiell eine Auftragsverarbeitung zwischen dem Leistungserbringer und dem Universitätsklinikum Heidelberg vereinbart werden. Diese setzt aber voraus, dass der Auftragnehmer die Weisungen des Auftraggebers befolgt. Die Daten müssen darüber hinaus von jedem behandelnden Institut sicher und getrennt von den anderen Behandlungsdaten aufbewahrt werden. Diese Trennung hat die Konsequenz, dass unterschiedliche Behandler bei der Behandlung desselben Patienten nicht auf die gleichen Informationen zugreifen können (Mandatentrennung).

Darüber hinaus muss an dieser Stelle § 203 StGB beachten werden. Nach dieser Vorschrift macht sich strafbar, „wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Arzt (...) anvertraut oder sonst bekannt geworden ist.“ Das Verbot der Geheimnisoffenbarung umfasst grundsätzlich auch die Kommunikation zwischen Ärzten. Der Tatbestand des Geheimnisverrats entfällt, wenn die Offenbarung mit Einverständnis des Patienten erfolgt. Das Einverständnis kann ausdrücklich oder konkludent erklärt werden und ist an keine Form

[10] Weichert, DANA 2019, 5.

gebunden. Jedoch dürfte aus Gründen der Rechtssicherheit und Effektivität auch hier die Schriftform vorzugswürdig sein, zumal die datenschutzrechtliche Einwilligungserklärung ohnehin auch schriftlich zu erfolgen hat.

Durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. 10. 2017 hat § 203 StGB nunmehr eine Novellierung erfahren. Zwar hat sich der Gesetzgeber in der Gesetzesbegründung dafür ausgesprochen, dass selbstständig tätige oder in den Betrieb eines Dritten eingebundene externe Personen regelmäßig keine Gehilfen iSd § 203 Abs. 3 Satz 1 StGB sind. Gleichwohl hat er das enorme praktische Bedürfnis für die Auslagerung insbesondere routinemäßig anfallender Tätigkeiten erkannt und im Zuge dessen die Kategorie der *sonstigen mitwirkenden Person* geschaffen, § 203 Abs. 3 Satz 2 StGB. Gegenüber diesen dürfen Berufsgeheimnisträger unter den Voraussetzungen des § 203 Abs. 3 Satz 2 Hs. 1 StGB fremde Geheimnisse straflos offenbaren. „Sonstige mitwirkende Person" ist, wer – etwa aufgrund eines Vertragsverhältnisses – an der beruflichen oder dienstlichen Tätigkeit des Geheimnisträgers mitwirkt, ohne notwendigerweise in dessen Sphäre eingegliedert zu sein. Als mitwirkende Tätigkeiten in dem Sinne wird in der Gesetzesbegründung beispielhaft ua die Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten genannt[11]. Vorliegend stellt das Universitätsklinikum Heidelberg die technischen Voraussetzungen für RefCare bereit und ist somit eine „sonstige mitwirkende Person".

7.2 Verantwortlichkeiten im Anwendungsfall 2: „Statistik (Surveillance) und Forschung"

7.2.1 Verantwortlichkeit des Leistungserbringers

Im Anwendungsfall 2 gehen wir davon aus, dass drei mögliche Konstellationen zur Verantwortlichkeit auf Seiten des Leistungserbringers in Betracht kommen. Es kann jedoch nicht abschließend beurteilt werden, welche der drei möglichen Konstellationen einschlägig ist. Dabei kommt es auf die jeweilige vertragliche Ausgestaltung an.

Zum einen besteht die Möglichkeit die Ambulanz als öffentliche Stelle des Landes als verantwortliche Stelle zu sehen. Dies könnte man annehmen, wenn die Leistungserbringer in der Ambulanz angestellt sind. Dafür spräche auch, dass es für die datenschutzrechtliche Zulässigkeites nicht darauf ankommen kann, woher der Leistungserbringer in die Ambulanz kommt. Wenn die Erstaufnahmeeinrichtung als öffentliche Stelle des Landes als verantwortliche Stelle betrachtet wird, hätte dies den Vorteil, dass die datenschutzrechtliche Rechtslage für die Weiterverarbeitung der in RefCare© gespeicherten Behandlungsdaten allein nach dem Landesdatenschutzgesetzen der beteiligten Länder beurteilt werden könnte.

[11] von dem Bussche/Voigt Konzerndatenschutz, Teil 3. Kapitel 4. Auftragsverarbeitung im Konzern Rn. 12.

Zum anderen kann der jeweilige Leistungserbringer als natürliche Person verantwortliche Stelle sein. Dies könnte der Fall sein, wenn der Leistungserbringer in keinem Arbeitsverhältnis mit der Ambulanz steht, sondern beispielsweise lediglich ein Dienstleistungsvertrag mit der zuständigen Behörde besteht.

Letzlich kommt auch der Dienstleister oder „Vermittler“ der Leistungserbringer als verantwortliche Stelle in Betracht. Dies wäre der Fall, wenn der Leistungserbringer einen Arbeitsvertrag mit dem jeweiligen Dienstleister hat.

Der Leistungserbringer ist somit eine verantwortliche Stelle. Dafür spricht, das die Leistungserbringer für das aktive Auslösen der lokalen, automatisierten Auswertung (Push-Verfahren) sowie für die Prüfung der Ergebnisse und das Auslösen des Datenexports zum Surveillance Server verantwortlich sind. Die Verantwortung für die Qualität und Vollständigkeit der Primärdokumentation im Sinne des § 630f BGB liegt bei den Leistungserbringern. Letzteres ist auch maßgeblich für die Datenqualität einer automatisierten Auswertung.

Außerdem prüft ein Data Use and Access Committee, dem u.a. beteiligte Ärztinnen und Ärzte aus Versorgungseinrichtungen (Leistungserbringer) angehören, eingehende Vorschläge für Analysen zu wissenschaftlichen oder statistischen Zwecken seitens der Verbundpartner (vgl. 10.2.1) und spricht eine Empfehlung für oder gegen die Durchführung der Analysen aus. Basierend auf dieser Empfehlung entscheiden die einzelnen Leistungserbringer auf Grundlage des eigenen Planungsbedarfs und der eigenen Forschungsinteressen über die Teilnahme an einer Analyse.

7.2.2 Verantwortlichkeit des Universitätsklinikums Heidelberg

Das Universitätsklinikum Heidelberg ist im Rahmen des Anwendungsfall 2 „Statistik und Forschung“ ebenfalls eine verantwortliche Stelle. Dafür spricht, dass sie maßgeblich die Verabeitung der Daten zum Zwecke der Statistik und Forschung bestimmt. Dies ergibt sich daraus, dass sie die Prozesse der Datenverarbeitung (Sekundärdatenanalyse) formuliert, die Programmierung und Aktualisierung des R-Scripts vornimmt und die Datenhaltung und Datenverarbeitung der zentral zusammengeführten, anonymen Kennzahlen durchführt. Eine Verantwortung für die Anwendungsfälle 1 („Medizinische Primärdokumentation“) und 3 („Einrichtungsübergreifender Informationsaustausch“) lässt sich sich daraus nicht automatisch ableiten, sondern muss im Einzelfall geprüft werden.

7.3 Gemeinsame Verantwortlichkeit nach Art. 26 DSGVO

Aufgrund der aktuellen Rechtslage ist für den Anwendungsfall „Statistik und Forschung“ davon auszugehen, dass das Universitätsklinikum Heidelberg mit der jeweiligen verantwortlichen Stelle seitens des Leistungserbringers gemeinsam Verantwortlicher gem. Art. 26 DSGVO ist. Dem steht nicht entgegen, dass das Universitätsklinikum Heidelberg keinen Zugriff auf die Daten hat.

Für eine gemeinsame Verantwortlichkeit ist es vielmehr nicht erforderlich, dass jeder der für dieselbe Verarbeitung Verantwortlichen Zugang zu den betreffenden Daten hat. Relevant ist, dass jede Stelle aus Eigeninteresse Einfluss auf die Verarbeitung nimmt und damit an der Entscheidung zur Festlegung über Zwecke und Mittel dieser Verarbeitung faktisch mitwirkt. Dies kann ausdrücklich, aber auch stillschweigend erfolgen. Es ist sogar möglich, dass ein Verantwortlicher gar nicht weiß, mit wem er in gemeinsamer Verantwortung steht. Jeder der Verantwortlichen hat eine rechtliche oder tatsächliche Möglichkeit, Zwecke sowie wesentliche Elemente der Mittel der Verarbeitung zu bestimmen. Die Einflussnahme eines Verantwortlichen kann sich auf die Organisation bzw. Koordinierung der Datenverarbeitung beschränken. Selbst ein Abhängigkeitsverhältnis kann die Grundlage für eine gemeinsame Verantwortung sein, wenn in dem organisatorischen Zusammenhang dem untergeordneten Beteiligten eine wesentliche Bestimmungs- und Einflussmöglichkeit über die Verarbeitung verbleibt[12].

Der Leistungserbringer nimmt Einfluss auf die Verarbeitung, indem er die Entscheidung über die Analysen zu wissenschaftlichen oder statistischen Zwecken trifft und somit über die Zwecke der Datenverarbeitung entscheidet. Seitens des Universitätsklinikums Heidelberg werden die Prozesse der Datenverarbeitung formuliert und das R-Skript programmiert und aktualisiert und zudem findet die Datenhaltung und Datenverarbeitung, der zentral zusammengeführten anonymen Kennzahlen im Universitätsklinikum Heidelberg statt. Somit werden seitens des Universitätsklinikums Heidelberg die Mittel der Verarbeitung festgelegt.

7.4 Folgen der Gemeinsamen Verantwortlichkeit

Die gemeinsame Verantwortlichkeit für den Anwendungsfall der Statistik und Forschung hat verschiedene Rechtsfolgen.

Zunächst kommt es wegen der Tatsache, dass es sich um gemeinsam Verantwortliche handelt, nicht zu einer Erleichterung bei der Beurteilung der Zulässigkeit einer Datenverarbeitung. Es bleibt weiterhin bei dem Erfordernis einer Rechtsgrundlage.

An die verantwortliche Stelle können sich Betroffene zur Wahrnehmung ihrer Rechte, insbesondere Art. 13-22 DSGVO, wenden (Art. 26 Abs. 3 DSGVO). Da die Daten anonymisiert werden, verfügt das Universitätsklinikum Heidelberg nicht mehr über die zur Auskunftserteilung nötigen Informationen. Gemäß Art. 11 Abs. 1 DSGVO ist ein Verantwortlicher nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren. Zur „Einhaltung dieser Verordnung“ gehört auch die Umsetzung der Betroffenenrechte in den Art. 12 ff. DSGVO. Art. 11 DSGVO entbindet den Verantwortlichen von einer weiteren Datenbeschaffung.

[12] Datenschutz und medizinische Forschung gemäß der Datenschutz-Grundverordnung und nationalem Recht – Aktuelle Veränderungen des datenschutzrechtlichen Rahmens nach der EU-DSGVO und anderer Gesetze in der patientenorientierten Forschung – Gutachten Dr. Thilo Weichert im Auftrag der TMF, S. 57.

Folglich kann im Universitätsklinikum Heidelberg den Betroffenenrechten nicht nachgekommen werden.

Was wichtig ist, aber häufig übersehen wird: Art. 26 DSGVO gilt nicht für die Geltendmachung von Schadensersatzansprüchen. Zu den „Rechten der betroffenen Person“ iSv Art. 26 DSGVO gehören zwar die Artikel 15 bis 22 DSGVO. Schadensersatzansprüche sind allerdings gesondert in Art. 82 DSGVO geregelt. Und Art. 82 enthält eine differenzierende Regelung:

Somit ist zwar in Art. 82 DSGVO eine gesamtschuldnerische Haftung angelegt. Diese hängt jedoch nicht von der „Gemeinsamen Verantwortlichkeit“ nach Art. 26 DSGVO ab, sondern nur davon, welche Verantwortlichen an einer Datenverarbeitung „beteiligt“ sind (Art. 82 Abs. 2 und Abs. 4 DSGVO). Unter hohen Voraussetzungen ermöglicht Art. 82 Abs. 3 DSGVO außerdem jedem Verantwortlichen einen individuellen Entlastungsbeweis.

Auch bei den Bußgeldern gibt es keine „gemeinsame“ Bußgeldhaftung, die sich auf Art. 26 DSGVO ergibt. Das Bußgeld wir immer gegen denjenigen verhängt, der auch selbst die DSGVO verletzt hat.

Die „gemeinsame Verantwortlichkeit“ der Verarbeitenden löst nach Art. 26 Abs. 1 DSGVO außerdem die Pflicht aus, eine Vereinbarung zu schließen. In dieser Vereinbarung müssen die Verantwortlichen in erster Linie die Pflichten untereinander aufteilen. Gegenstände der Arbeitsteilung können sein: das Einholen einer Einwilligung (Art. 7 DSGVO); die Information über die Verarbeitung (Art. 12-14 DSGVO), die Bearbeitung von Betroffenenanträgen, etwa auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Verarbeitungseinschränkung (Art. 18 DSGVO) . Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen der Beteiligten widerspiegeln (Art. 26 Abs. 2 S. 1 DSGVO). [13]

Die Vereinbarung muss außerdem in transparenter Form vorliegen. Das heißt, sie muss präzise, leicht zugänglich, verständlich sowie in klarer Sprache abgefasst sein.

7.5 Betroffenenrechte

Jedoch ist seitens des Leistungserbringers als verantwortliche Stelle den Betroffenenrechten nach Art. 13-22 DSGVO nachzukommen. Dabei ist hier insbesondere auf die Informationspflicht nach Art. 13 DSGVO hinzuweisen. Art. 13 DSGVO statuiert umfangreiche Mitteilungspflichten bei der Erhebung der Datenverarbeitung.

Angegeben werden muss nach Art. 13 Abs. 1 lit. a DSGVO der Verantwortliche mit seinem Namen und seinen Kontaktdaten und Angaben zum Vertreter des Verantwortlichen. Nach Art. 13 Abs. 1 lit. b DSGVO müssen die Kontaktdaten des Datenschutzbeauftragten angegeben

[13] Datenschutz und medizinische Forschung gemäß der Datenschutz-Grundverordnung und nationalem Recht – Aktuelle Veränderungen des datenschutzrechtlichen Rahmens nach der EU-DSGVO und anderer Gesetze in der patientenorientierten Forschung – Gutachten Dr. Thilo Weichert im Auftrag der TMF, S. 66.

werden, wenn ein solcher bestellt wurde. Zudem hat der Verantwortliche nach Art. 13 Abs. 1 lit. c über die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, zu informieren. Der Verantwortliche muss gemäß Art. 13 Abs. 1 lit. c die Rechtsgrundlage der Verarbeitung angeben. Nach Art. 13 Abs. 1 lit. e DSGVO sind ggf. die Empfänger oder die Kategorien der Empfänger der personenbezogenen Daten anzugeben. Empfänger ist nach Art. Artikel 4 Nr. 9 S. 1 DSGVO jede Stelle, der personenbezogene Daten offengelegt werden. Dies ist vorliegend aufgrund der Anonymisierung der Daten nicht das Universitätsklinikum Heidelberg. Angegeben werden muss nach Art. 13 Abs. 2 lit. a DSGVO die Dauer, für die die personenbezogenen Daten gespeichert werden oder falls dies nicht möglich ist, die Kriterien für die Festlegung der Dauer. Die betroffene Person ist nach Art. 13 Abs. 2 lit. b-d DSGVO über ihre Rechte aufzuklären. Dazu gehören die Information über den Auskunftsanspruch nach Art. 15 DSGVO, das Recht auf Berichtigung unzutreffender Daten nach Art. 16 DSGVO, das Recht auf Löschung von Daten nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung von Daten nach Art. 18 DSGVO, das Widerspruchsrecht gegen unzumutbare Datenverarbeitung nach Art. 21 DSGVO, das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO, das Recht auf Widerruf einer erteilten Einwilligung nach Art. 7 Abs. 3 DSGVO und das Beschwerderecht bei einer Aufsichtsbehörde nach Art. 77 DSGVO. Eine Aufzählung dieser Rechte genügt. [14]

Fraglich ist, wie man die Informationen bereitstellt. Für die von Art. 13 umfassten Informationen gelten keine speziellen Formerfordernisse.[15] Vielmehr ist auf die allgemeinen Vorgaben aus Art. 12 Abs. 1DSGVO zurückzugreifen. Demnach sind die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“. Vorliegend könnte man beispielsweise die erforderlichen Informationen als Poster in de Ambulanzen aushängen. Zudem sollte die Information in verschiedenen Sprachen zur Verfügung gestellt werden.

Bei der Erstellung der Informationsmaterialien sollten die möglichen Kanäle, wie beispielsweise Flyer oder Handzettel, identifiziert und dann umgesetzt werden. Zudem sollten die gängigsten Sprachen identifiziert werden und das Informationsmaterial dann in diese übersetzt werden. Ansonsten wäre es denkbar, den teilweise in den Ambulanzen verfügbaren Dolmetschern etwas an die Hand zu geben, das sie dann dem Asylsuchenden in seiner Sprache in einfachen Worten erklären können. Desweiteren könnte man die erforderlichen Informationen auf einem Poster in Bildsprache im Wartezimmer der jeweiligen Ambulanz aushängen um auch Analphabeten anzusprechen und mögliche Sprachbarrieren zu überwinden.

Die Erstellung des Informationsmaterials durch die gemeinsam Verantwortlichen wird für Anwendungsfall 2 durch das UniversitätsKlinikum Heidelberg entsprechend unterstützt. Die im Rahmen der Informationspflicht zu erfüllenden Aufgaben werden dabei durch eine Vereinbarung zwischen den gemeinsamen datenschutzrechtlich Verantwortlichen festgehalten.

---

[14] VuR 2019, 213.

[15] BeckOK DatenschutzR/Schmidt-Wudy, 32. Ed. 1.5.2020, DS-GVO Art. 13 Rn. 85.

8 Rechtsgrundlagen

Ausgehend von den im vorigen Kapitel beschriebenen Anwendungsfällen werden im Folgenden die Rechtsgrundlagen für die Fälle der Primärnutzung (Ärztliche Primärdokumentation mit RefCare© und Informationsaustausch zwischen Leistungserbringern) und die Sekundärnutzung (Surveillance und Forschung) der Daten beschrieben. Dabei wird davon ausgegangen, dass Anwendungsfall 1 und 3 rein im Behandlungskontext zu sehen ist und eine genaue Prüfung darum nicht Gegenstand ist.

8.1.1 Datenerhebung und Dokumentation auf Arztrechner zu Behandlungszwecken (Anwendungsfall 1)

Bei Patientendaten handelt es sich um personenbezogene Daten deren Erhebung, Verarbeitung oder Nutzung verboten ist, soweit nicht eine spezielle Erlaubnis durch Rechtsnorm bzw. durch den Betroffenen selbst erteilt ist (Art. 5 Abs. 1 lit.a, 6, 9 DSGVO)Die Ärztin und der Patient vereinbaren in der Regel mündlich das ärztliche Tätigwerden, was regelmäßig die Durchführung von Untersuchungen, Behandlungen bzw. Beratungen umfasst. Die Verarbeitung personenbezogener Daten, könnte zur Durchführung dieses Behandlungsvertrages erforderlich sein und damit nach Art. 9 Abs. 2 lit. h) .V.m. Art. 6 Abs. 1 lit. b) DS-GVO, § 22 Abs. 1 Nr. 1 lit. b BDSG auf Grund des Behandlungsvertrages zulässig sein.

Ärztliche Behandlungs- und Befunddaten stellen besondere Arten personenbezogener Daten gem.Art. 9 Abs. 1 DSGVO dar.Eine Erhebung und Speicherung solcher sensitiver Daten ist zulässig, wenn dies zu Zwecken der Gesundheitsvorsorge, Diagnostik oder Behandlung erforderlich ist(Art. 9 Abs. 2 lit. h) DSGVO .

In Abgrenzung zu einer zulässigen Datenverarbeitung nach Art. 9 Abs. 2 lit. h) i.V.m. Art. 6 Abs. 1 lit. b) DSGVO, § 22 Abs. 1 Nr. 1 lit. b BDSG stellen die Regelungen der § 630f BGB, § 10 Abs. 1 MBO, § 57 Abs. 3 BMV-Ä keine datenschutzrechtliche Gestattungsnorm dar. Diese Normen statuieren lediglich vertragliche und berufsrechtliche Verfahrens- und Dokumentationspflichten im Rahmen der ärztlichen Behandlung.

8.1.2 Übermittlung von Patientendaten an weiterbehandelnden Arzt (Anwendungsfall 3)

Die Übermittlung von Patientendaten an einen weiterbehandelnden Arzt unterliegt ebenfalls dem Verbot mit Erlaubnisvorbehalt(Art. 5 Abs. 1 lit. a, 6, 9 DSGVO). Das bedeutet, dass ein solcher Vorgang nur zulässig ist, wenn ein Gesetz oder eine andere Rechtsvorschrift diesen erlaubt oder der Betroffene eingewilligt hat. Eine Einbeziehung weiterer behandelnder Ärzte wird grundsätzlich im Rahmen des Behandlungsvertrages festgelegt, woraus sich auch die Rechtsgrundlage für weiterbehandelnde Ärzte ergibt. Mit diesen werden dann jeweils eigene Behandlungsverträge geschlossen, die die Rechtsgrundlage für deren Datenverarbeitung bieten. Für die Übermittlung von Patientendaten an einen weiterbehandelnden Arzt kommt § 73

Abs. 1b SGB V in Betracht. Dieser regelt ein Verfahren zur vereinfachten Datenweitergabe zwischen den Haus- und Fachärzten. Voraussetzung für eine Datenübermittlung ist das Einverständnis des Patienten. Die Anwendbarkeit von § 73 Abs. 1b SGB V auf den vorliegenden Fall scheidet jedoch aus. § 73 Abs. 1b SGB V soll den vereinfachten Datenaustausch in der hausarztzentrierten Versorgung ermöglichen. Von einer hausärztlichen Versorgungssituation kann jedoch vorliegend nicht ausgegangen werden. Denn die hausärztliche Versorgung beinhaltet gemäß § 73 Abs. 1 Nr. 1 SGB V eine allgemeine und fortgesetzte ärztliche Betreuung des Patienten. Das geplante Vorhaben entspricht jedoch eher einer ambulanten Erstversorgungssituation. Von einem dauerhaften Arzt-Patienten-Verhältnis kann nicht ausgegangen werden. Folglich kommt eine Anwendung von §73b Abs. 1b SGB V nicht in Betracht. Folglich bedarf es einer Einwilligung des Patienten. Die Schriftform ist nach der DSGVO zwar nicht gefordert, ihre Wahrung ist aber im Hinblick auf Nachweispflichten gem. Art. 7 Abs. 1 DSGVO zu empfehlen.

Darüber hinaus muss bei der Weitergabe von Behandlungsdaten an einen weiterberhandelnden Arzt § 203 StGB beachten werden. Das Verbot der Geheimnisoffenbarung umfasst grundsätzlich auch die Kommunikation zwischen Ärzten(vgl. § 9 Abs. 4 MBO). Der Tatbestand des Geheimnisverrats entfällt, wenn die Offenbarung mit Einverständnis des Patienten erfolgt. Das Einverständnis kann ausdrücklich oder konkludent erklärt werden und ist an keine Form gebunden. Auch soweit in allgemeinen oder bereichsspezifischen Datenschutznormen für ihren jeweiligen Anwendungsbereich die Schriftform als Regelfall oder auch zwingend vorgeschrieben ist. Jedoch dürfte aus Gründen der Rechtssicherheit und Effektivität auch hier die Schriftform vorzugswürdig sein, zumal die datenschutzrechtliche Einwilligungserklärung ohnehin auch schriftlich zu erfolgen hat (s.o.).

8.1.3 Notwendigkeit einer gesetzlichen Rechtsgrundlage für die Anonymisierung der Daten bei den medizinischen Leistungserbringern

Ziel des Projektes ist es, die im Umfeld von Erstaufnahmeeinrichtung entstehenden medizinischen Behandlungsdaten von Asylsuchenden für wissenschaftliche Forschungsfragen und statistische Auswertung (Surveillance) vor Ort und ohne entsprechende Einwilligung zu anonymisieren. Die Behandlungsdaten sind in der speziellen RefCare© Software gespeichert (vgl. 9.1) und werden durch die automatisierte Auswertung bzw. das R-Skript anonymisiert (vgl. 10.2.3). Die auf diesem Weg generierten anonymen Fallzahlen werden durch die Leistungserbringer an die Universitätsklinik Heidelberg übermittelt.

Nach Sinn und Zweck des Datenschutzrechts, das nur die Verarbeitung personenbezogener Daten unter einen Erlaubnisvorbehalt stellt, stellt sich die Frage, ob die automatisierte Generierung von anonymisierten Auswertungsergebnissen, wie sie in dem Anwendungsfall 2 anvisiert wird, überhaupt einer Rechtsgrundlage bedarf.

Hierzu werden zwei verschiedene Rechtsaufassungen vertreten: Nach der ersten ist keine Rechtsgrundlage erforderlich, da durch die Anonymisierung eine Löschung der expliziten bzw. direkten Identifikationsmerkmale erfolgt und ggf. weitere identifizierende Merkmale durch

allgemein gehaltene Aussagen ersetzt werden. Löschungen bedürfen nach herrschender Auffassung keiner gesetzlichen Grundlage und können jederzeit durchgeführt werden. Nach der zweiten Auffassung, wird auch für das verteilte Rechnen mit lokalen Auswertungen und lediglich anonymer Datenweitergabe an andere Stellen eine datenschutzrechtliche Erlaubnis benötigt, weil eben auch die lokale Auswertung eine Verarbeitung personenbezogener Daten darstellt. Die Anonymisierung stellt eine Verarbeitung dar und bedarf als solche einer Rechtsgrundlage. [16]

Im vorliegenden Fall werden die personenbezogenen Daten durch das R-Skript bereits im ersten Schritt in eine csv Datei umgewandelt, in der die identifizierenden Merkmale durch Zufalls-IDs ersetzt werden. Lediglich die für die Abbildung der Indikatoren und wissenschaftlichen Fragestellungen notwendigen Datenfelder sind noch als Exportinformation vorhanden, die nach temporärer lokaler Speicherung automatisch gelöscht werden (vgl. Abbildung 1). Sämtliche zwischengespeicherten Daten werden ebenfalls automatisch bei diesem Vorgang umgehend nach Speicherung der anonymen Kennzahlen gelöscht, ohne dass jemand Einblicke in diesen Verarbeitungsprozess hat. Die als Ergebnis entstandenen Kennziffern sind anonym da auch unter Berücksichtigung des Zusatzwissens des Computers keine Re-Identifikation mehr möglich ist. Daher kann mit der ersten Rechtsauffassung hier gut vertreten werden, dass keine Rechtsgrundlage erforderlich ist. Dies dürfte aber eher eine Mindermeinung darstellen, da der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die gegenteilige Auffassung vertritt. Da diesbezüglich keine Rechtssicherheit besteht, werden im nachfolgenden Kapitel die Rechtsgrundlagen für den Anwendungsfall 2 geprüft, wobei der Fokus auf der Rechtsgrundlage für den Datenverarbeitungsvorgang in der Ambulanz liegt.

8.1.4 Rechtsgrundlagen im Anwendungsfall 2: „Statistik (Surveillance) und Forschung“

Für die unter 5.2 beschriebenen Konstellationen, kommen verschiedene Rechtsgrundlagen in Betracht, die im folgenden beschrieben werden.

8.1.4.1 Rechtsgrundlagen, wenn Ambulanz als verantwortliche Stelle (Konstellation 1)

Für den Fall, dass die Ambulanz als öffentliche Stelle des Landes angesehen werden kann, gelten die jeweiligen Forschungsparagraphen aus den Landesdatenschutzgesetzen der Länder. Die Landesdatenschutzgesetze sind auf die jeweiligen öffentlichen Stellen des Landes anwendbar. In Tab. 2 findet sich eine Übersicht mit den jeweils möglichen Rechtsgrundlagen.

Tab. 2: Übersicht der länderspezifischen möglichen Rechtsgrundlagen

Bundesland	**Rechtsgrundlage**

[16] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand: 29.Juli 2020, S. 5; https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DSGVO-TKG.html.

Bayern	Art. 4, 6 Abs. 2 BayDSG
Baden-Württemberg	§ 13 LDSG BW
Hamburg	§ 11 Abs. 1, 2 LDSG Hamburg
Nordrhein Westfalen	§ 6 Abs. 2 Nr. 2 GDSG NW
Saarland	§ 30 SDSG
Hessen	§ 24 Abs. 1 HDSIG
Berlin	§ 17 Abs. 1 BlnDSG
Brandenburg	§ 25 Abs. 1 BbgDSG
Sachsen	§ 36 Abs. 1 SächsDSG
Sachsen-Anhalt	§§ 10 Abs. 2 Nr. 9, 27 DSG LSA
Bremen	§ 19 Abs. 1 BremDSG
Mecklenburg-Vorpommern	§ 9 Abs. 1 DSG MV
Rheinland-Pfalz	§ 22 Abs. 1 LDSG
Schleswig-Holstein	§ 13 Abs. 1 Nr. 2 LDSG
Thüringen	§ 28 ThürDSG

8.1.4.1 Rechtsgrundlagen, wenn Leistungserbringer als verantwortliche Stelle (Konstellation 2)

Für den Fall, dass der Leistungserbringer als natürliche Person die verantworliche Stelle ist, findet das BDSG Anwendung, da der Leistungserbringer eine vertragliche Verpflichtung mit der zuständigen Behörde hat und es somit nicht darauf ankommt in welchem Anstellungsverhältnis er sich normalerweise befindet. In § 27 BDSG ist von der Möglichkeit Gebrauch gemacht worden, eine Rechtsgrundlage für die wissenschaftliche Forschung ohne Einwilligung zu schaffen. § 27 Abs. 1 BDSG enthält folgende Rechtsgrundlage für z.B. niedergelassene Ärzte: „Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der

Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß §22 Absatz 2 Satz 2 vor."

Hier kommt es also darauf an, dass das Forschungsinteresse das Interesse der betroffenen Person überwiegt.

Für die Nutzung zu Forschungszwecken ist entscheidend, dass die Datenverarbeitung für die Durchführung eines Forschungsvorhabens erforderlich ist und dass das wissenschaftliche Interesse der Forschung das Geheimhaltungsinteresse der betroffenen Person überwiegt. Zudem darf der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden. In Anbetracht der Tatsache, dass nur anonyme Fallkennzahlen an die Forschungseinrichtungen herausgegeben werden, die eine Re-Identifizierung betroffener Personen ausschließen, ist von dem Überwiegen des Forschungsinteresses auszugehen. Der Zweck der Forschung kann auch nicht durch die Einholung von Einwilligungen erreicht werden, da für die Forschung die Gesamtsumme der Gesundheitsdaten von Relevanz sind. Einwilligungen sind jedoch freiwillig bzw. können widerrufen werden, so dass ein einwilligungsbasiertes Vorgehen nicht die Gesamtanzahl an Asylsuchenden beinhaltet.

8.1.4.2 Rechtsgrundlage, wenn Dienstleister als verantwortliche Stelle (Konstellation 3)

Hinsichtlich der Rechtsgrundlage ist auch hier § 27 BDSG einschlägig, weswegen auf Konstellation 2 verwiesen werden kann (vgl. 0).

8.1.5 Zwischenergebnis

Die Rechtslage gestaltet sich komplex und ist abhängig davon, welche Konstellation man als einschlägig betrachtet.

Für die Nutzung zu Forschungszwecken aufgrund der jeweiligen Forschungsklausel des Landesdatenschutzgesetzes ist in der Regel entscheidend, dass die Datenverarbeitung für die Durchführung eines Forschungsvorhabens erforderlich ist und dass das wissenschaftliche Interesse der Forschung das Geheimhaltungsinteresse der betroffenen Person überwiegt. Zudem darf der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden. In Anbetracht der Tatsache, dass nur anonyme Fallkennzahlen an die Forschungseinrichtungen herausgegeben werden, die eine Re-Identifizierung betroffener Personen ausschließen, ist von dem Überwiegen des Forschungsinteresses auszugehen. Der Zweck der Forschung kann auch nicht durch die Einholung von Einwilligungen erreicht werden, da für die Forschung die Gesamtsumme der Gesundheitsdaten von Relevanz sind. Einwilligungen sind jedoch freiwillig bzw. können widerrufen werden, so dass ein einwilligungsbasiertes Vorgehen nicht die Gesamtanzahl an Asylsuchenden beinhaltet.

Hilfsweise kann man sich auch auf die ursprüngliche Rechtsgrundlage der Datenerhebung stützen. Somit würde die ursprüngliche Rechtsgrundlage Weitergelten. Dies stützt sich auf eine Argumentation des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:

Im Regelfall werden die personenbezogenen Daten, die anonymisiert werden sollen, zu einem bestimmten anderen Zweck erhoben. Vorliegend zum Zweck der Behandlung. Eine anschließende Anonymisierung stellt deshalb in diesen Fällen eine Weiterverarbeitung dar, deren Zweck mit dem ursprünglichen Erhebungszweck vereinbar sein muss, vgl. Art. 5 Abs. 1 Buchst.b) DSGVO. Ist diese Vereinbarkeit gegeben, ist die Rechtsgrundlage für die zweckändernde Weiterverarbeitung weiterhin die Rechtsgrundlage, die die ursprüngliche Verarbeitung legitimiert hat. Erwägungsgrund 50 Satz 2 DSGVO bringt den entsprechenden Willen des Verordnungsgebers deutlich zum Ausdruck.[17]

8.1.6 Politische Implikationen: Notwendigkeit einer bundesweiten gesetzlichen Rechtsgrundlage

In Deutschland herrscht ein regelrechter Flickenteppich an datenschutzrechtlichen Regelungen für die Forschung. Auf Grund der in Deutschland zwischen Bund und Ländern aufgeteilten Gesetzgebungskompetenzen finden sich Regelungen zur medizinischen Forschung z. B. im BDSG, in den Landesdatenschutzgesetzen und in den Krankenhausgesetzen der Länder. Diese sehen z. T. sehr unterschiedliche Voraussetzungen für die Verarbeitung personenbezogener Daten vor.

Das nordrhein-westfälische Gesundheitsdatenschutzgesetz (GDSG NW) ermöglicht zum Beispiel die Forschung mit Daten von Patienten, auf die das wissenschaftliche Personal auf Grund der Behandlung ohnehin Zugriff hat (§ 6 Abs. 1 S. 1 GDSG NW). Nach § 12 Abs. 1 HmbKHG darf ein Krankenhaus oder eine Krankenhausgruppe die dort im Zusammenhang mit der Behandlung erhobenen Patientendaten ohne Einwilligung für eigene wissenschaftliche Forschung weiterverarbeiten und -sammeln. Darüber hinaus darf ein Krankenhaus besondere Kategorien personenbezogener Daten ohne Einwilligung für wissenschaftliche Forschung dann verarbeiten und sammeln, wenn die Verarbeitung und Sammlung zu diesem Zweck erforderlich ist und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt. Nach dem HmbKHG muss das Interesse an der

[17] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, Stand: 29.Juli 2020, S. 6, https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DSGVO-TKG.html .

Forschung die schützenswerten Interessen der betroffenen Person lediglich überwiegen. In Nordrhein-Westfalen muss das Forschungsinteresse erheblich überwiegen. [18]

Eine Vereinheitlichung der rechtlichen Rahmenbedingungen im Forschungsbereich ist daher anzustreben, wobei ein ausreichender Schutz der Interessen der Patienten weiterhin zu gewährleisten ist. Eine Harmonisierung wird jedoch auf Grund der unterschiedlichen Regelungskompetenzen mit großen Umsetzungsschwierigkeiten verbunden sein.

9 Daten und Datenkategorien

In diesem Kapitel werden ausgehend von den Anwendungsfällen die zu verarbeitenden Daten und Datenkategorien beschrieben. In der aktuellen Version der geltenden europäischen Datenschutzgrundverordnung (DSGVO) werden in Artikel 9 die besonderen Kategorien personenbezogener Daten erfasst:

- rassische oder ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische Daten,
- biometrische Daten,
- Gesundheitsdaten,
- Sexualleben sowie sexuelle Orientierung.

Diese Datenkategorien werden, sofern beinhaltet, in der Darstellung besonders berücksichtigt.

Zum Zweck der Qualitätssicherung werden Daten sekundär genutzt, lokal analysiert und diese Ergebnisse im Zuge eines Surveillance-Ansatzes zur Berichterstattung anonym ohne Weitergabe personenbezogener Daten an Dritte zentral zusammengeführt. Für diese Sekundärnutzung werden die Anforderungen an Datensparsamkeit und Anonymisierung beachtet.

9.1 Lokale Behandlungsdaten der Leistungserbringer (Datenquelle)

Die Darstellung der Daten wird anhand der Anwendungsfälle differenziert.

9.1.1 Daten Ärztliche Primärdokumentation (Software RefCare©)

Im Rahmen der ärztlichen Primärdokumentation werden im Rahmen einer medizinischen Konsultation durch die Leistungserbringer alle für die medizinische Versorgung notwendigen

[18] ZD-Aktuell 2020, 07046

Daten der Patientinnen und Patienten erhoben und gespeichert. Welche der Daten als Pflichtfelder dokumentiert werden, entscheiden die Ärztinnen und Ärzten in den Versorgungseinrichtungen.

9.1.1.1 Identitätsdaten und medizinische Basisdaten Patienten

Folgende personenbezogene Daten können im Rahmen der Patientenverwaltung mittels RefCare© potentiell erhoben werden:

Stammdaten	**Ausprägung/Form**
Lfd.Nr.	[Laufende Nummer, automatisch generiert]
Kennungs-ID einrichtungsübergreifend	Freitext [Z.B. Nr. des Ankunftsnachweises]
Kennungs-ID einrichtungsintern	Freitext [Z.B. Nr. des Bewohnerausweises]
Geschlecht	Auswahl (männlich; weiblich; unbestimmt)
Vorname	Freitext
Nachname	Freitext
Geburtsdatum	TT.MM.JJJJ
Nationalität	Listenauswahl (Länderliste ISO 3166-1)
Hauptsächlich gesprochene Sprache	Listenauswahl (Sprachenliste ISO 639-1)
Weitere Sprachen [bis 5 Sprachen]	Listenauswahl (Sprachenliste ISO 639-1)
Zusatzdaten	
Unterkunft	Listenauswahl [Zugeordnete Unterkünfte]
Zimmernummer	Freitext
Mobilnummer	Freitext
In Deutschland seit	Freitext
Medizinische Basisdaten	Inkl. biometrischen Daten
Gewicht	Numerisch [kg]
Körpergröße	Numerisch [cm]
Allergien / Unverträglichkeiten	Freitext
Stillend	Auswahl [Ja; Nein; nicht anwendbar]
Schwanger	Auswahl [Ja; Nein; nicht anwendbar]
Bemerkung	Freitext

9.1.1.2 Medizinische Gesundheits- und Versorgungsdaten Patienten

Im Rahmen einer medizinischen Konsultation erfolgt die ärztliche Verlaufsdokumentation und damit verbunden die Speicherung von folgenden Gesundheitsdaten, deren Inhalt und Umfang der Dokumentation von Fall zu Fall unterschiedlich ausfällt.

Daten Konsultation und Verlauf	**Ausprägung/Form**
Anamnese (inkl. Sozialanamnese)	→ Listenauswahl „Beratungsanlass“ (nach ICPC-2) → Freitext (z.B. Eigenanamnese, Familienanamnese, Vegetative Anamnese, Medikamentenanamnese, Genussmittelanamnese, Sozialanamnese)
Befund	Freitext
Vitalparameter	→ Gewicht → Größe → BMI → Herzfrequenz → Temperatur → Blutdruck → Atemfrequenz
Diagnose	→ Listenauswahl „Diagnose“ (nach ICD-10)

	→ Auswahlfeld „Art der Diagnose“ (Gesicherte Diagnose, Verdachtsdiagnose, Zustand nach)
Therapie (inkl. medizinisches Procedere)	Freitext
Fremdbefunde und externe Dokumente	Dokument (pdf-Format)
Medikamentenplan	ATC-Code (Anatomisch-Therapeutisch-Chemische Klassifikation) PZN (Pharmazentralnummer)
Arzneimittelverordnung(KBV-Formular Muster 16)	Strukturierte Formulardaten, inkl. • PZN (Pharmazentralnummer) • Ggfs. Hilfsmittel (inkl. Diagnose ICD-10)
Verordnung von Krankenhausbehandlung (KBV-Formular Muster 2)	Strukturierte Formulardaten, inkl. • Einweisungsdiagnose (ICD-10) • Anlass: Kurativ (Geplant), Unfall, Notfall • Angabe der beiden nächsterreichbaren geeigneten Krankenhäuser
Überweisung/Überweisungsschein (KBV-Formular Muster 5/6)	Strukturierte Formulardaten, inkl. • Überweisungsanlass [Diagnostik, Konsiliaruntersuchung, Therapie (Mit-/Weiterbehandlung), Beratung] • Diagnose/Verdachtsdiagnose (ICD-10) • Zutreffende Gebietsbezeichnung (z.B. Augenheilkunde)
Ggfs. weitere KBV-Formulare	-

9.1.1.3 Benutzerverwaltung

Zu Zwecken der medizinischen Behandlung, Dokumentation und Datenspeicherung ist eine Benutzerverwaltung mit Rollendefinition und Zugriffsrechtevergabe erforderlich. Hierfür werden folgende Benutzerdaten erhoben und gespeichert:

Daten	**Ausprägung/Form**
Lfd.Nr.	[Laufende Nummer, automatisch generiert]
Rolle [Zugriffsrechte]	Auswahl (Administrator; behandelnde Ärztin/Arzt; Gesundheitsfachpersonal)
Personenidentifizierende Daten	
Geschlecht	Auswahl (männlich; weiblich; unbestimmt)
Vorname	Freitext
Nachname	Freitext
Geburtsdatum	TT.MM.JJJJ
Kürzel	Freitext [selbstgewähltes Namenskürzel]
LANR [Lebenslange Arztnummer]	Freitext
Nationalität	Auswahl (Länderliste ISO 3166-1)
Hauptsächlich gesprochene Sprache	Auswahl (Sprachenliste ISO 639-1)
Weitere Sprachen [bis 5 Sprachen]	Auswahl (Sprachenliste ISO 639-1)
Zugangsdaten	
Benutzername	Freitext
Passwort	Freitext
Qualifikation	
Berufsgruppe	Auswahl (Arzt/Ärztin; Kranken- und Gesundheitspfleger/-schwester; Sanitäter/in; Hebamme; Sonstiges Fachpersonal
Berufsjahre (Arzt/Ärztin)	Numerisch (JJ)
Fachgebiet (Arzt/Ärztin)	Listenauswahl[1]
Facharzt-/Schwerpunktbezeichnung (Arzt/Ärztin)	Listenauswahl[1]
Arzt/Ärztin in Weiterbildung	Auswahl (Ja; Nein)

Zusatzqualifikationen	Listenauswahl[1]

[1]Bundesärztekammer/Arbeitsgemeinschaft der Deutschen Ärztekammern: Muster-Weiterbildungsordnung (MWBO) gemäß Beschluss 106. Deutscher Ärztetag 2003

9.1.2 Assessment Einrichtungsstrukturdaten

Die Strukturdaten der Unterkunft werden einmalig bzw. regelmäßig per Assessment bei den Trägern der Unterkunft erfragt. Die Strukturdaten der leistungserbringenden Versorgungseinrichtung werden einmalig bzw. regelmäßig bei einer verantwortlichen Person per Assessment bzw. Strukturqualitätsbogen bei den Leistungserbringern selbst oder bei der Einrichtung erfragt.

9.1.2.1 Strukturdaten der medizinischen Versorgungseinrichtung

Daten	Ausprägung/Form
Lfd.Nr.	[Laufende Nummer, automatisch generiert]
Name der Einrichtung	Freitext
Straße	Freitext
Postleitzahl	Freitext
Ort	Freitext
Telefon	Freitext
Email	Freitext
Daten zur Qualität der Versorgung	Strukturqualitätsbogen

9.1.2.2 Strukturdaten der Unterkunft

Daten	Ausprägung/Form
Lfd.Nr.	[Laufende Nummer, automatisch generiert]
Name der Unterkunft	Freitext
Straße	Freitext
Postleitzahl	Freitext
Ort	Freitext
Art der Unterkunft	Listenauswahl (Erstaufnahmeeinrichtung, Gemeinschaftsunterkunft, Andere)
Maximale Belegungskapazität	Numerisch
Aktuelle Belegungszahl	Numerisch

9.1.3 Weiterentwicklung der Software RefCare©

Die Software RefCare© wird im Verlauf ausgehend von den Anforderungen der medizinischen Leistungserbringer und den Bedarfen der Patienten weiter entwickelt und ggfs. adaptiert. Sofern sich wesentliche Änderungen bezüglich der erhobenen Daten ergeben wird das Datenschutzkonzept entsprechend angepasst.

9.2 Lokal gespeicherte Daten zur Surveillance (Indikatoren)

Zu Zwecken der Surveillance (Statistik) werden die dafür notwendigen Daten aus der Primärdokumentation der Leistungserbringer innerhalb der eigenen Server-Struktur der Leistungserbringer automatisiert weiterverarbeitet. Die Datenauswertung und Berichterstattung erfolgt anhand von vier Domänen:

- Morbidität/Gesundheitsrisiken
- Versorgungsprozesse
- Qualität der Versorgung
- Syndromische Surveillance: Frühwarnsystem

Diese vier Domänen wurden mit allen bisher beteiligten Standorten und Leistungserbringern des Projekts abgestimmt und bilden die Grundlage für die Operationalisierung des einheitlichen Indikatorensatzes. Der lokal gespeicherte Datensatz wird anhand des abgestimmten Analyseplans ausgewertet (siehe Abbildung 1), die dabei generierten Kennzahlen (z.B. Diabetesprävalenz, adjustiert für Alter und Geschlecht) werden zentral zusammengeführt und meta-analytisch seitens der Universitätsklinik Heidelberg ausgewertet. Die für den Zweck der Surveillance notwendigen Daten werden im Folgenden anhand der vier Domänen detailliert dargestellt.

9.2.1 Morbidität

Als Hinweis auf den Gesundheitszustand und die Erkrankungshäufigkeiten werden in Anlehnung an die Gesundheitsberichterstattung des Bundes (GBE) die folgenden Indikatoren herangezogen. Die Indikatoren 3 -32 werden für die Berichterstattung nach Geschlecht und Altersgruppen stratifiziert sowie ggfs. alters- und geschlechtsstandardisiert in Tabellenform dargestellt.

	Indikator	**Zur Berechnung erforderliche personenbezogene Daten (Zur Surveillance anonymisiert)**	**Datenquelle**
	Demografie/Populationen		
1	Gesamtpopulation Einrichtung	-	3
2	Ambulante Behandlungsfälle insgesamt (Inanspruchnahmepopulation)	-	1
	Morbidität		
3	Multimorbidität	ICD-10	1
4	Behinderungen nach Diagnose	ICD-10	1
5	Krankheiten der Haut und Unterhaut nach Diagnose	ICD-10	1
6	Äußere Ursachen von Morbidität und Mortalität nach Diagnose	ICD-10	1
7	Folgen äußerer Ursachen	ICD-10	1
8	Häufige ambulante Diagnosen nach ICD-10	ICD-10	1
9	Krankheiten des Verdauungsystems nach Diagnose	ICD-10	1
10	Krankheiten der blutbildenden Organe nach Diagnose	ICD-10	1
11	Bestimmte infektiöse und parasitäre Erkrankungen	ICD-10	1
12	Meldepflichtige Infektionserkrankungen	ICD-10	1
13	Infektionserreger mit Resistenzen gegen bestimmte Antibiotika oder Chemotherapeutika	ICD-10	-
14	Krankheiten des Kreislaufsystems nach Diagnose	ICD-10	1
15	Hypertonie	ICD-10	1
16	BMI	ICD-10	1
17	Hypercholesterinämie	ICD-10	1
18	Endokrine, Ernährungs- und Stoffwechselerkrankungen nach Diagnose	ICD-10	1
19	Diabetes Mellitus	ICD-10	1
20	Krankheiten des Muskel-Skelett-Systems und des Bindegewebes nach Diagnose	ICD-10	1
21	Neubildungen nach Diagnose	ICD-10	1
22	Krankheiten des Nervensystems nach Diagnose	ICD-10	1
23	Krankheiten der Ohren und des Mastoids nach Diagnose	ICD-10	1
24	Krankheiten der Augen und Augenanhangsgebilde nach Diagnose	ICD-10	1
25	Bestimmte Zustände, die ihren Ursprung in der Perinatalperiode haben nach Diagnose	ICD-10	1

26	Ereignisse im Zusammenhang mit Schwangerschaft, Geburt und Wochenbett	ICD-10	1
27	Häufigkeit von Schwangerschaften	ICD-10	1
28	Psychische Störungen und Verhaltensauffälligkeiten nach Diagnose	ICD-10	1
29	Therapie mit Psychopharmaka	ATC-Codes	
30	Verschreibungen Benzodiazepine	ATC-Codes	
31	Krankheiten des Atmungssystems nach Diagnose	ICD-10	
32	Krankheiten des Urogenitaltrakts nach Diagnose	ICD-10	

1 Primärdokumentation RefCare
2 Strukturerhebung Versorgungseinrichtung
3 Strukturerhebung Unterkunft

9.2.2 Versorgungsprozesse

Folgende Indikatoren wurden hinsichtlich ambulanzinterner sowie schnittstellenübergreifender Versorgungsprozesse über die Einrichtung hinaus formuliert. Die Indikatoren zur schnittstellenübergreifenden Versorgung geben Hinweise auf mögliche Versorgungsbedarfe, die bei der Planung des regionalen Versorgungsangebotes berücksichtigt werden müssen

	Indikator	**Zur Berechnung erforderliche personenbezogene Daten (Zur Surveillance anonymisiert)**	**Datenquelle**
33	Gesamtzahl Patientenkontakte	-	1
34	Durchschnittliche Anzahl Kontakte pro Patient	-	1
35	Inanspruchnahme pro Einwohner	-	1,3
36	10 häufigste Beratungsanlässe	Beratungsanlass (ICPC)	1
37	Faktoren, die den Gesundheitszustand beeinflussen und zur Inanspruchnahme des Gesundheitswesens führen	ICD-10	1
38	Potentiell gesundheitsgefährdende Vorkommnisse (Critical Incidents)	-	3

39	Überweisung zu spezialisierten Fachärzten	Formulardaten der Überweisung/Überweisungsschein (KBV-Formular Muster 5/6)
		• Überweisungsanlass:
		  ○ Diagnostik (Konsiliaruntersuchung)
		  ○ Therapie (Mit-/Weiterbehandlung)
		  ○ Beratung
		• Diagnose/Verdachtsdiagnose (ICD-10)
		• Zutreffende Gebietsbezeichnung (z.B. Augenheilkunde)
			1

40	Einweisung in ein Krankenhaus zur stationären Behandlung	Formulardaten der Verordnung von Krankenhausbehandlung (KBV-Formular Muster 2)
		• Einweisungsanlass
		  ○ Elektiv
		  ○ Unfall
		  ○ Notfall
		• Einweisungsdiagnose (ICD-10)
		• Entfernung der angegebenen beiden, nächsterreichbaren und geeigneten Krankenhäuser
			1

1 Primärdokumentation RefCare
2 Strukturdaten Versorgungseinrichtung
3 Strukturdaten Unterkunft

9.2.3 Qualität der Versorgung

Das Messen der Qualität der Versorgung ist besonders relevant und erfolgt mit dem Ziel des Initiierens von Qualitätsverbesserungsmaßnahmen in den Einrichtungen. Die folgenden Qualitätsindikatoren werden über einen Feedbackbericht an die einzelnen Leistungserbringer und ggfs. Erstaufnahmeeinrichtungen zurückgespiegelt. Jede Einrichtung erhält einen einrichtungsspezifischen Report, in dem die eigenen Ergebnisse der Einrichtung mit den Ergebnissen aller Einrichtungen (anonym) vergleichend dargestellt werden. Die Ergebnisse können sowohl

in die Formulierung übergreifender Versorgungsstandards einfließen als auch für ein internes Qualitätsmanagement genutzt werden.

Um die Qualität der Versorgung abzubilden ist ein Qualitätskonzept notwendig, das im Verlauf des Projektes weiter operationalisiert wird. Das initiale Konzept ist anhand der Qualitätsdimensionen nach Donabedian strukturiert (Struktur-, Prozess-, Ergebnisqualität):

	Indikator	**Zur Berechnung erforderliche personenbezogene Daten (Zur Surveillance anonymisiert)**	**Datenquelle**
	Strukturqualität		
41	Verfügbarkeit eines niedrigschwelligen, primärmedizinischen Versorgungsangebots (Werktage/Woche)	-	2
42	Verfügbarkeit eines niedrigschwelligen, primärmedizinischen Versorgungsangebots (Gesamtstunden/Woche)	-	2
43	Bereitstellung von Informationen zum deutschen Gesundheitssystem (Gesundheitssystemkompetenz)	-	2
44	Qualität des Angebots einer Sprachmittlung durch Dolmetscher	-	2
45	Einhalten der Hygienemaßnahmen (Hygieneplan, Händedesinfektionsspender)	-	2
46	Personalausstattung ärztliches Personal (Vollzeitäquivalente)	-	1/2
47	Personalausstattung nicht-ärztliches Personal (Vollzeitäquivalente	-	1/2
	Prozessqualität		
48	Vorhandensein von Sprachbarrieren	-	1/2
49	Bewilligte Kostenübernahmeanträge	-	1/2
50	Vorhandensein einer Impfanamnese	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender: Ja/Nein	1
51	DPT Impfung bei Kindern <1 Jahr	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
52	DPT Impfung bei Kindern 1-5 Jahre	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
	Grundimmunisierung Diphtherie, Tetanus, Polio begonnen	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
	Grundimmunisierung Diphtherie, Tetanus, Polio vollständig	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
	Häufigkeit intern durchgeführter STIKO Impfungen	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
	Häufigkeit extern durchgeführter STIKO Impfungen	Operationalisierung anhand der Dokumentation des Impfstatus im Impfkalender	1
	Patienten mit HIV-Diagnose unter Therapie		1
	Diabetes Mellitus Therapie		
	Ergebnisqualität		
59	Potentiell inadäquate Antibiotikaverordnungen bei Erwachsenen	Operationalisierung anhand von häufig vorkommenden, selbstlimitierenden Infektionen (Tonsillitis, Bronchitis, Atemwegsinfektion, Sinusitis oder Mittelohrentzündung) und gleichzeitigen Antibiotikaverordnungen: 1. Antibiotikaverordnungen: ATC-Code J01 2. Diagnosestellung einer der genannten Infektionserkrankungen: ICD-10	1
60	Stoffwechselentgleisungen bei Diabetes Mellitus	ICD-10	1
61	Ambulanzsensitive Krankenhauseinweisungen bei Erwachsenen	Operationalisierung der Diagnosen (ICD-10) anhand von einer Liste von ambulanzsensitiven Erkrankungen, die spezifisch für den deutschen Kontext entwickelt wurde und die von der WHO empfohlenen Schlüsselerkrankungen enthält: 1. Einweisungsdiagnose (ICD-10) lt. Formulardaten der Verordnung von Krankenhausbehandlung (KBV-Formular Muster 2)	1
62	Ambulanzsensitive Krankenhauseinweisungen bei Kindern	Operationalisierung der Diagnosen (ICD-10) anhand von einer Liste von ambulanzsensitiven Erkrankungen, die spezifisch für den deutschen Kontext entwickelt wurde und die von der WHO empfohlenen Schlüsselerkrankungen enthält:	1

		Einweisungsdiagnose (ICD-10) lt. Formulardaten der Verordnung von Krankenhausbehandlung (KBV-Formular Muster 2)	

1 Primärdokumentation RefCare
2 Strukturdaten Versorgungseinrichtung (ggfs. ergänzt durch Visitationen)
3 Strukturdaten Unterkunft

9.2.4 Syndromische Surveillance: Frühwarnsystem

Eine Syndromische Surveillance hat zum Ziel, Ausbruchsgeschehen von übertragbaren Infektionserkrankungen frühzeitig zu erkennen. Die Früherkennung von meldepflichtigen und nichtmeldepflichtigen Infektionsgeschehnissen soll durch die Erhebung von Einzelfällen oder Inzidenzanstiegen bestimmter Syndrome gewährleistet werden. Die Auswahl und Definition dieser Syndrome basiert auf Empfehlungen zur syndromischen Surveillance in Massenunterkünften für Asylsuchende des RKI sowie dem Handbuch zur Implementierung von syndromischer Surveillance in Erstaufnahmestellen und anderen Flüchtlingskontexten des Europäischen Zentrums für die Prävention und die Kontrolle von Krankheiten (ECDC). Die Operationalisierung dieser Syndrome basiert auf dokumentierten Beratungsanlässen (nach ICPC), Verdachtsdiagnosen (nach ICD-10) und in Einzelfällen auch der Dokumentation einer erhöhten Körpertemperatur in der RefCare-Software©.

Dabei kann man unterscheiden zwischen Syndromen, bei denen

(i) ein Alarmhinweis bei ***signifikantem Inzidenzanstieg*** erfolgt (Gastroenteritis, Akuter Atemwegsinfekt, Hautparasitose) sowie

(ii) Syndromen, bei denen bereits ein ***Einzelfall*** zur Auslösung eines Alarmhinweises führt (Chronischer Husten, Fieber und Hautausschlag, Meningitis /Enzephalitis, Blutige Diarrhoen, Fieber und Blutungen).

In beiden Fällen erfolgt auf lokaler Ebene in der versorgenden Einrichtung eine unmittelbare Rückmeldung an die behandelnden Ärzte (Leistungserbringer), um eine zeitnahe, einrichtungsinterne Intervention einzuleiten, wie z.B.:

- Weiterführende Diagnostik
- Meldung an das Gesundheitsamt
- Einleiten von Infektionsschutzmaßnahmen

Das Frühwarnsystem wird vorrangig lokal, in den versorgenden Einrichtungen implementiert, sodass keine personenbezogenen Daten an Dritte übermittelt werden. Zur syndromischen Surveillance werden folgende Indikatoren formuliert:

	Indikator	**Zur Berechnung erforderliche personenbezogene Daten (Zur Surveillance anonymisiert)**	**Datenquelle**
	Einzelfallbasierte Indikatoren		
63	Auftreten eines Einzelfalls „Chronischer Husten“ (Zielerkrankung Tuberkulose/Pertussis)	ICD-10- Codes ICPC-Codes	1
64	Auftreten eines Einzelfalls „Fieber und Hautausschlag“ (Zielerkrankung Masern, Varizellen, Rubella, Dengue, u.a.)	ICD-10- Codes ICPC-Codes Vitalparameter (Fieber)	1
65	Auftreten eines Einzelfalls „Meningitis /Enzephalitis“ (Zielerkrankungen: Infektionen durch Meningokokken, HiB, Pneumokokken, Listerien, Tuberkulose, Syphillis, Leptospiren, Cryptokokken, Masern, Mumps, Polio, Enteroviren, u.a.)	ICD-10- Codes ICPC-Codes Vitalparameter (Fieber)	1

66	Auftreten eines Einzelfalls „Blutige Diarrhoen“ Zielerkrankungen: Enteroinvasise bakterielle Infektionen (E-HEC, EIEC), C difficle, Amöbenruhr)	ICD-10- Codes ICPC-Codes	1
67	Auftreten eines Einzelfalls „Fieber und Blutungen“ (Zielerkrankungen: Hämorrhagisches Fieber, z.B. Gelbfieber, Dengue, Ebola, u.a.)	ICD-10- Codes ICPC-Codes Vitalparameter (Fieber)	1
	Indikatoren, basierend auf kumulativem, signifikantem Inzidenzanstieg von Symptomen/Syndromen		
68	Inzidenz „Akuter Atemwegsinfekt“ (Zielerkrankungen: Pharyngitis, Tracheitis, Bronchitis, Bronchopneumonie – u.a. durch: Influenza, Parainfluenza, RSV, Adenoviren, Rhinoviren , Bakterien (Streptokokken, Pneumokok-ken, Mykoplasmen, u.a.)	Operationalisierung anhand der auslösenden Kombination von • Beratungsanlass (nach ICPC) • Verdachtsdiagnose (nach ICD-10) • Vitalparameter (Fieber)	1
69	Inzidenzanstieg „Gastroenteritis“ (Zielerkrankungen: Noroviren, Rotaviren, Staphylokokken, Salmonellen, u.a.)	Operationalisierung anhand der auslösenden Kombination von • Beratungsanlass (nach ICPC) • Diagnose (nach ICD-10)	1
70	Inzidenzanstieg „Hautparasitose“ (Zielerkrankungen: Skabies / Läuse)	Operationalisierung anhand der auslösenden Kombination von • Beratungsanlass (nach ICPC) • Diagnose (nach ICD-10) • Medikamentenverordnung (nach ATC)	1
71	Inzidenzanstieg „Akuter Ikterus“	Operationalisierung anhand der auslösenden Kombination von • Beratungsanlass (nach ICPC) • Diagnose (nach ICD-10) •	

1 Primärdokumentation RefCare
2 Strukturerhebung Versorgungseinrichtung (ggfs. ergänzt durch Visitationen)
3 Strukturerhebung Unterkunft

Im Rahmen der routinemäßigen, einrichtungsübergreifenden Surveillance (Statistik) werden lediglich anonymisierte Alarmhäufigkeiten (bei Inzidenzindikatoren) sowie Tagesinzidenzen (bei Einzelfallindikatoren) ausgewertet. Eine Re-identifikation von Patienten anhand der Ergebnisse der routinemäßigen Surveillance ist daher nicht möglich.

10 Beschreibung der datenbezogenen Prozesse

Die datenschutzbezogenen Prozesse werden im Folgenden anhand der in Kapitel 5 beschriebenen Anwendungsszenarien beschrieben.

10.1 Ärztliche Primärdokumentation (Software RefCare)

10.1.1 Prozesse in der Versorgungssituation

Bei der RefCare-Software handelt es sich um eine Intranet-Lösung, d.h. der Webserver und die Datenbank liegen auf einem eigenen, lokalen Server der datenschutzrechtlich verantwortlichen Stelle (dezentral). Der Zugriff zu Zwecken der ärztlichen Primärdokumentation erfolgt mittels Endgerät (Laptop/Tablet/PC) per Browser über ein Netzwerk (LAN/WLAN) in der Verantwortung der leistungserbringenden Versorgungseinrichtung. Alternativ kann ein Zugriff auf den Web-Server Remote über eine VPN Verbindung z.B. über LTE (o.ä.) erfolgen.

Zugriff, Dateneingabe, Benutzerverwaltung

Der behandelnde Arzt loggt sich mit seinen Benutzerdaten (Benutzername und Passwort) in die RefCare-Software ein und öffnet die Patientenakte des Patienten. Er gibt Daten, die zum

Zweck der medizinischen Behandlung dokumentiert werden, über die Tastatur ein und speichert diese.

Darüber hinaus ist über ein Patienteninterface die Eingabe von Daten zur Beantwortung von Fragebögen durch die Patienten selbst möglich. Dies erfolgt über Tablets, die über WLAN mit dem Server verbunden sind, auf dem RefCare© installiert ist. Die Tablets werden durch den behandelnden Arzt über RefCare© für den jeweiligen Patienten und ausgewählten Fragebogen individuell freigeschaltet. Daraufhin wird in RefCare© ein Code generiert, den der Arzt im vorgesehenen Tablet eingeben muss um dort den Eingabemodus zu öffnen. Das Tablet wird erst nach dieser Autorisierung an den Patienten ausgehändigt. Der Patient kann nun über den Touchbildschirm oder eine Tastatur Eingaben vornehmen und nach beendigen des Fragebogens, z.B. eines mehrsprachigen Anamnesebogens, das Tablet zurückgeben. Für weitere Fragebögen oder weitere Patienten muss der Arzt das Gerät neu autorisieren. Der Patient loggt sich hierbei nicht in RefCare© ein. Das Umfragetool liegt in einem separaten Verzeichnis und besitzt keine Durchgängigkeit zu den Patientendaten.

Die Datenhaltung erfolgt dezentral durch die datenschutzrechtlich verantwortliche Stelle.

Nur der behandelnde Arzt und autorisiertes medizinisches Personal haben Zugriff auf die Patientenakte des Patienten. Jeder Benutzer bekommt eine Rolle zugewiesen. Die Zuordnung von Nutzern zu Rollen wird in der Benutzerverwaltung dezentral, d.h. innerhalb der leistungserbringenden Versorgungseinrichtung, von einem Administrator durchgeführt. Nur ein Administrator ist berechtigt, Rollen zu ändern und Passwörter zu setzen. Über das Patienteninterface können keine Patientendaten gelesen werden, Patienten erhalten keinen Zugriff auf Patientenakten.

Plausibilität und Vollständigkeit

Die RefCare-Software prüft vor dem Speichern die Plausibilität und Vollständigkeit der Benutzereingaben, die im Rahmen der ärztlichen Dokumentation durchgeführt werden (z.B. Formate, Pflichtfelder). Der Benutzer bekommt im Falle von Unplausibilität und/oder Unvollständigkeit eine Warnmeldung.

Datenspeicherung

Die eingegebenen Daten werden in einer lokalen Datenbank auf eigenen Servern der datenschutzrechtlich verantwortlichen Stelle. Zusätzlich können behandlungsrelevante Dokumente (z.B. Arztbriefe, externe Befunde) patientenbezogen als Dokumente abgelegt werden. Das aufkommende Datenvolumen für jede einzelne leistungserbringende Versorgungseinrichtung ist abhängig vom Format der gespeicherten Dokumente und der Anzahl der behandelnden Patientinnen und Patienten, ist aber insgesamt betrachtet als mittel einzustufen.

Patienten-ID

Im Zuge der ersten Konsultation wird jedem Patienten eine eindeutige Kennung (Patienten-ID) zugeordnet. Hierzu werden systemseitig automatisch laufende Nummern generiert. Über diese eindeutige ID können auch Folgebesuche in der Patientenakte dokumentiert und ein

Behandlungsverlauf über Zeit dargestellt werden. Die Patienten-ID (Patientenliste) wird ausschließlich zu Behandlungszwecken lokal in der Datenbank der datenschutzrechtlich verantwortlichen Stelle gespeichert und ist durch die Benutzerverwaltung durch nicht-autorisierten Zugriff geschützt.

Technische Voraussetzungen der ärztlichen Primärdokumentation mittels RefCare

Die technischen Voraussetzungen für die Umsetzung der unter Kapitel 5.1 beschriebenen ärztlichen Primärdokumentation sind abhängig von den Anforderungen der Behandlungsdokumentation mittels der RefCare© Software

Standortseitig kann auf eine eventuell bereits vorhandene EDV Infrastruktur zurückgegriffen werden, soweit vorhanden, kompatibel, datenschutzkonform und sicherheitstechnisch möglich. Ansonsten kann ein handelsüblicher, aktueller Windows Rechner mit Betriebssystem ab Windows 8.1 als Server genutzt werden, auf dem die Software läuft. Bei Leistungserbringern, die gleichzeitig mehrere Dokumentationsplätze betreiben, kommen Endgeräte zur ärztlichen Dokumentation zum Einsatz, die über LAN/WLAN oder alternativ LTE mit dem lokalen Server der datenschutzrechtlich verantwortlichen Stelle verbunden sind.

10.1.2 Kommunikationsprozesse und dezentrale Datenhaltung durch die Leistungserbringer

Die Endgeräte (Laptop/ Tablet/PC) übertragen die über eine Browseranwendung eingegebenen Daten der medizinischen Behandlung zu Dokumentationszwecken über den Weg einer TLS-gesicherten Verbindung direkt zum lokalen Server des Leistungserbringers. Die Daten werden dort in einer relationalen Datenbank gespeichert. Die Daten (vgl. Kapitel 10.1.1), die über die Endgeräte dokumentiert werden, werden nach Aktivieren der Schaltfläche "Speichern" innerhalb des Browsers auf den lokalen Server der Leistungserbringer übertragen und in der Datenbank gespeichert. Jeder Speichervorgang schreibt die Daten in die Datenbank. Es werden **keine Daten zu Behandlungs- und Primärdokumentationszwecken außerhalb der Zuständigkeit der datenschutzrechtlich verantwortlichen Stelle gespeichert**.

10.1.3 Datennutzung und Auswertung

Die dezentral gespeicherten Daten werden im Rahmen der ärztlichen Primärdokumentation zum Zweck der medizinischen Behandlung seitens der Leistungserbringer genutzt.

10.1.4 Löschung/Anonymisierung

Zum Zweck der ärztlichen Primärdokumentation erfolgt keine Anonymisierung der Daten. Die Speicherfrist der Behandlungsdaten beträgt 10 Jahre, empfohlen werden aus forensischen Gründen 30 Jahre. Das Löschen während der Speicherfrist von 10 Jahren ist nicht möglich. Etwaige Änderungen der Dokumentation werden als eindeutig nachvollziehbar gekennzeichnet (Veränderung, Zeitpunkt, Nutzer).

Für die Durchführung der Archivierung, Einhaltung der Speicherfrist und Löschung der Behandlungsdaten nach 10 Jahren ist die datenschutzrechtlich verantwortliche Stelle zuständig.

10.2 Statistik (Surveillance) und Forschung

Zweck der Surveillance ist eine regelmäßige, über mehrere Standorte und Einrichtungen hinweg harmonisierte Erstellung von Statistiken zum Gesundheitszustand der Population Asylsuchender und zur Abbildung der Versorgung und Versorgungsqualität in Erstaufnahmeeinrichtungen und großen Gemeinschaftsunterkünften. Basierend auf relevanten medizinischen Behandlungsdaten erfolgt eine indikatorbasierte, automatisierte und lokal durchgeführte Sekundärdatenanalyse (vgl. 10.2.2). Die dadurch generierten anonymen Kennzahlen werden auf einen zentralen Surveillance-Server exportiert zur einrichtungsübergreifenden Metaanalyse und Berichterstattung (vgl. 10.2.7). Technisch analog zu diesem Verfahren erfolgt eine anlassbezogene Forschung im Verbund der teilnehmenden Leistungserbringer (vgl. 10.2.8) .Um die Interessen der einzelnen Leistungserbringer bei der Auswahl der Inhalten der Statistik (Surveillance) sowie bei der Formulierung der Forschungsfragen zu berücksichtigen, wurde ein Forschungsverbund eingerichtet, der sowohl die Inhalte als auch die Nutzung der Daten regelt (PriCare*net*) (vgl. 10.2.1)

Im Folgenden werden die entsprechenden Bedingungen und datenbezogenen Prozesse beschrieben. Der Überblick über den Datenfluss ist in Abbildung 2 dargestellt.

10.2.1 Abstimmung der Surveillance und Forschung im Forschungsverbund PriCare*net*

Grundlage einer automatisierten Auswertung der Behandlungsdaten durch die einzelnen Leistungserbringer ist ein standardisierter Indikatorensatz, der im Forschungsverbund PriCare*net* konsentiert wird (vgl. Abbildung 2)

Im Forschungsverbund PriCare*net* sind alle teilnehmenden Leistungserbringer und ggf andere datenschutzrechtlich verantwortliche Stellen und kooperierende wissenschaftliche Partner vertreten. Der Forschungsverbund PriCare*net* wurde durch Unterzeichnung eines Konsortialvertrages zwischen den Kernpartnern Universität Bielefeld, St. Josef Klinikum Schweinfurt und dem UniversitätsKlinikum Heidelberg als Verbundleitung gegründet. Weitere Einrichtungen können dem Forschungsverbund über eine Beitrittserklärung beitreten. Jeder Verbundpartner bestimmt einen stimmberechtigten Vertreter, der bei Entscheidungen des Verbundes abstimmen darf, sowie einen stellvertretenden Vertreter.

Der Forschungsverbund PriCare*net* regelt die Forschung im Verbund im Rahmen des Anwendungsfall 2. Er beinhaltet drei Organe:

10.2.1.1 Verbundleitung

Die Verbundleitung vertritt die Interessen des Verbundes gegenüber Dritten, koordiniert Öffentlichkeitsarbeit und Kommunikation der Ergebnisse der Surveillance und übernimmt koordinative und organisatorische Aufgaben des Verbundes.

10.2.1.2 Data Use and Access Committee (DUAC)

Das DUAC besteht aus vier Personen und ist paritätisch besetzt mit Vertretern der wissenschaftlichen Partner und medizinischen Leistungserbringern. Es wird alle zwei Jahre auf dem Verbundtreffen gewählt. Das DUAC hat eine Beratungs- und Vorschlagsfunktion zu eingehenden Vorschlägen der Verbundmitglieder in Bezug auf Inhalte der Surveillance (Statistik) und Forschung. Es spricht nicht-bindende Empfehlungen an die Verbundpartner aus.

10.2.1.3 Verbundbeirat

Der Verbundbeirat besteht aus jeweils ei einer/m Vertreter/in des Bundesministeriums für Gesundheit, des Robert Koch Instituts sowie der Behörden, die zuständig sind für die teilnehmenden Aufnahmeeinrichtungen, jedoch nicht datenschutzrechtlich verantwortliche Stelle sind. Der Verbundbeirat kann Inhalte der Surveillance (Statistik) und Forschung vorschlagen. Die Mitglieder des Verbundbeirates sind keine Mitglieder des Verbundes und haben kein Wahlrecht.

10.2.1.4 Verbundtreffen

Das Verbundtreffen findet einmal jährlich sowie auf Antrag statt. Auf dem Verbundtreffen werden die Inhalte der Surveillance (Statistik) und Forschung diskutiert und konsentiert. ZUdem wir das DUAC gewählt und es können Empfehlungen für Verbundleitung und DUAC erarbeitet werden. Stimmberechtigt sind Mitglieder des Verbundes (Medizinische Leistungserbringer, andere datenschutzrechtliche verantwortliche Stellen sowie wissenschaftliche Partner). Auch bei Konsentierung eines Forschungsvorhaben im Verbund und einer vorliegenden positiven Empfehlung des DUAC liegt die Entscheidung zur Teilnahme bei den einzelnen Einrichtungen und ist freiwillig. Hierdurch wird sichergestellt, dass das ärztliche Eigeninteresse des behandelnden Arztes und somit auch ein Interesse zur Teilnahme und ggfs. zur Eigenforschung berücksichtigt bleiben.

Der Indikatorensatz wurde anhand der vier Domänen operationalisiert, die in Vorgesprächen abgestimmt und im Forschungsverbund (inkl. der Leistungserbringer der Pilotphase) konsentiert:

- Morbidität/Gesundheitsrisiken
- Versorgungsprozesse
- Qualität der Versorgung
- Syndromische Surveillance: Frühwarnsystem

Anhand dieser vier Domänen wurde ein initialer Indikatorensatz operationalisiert (vgl. 9.2)

10.2.2 Automatisierte Analyse lokaler Daten durch die einzelnen Leistungserbringer

Die im Rahmen der medizinischen Behandlung dokumentierten Primärdaten werden anhand eines einheitlichen Indikatorsatzes zu Zwecken der Surveillance regelmäßig zur Sekundärdatenanalyse genutzt.

Alle Daten, die zur Berechnung der Indikatoren notwendig sind, werden anhand eines im Forschungsverbund PriCare*net* konsentierten Analyseplans automatisiert und innerhalb der lokalen Server-Strukturen der datenschutzrechtlich verantwortlichen Stelle ausgewertet, mit dem Ziel der Erstellung anonymer Kennzahlen. Die dafür notwendigen Zwischenergebnisse werden im Zuge des automatisierten Auswertungsprozesses als csv-Datei auf dem lokalen Server der datenschutzrechtlich verantwortlichen Stelle temporär gespeichert und nach Erstellung der anonymen Kennzahl wiederum automatisiert gelöscht. Aus dem Ergebnis der anonymen Kennzahl ist kein Personenbezug mehr herstellbar. (vgl. Abbildung 1)

10.2.2.1 Schritte des automatisierten Auswertungsprozesses

Die automatisierte Auswertung mit anonymem Output der Kennzahlen umfasst die folgenden wesentlichen Schritte:

i. Aktives Auslösen eines lokalen Exports aus den Datenbanken der Primärdokumentation zu definierten Zeitpunkten durch die Aktivierung einer Schaltfläche in der RefCare-Software (Push-Verfahren).
ii. Der Export der Daten erfolgt in Form einer csv-Datei mit den zur Berechnung der konsentierten Indikatoren erforderlichen Daten. Diese csv-Datei beinhaltet keine eindeutig personenidentifizierenden Merkmale wie bspw. Namen oder Geburtsdatum. Die csv-Datei wird temporär auf dem Server der datenschutzrechtlich verantwortlichen Stelle gespeichert und einer Fallzahlprüfung bzw. einer Prüfung der Belegung der erforderlichen Zellen unterzogen.
iii. Entlang der definierten Analyseschritte erfolgt automatisiert eine Weiterverarbeitung mit Reduktion der personenbezogenen Merkmale und eine Analyse mittels definierter Analyseverfahren (z.B. Erstellung einer einfachen Relation aus Fallzahlen, einfache oder multiple logistische Regressionsvefahren).
iv. Die dadurch generierten anonymen Kennzahlen (Output) werden lokal gespeichert.
v. Alle temporär gespeicherten Exporte aus den Datenbanken der Primärdokumentation (csv-Dateien) werden automatisiert gelöscht.

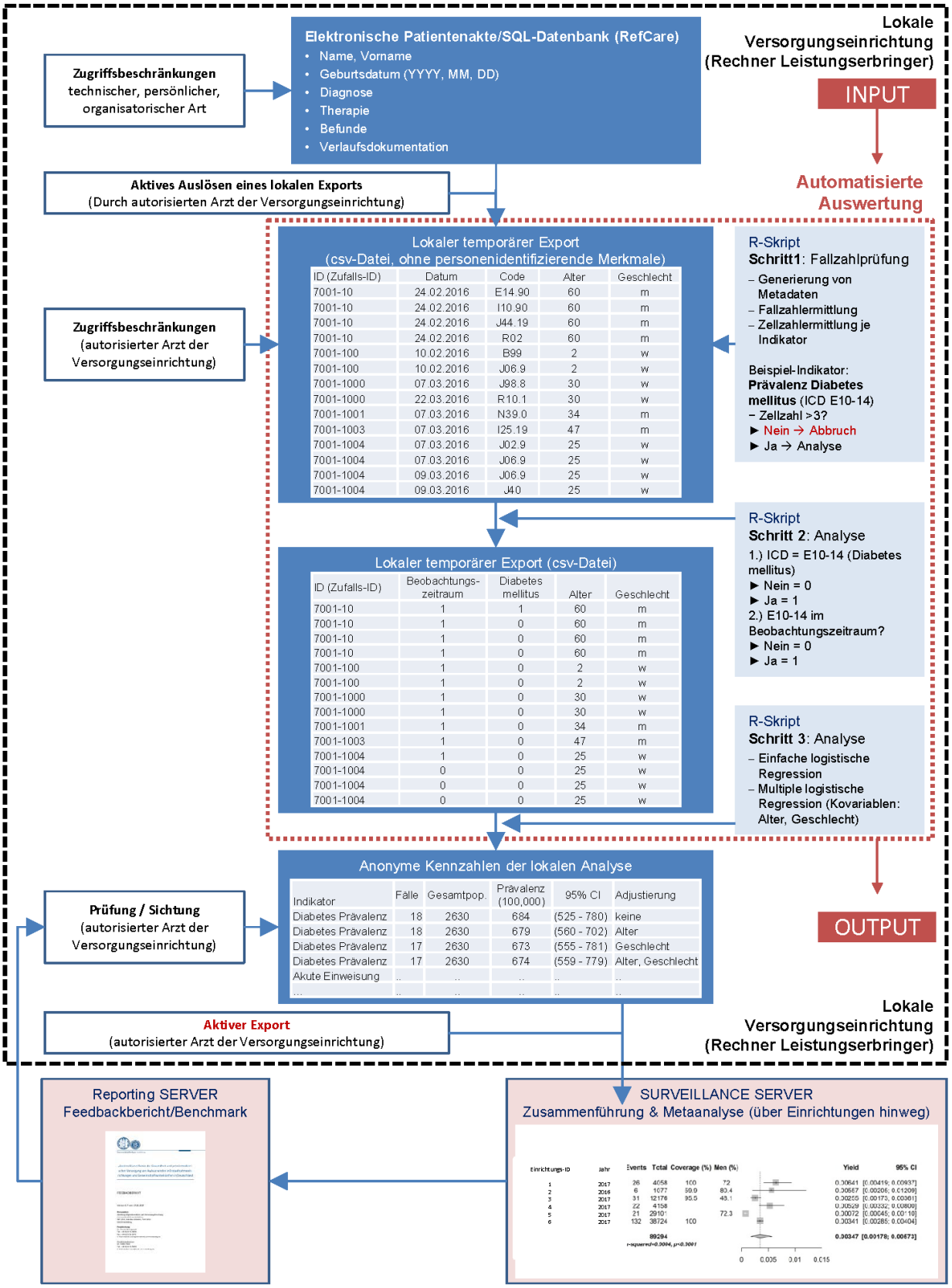

Abbildung 1: Automatisierte Auswertung am Beispiel des Indikators "Prävalenz Diabetes mellitus"

10.2.3 Grundlage der automatisierten Auswertung: Programmierung eines R-Skriptes und Transfer auf den lokalen Server der datenschutzrechtlich verantwortlichen Stelle

Zur automatisierten Auswertung wird durch das Universitätsklinikum Heidelberg ausgehend von den im Verbund konsentierten Indikatoren und dem Analyseplan ein Skript (Algorithmus) auf Basis der freien Programmiersprache R programmiert. Das Skript führt bei aktivem Initiieren eines autorisierten Arztes (1.) die lokalen Exporte der csv-Datei, (2.) die statistischen Berechnungen, (3.) die automatisierte Löschung der temporär gespeicherten csv-Dateien sowie (4.) die lokale Speicherung der anonymen Kennzahlen durch.

Das R-Skript wird in Abhängigkeit von der Abstimmung der Inhalte Forschungsverbund PriCare*net* (vgl. Kapitel 5) über den ZeDAC (Zentraler Datenaustausch Container) Server den Leistungserbringern zur Verfügung gestellt bzw. über dieses Verfahren aktualisiert (vgl. Abbildung 2)

10.2.4 Zentrales Zusammenführen der anonymen Kennzahlen (KTM-ZeDAC-Verfahren)

Die anonymen Kennzahlen (anonymisiertes Ergebnis der lokalen, automatisierten Auswertung) werden in regelmäßigen Abständen mittels der RefCare-Software von den Servern der datenschutzrechtlich verantwortlichen Stelle auf einen zentralen Surveillance-Server des Universitätsklinikums Heidelberg exportiert. Die Zeitintervalle des Exports liegen bei einem Monat, können aber in Abhängigkeit von Änderungen der Inhalte der Surveillance im Forschungsverbund PriCare*net* adaptiert werden Der verantwortliche, behandelnde Arzt einer Einrichtung (Leistungserbringer) stößt den Prozess des Datenexports aktiv an, in dem er die Export-Schaltfläche aktiviert (Push-Verfahren). Durch die Aktivierung der Exportschaltfläche werden die anonymen Kennzahlen als Ergebnis der vorab definierten Indikatoren (vgl. Kapitel 9.2) von dem lokalen Server der datenschutzrechtlich verantwortlichen Stelle mittels des generischen KTM-ZeDAC-Verfahrens sicher auf den zentralen Surveillance-Server übertragen. Die übermittelten Daten (anonymen Kennzahlen) sind frei von jedem Personenbezug. Das Datenvolumen ist gering, da R-, pdf- und excel-dateien übermittelt werden.

Die Kennzahlen ohne Personenbezug werden nach dem folgenden KTM-ZeDAC-Verfahren von dem lokalen Server der datenschutzrechtlich verantwortlichen Stelle zu dem zentralen Surveillance Server übertragen:

- Der nach dem Rollenkonzept autorisierte Benutzer (i.d.R. ein behandelnder Arzt) startet den Export der Daten zur Surveillance innerhalb der RefCare-Software (Push-Verfahren)
- Es werden ausschließlich die Kennzahlen exportiert, die anhand der Indikatorbeschreibungen zur Surveillance notwendig sind. Im Sinne einer Datensparsamkeit wird somit eine Vorratsdatenhaltung vermieden.

- Die RefCare-Software übergibt die anonymen Daten an das KTM (Krytopgraphie- und Transport-Modul). Dieses komprimiert und verschlüsselt die Daten mit dem öffentlichen Schlüssel des Ziels (Surveillance-Server).
- Das KTM legt die dadurch entstandene Transport-Datei auf dem externen ZeDAC (Zentraler Datenaustausch-Container) über eine TLS-gesicherte Verbindung ab.
- Das KTM des Ziels (Surveillance-Server) holt diese Transport-Datei auf dem externen ZeDAC über eine TLS-gesicherte Verbindung ab, entschlüsselt sie mit dem privaten Schlüssel des Ziels und dekomprimiert die Daten.
- Die anonymen Kennzahlen der leistungserbringenden Versorgungseinrichtungen stehen auf dem Surveillance-Server für die Erstellung der Berichterstattung zur Verfügung.

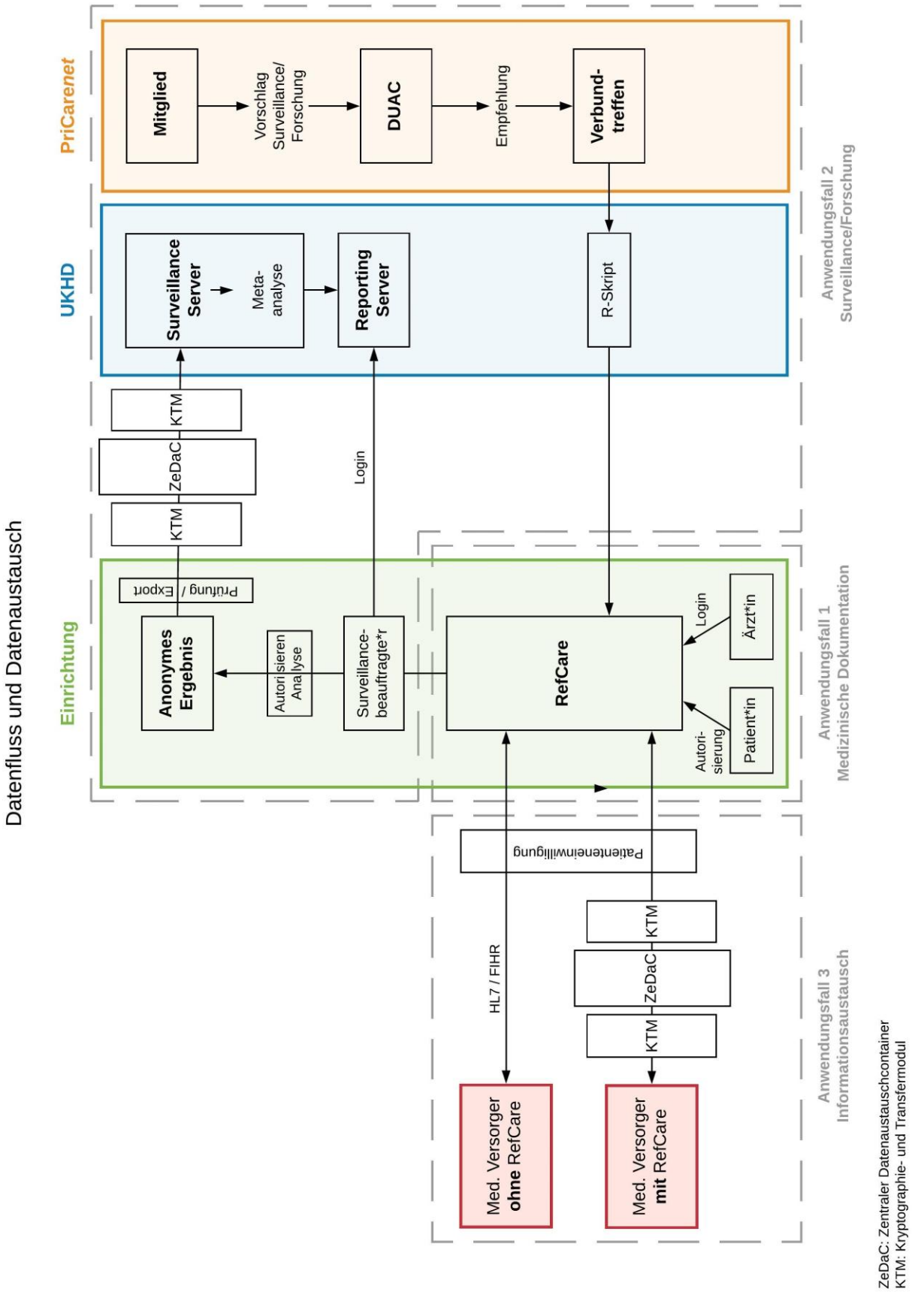

Abbildung 2: Datenfluss und Datenaustausch

10.2.5 Organisatorische Sicherheitsmaßnahmen bezüglich der automatisierten Auswertung

Da nicht in jedem Fall davon ausgegangen werden kann, dass die Leistungserbringer das R-Skript prüfen können, werden folgende organisatorischen Sicherheitsmaßnahmen implementiert:

a. Zur Vorbeugung, dass aufgrund des automatischen Verfahrens personenbezogene Daten die leistungserbringende Einrichtung verlassen könnten, wird der Export der anonymen Kennzahlen von den Server der datenschutzrechtlich verantwortlichen Stelle auf den zentralen Surveillance-Server nur aktiv durch einen autorisierten, behandelnden Arzt ermöglicht (Push-Verfahren). Vor dem Export werden die Inhalte (anonyme Kennzahlen) dem Arzt zur Prüfung bzw. Sichtung angezeigt.
b. Daraufhin muss der Export durch aktives Betätigen eines Export-Buttons durch den autorisierten Arzt ausgelöst werden.

10.2.6 Zentrale Speicherung anonymer Kennzahlen

Eine zentrale Datenhaltung der anonymen Kennzahlen der Einrichtungen erfolgt auf dem Surveillance-Server. Datenhalter ist das Universitätsklinikum Heidelberg. Die Kennzahlen werden in einer Datenbank gespeichert. Die zentral gespeicherten Kennzahlen enthalten keinen Personenbezug und sind somit anonym. Das Re-Identifizierungsrisiko anhand der Kennzahlen ist somit nahezu ausgeschlossen. Dennoch gelten strenge personelle und technische Organisationsmaßnahmen für den Surveillance-Server:

- Datensparsamkeit: Ausschließlich die für die Indikatoren der Surveillance notwendigen Kennzahlen werden exportiert. Es findet keine Vorratsdatenhaltung statt.
- Formulierung eines Zugriffskonzepts auf den Surveillance-Server: Der Kreis der Personen mit Zugriff auf den Surveillance Server wird so eng als möglich gehalten (ein Biometriker, ein IT-Verantwortlicher, ein Wissenschaftler). Die Personen mit Zugriff müssen der Schweigepflicht unterliegen (ggfs. über Arbeitsverträge abgedeckt) oder verpflichten sich schriftlich zur Verschwiegenheit.

10.2.7 Datennutzung der zentral gespeicherten Daten für ein Reporting (Surveillance)

Die zentral von unterschiedlichen Leistungserbringern und Standorten zusammengeführten, anonymen Kennzahlen werden (1.) mittels metaanalytischen Analyseverfahren über Einrichtungen hinweg zu Surveillance-Zwecken ausgewertet sowie (2.) einer Berichterstellung unterzogen.

Die anonymen Ergebnisse der Metaanalysen werden auf zwei Aggregationsebenen berichtet:

1. Report über alle Einrichtungen hinweg (Ergebnisse der Metanalyse; vgl. 10.2.7.1)

2. Feedbackbericht an einzelne Leistungserbringer: Reporting der Einrichtungsdaten im Vergleich zu den meta-analytisch generierten Ergebnissen über alle Einrichtungen hinweg (Benchmark; vgl. 10.2.7.2)

Im Zuge des Projektverlaufs werden weitere Formen der Berichterstattung (z.B. Public Reporting) erörtert und geprüft.

10.2.7.1 Report über alle Einrichtungen hinweg

Zum Zwecke einer Berichterstattung über alle Einrichtungen hinweg werden von dem Biometriker, der lt. Zugriffskonzept autorisierten Zugriff auf den Surveillance Server hat, meta-analytische Analysen der anonymen Kennzahlen durchgeführt und anhand von Forest-Plots für den Berichtszweck an einen Wissenschaftler der Abt. Allgemeinmedizin und Versorgungsforschung des Universitätsklinikum Heidelberg ausgehändigt. Die Form und der Inhalt der einrichtungsübergreifenden Berichterstattung wird im Forschungsverbund PriCare*net* abgestimmt (vgl. 10.2.1).

10.2.7.2 Feedbackbericht an einzelne Leistungserbringer

Jeder Leistungserbringer erhält einen einrichtungsspezifischen Feedbackbericht, in dem die eigenen Ergebnisse mit den gemittelten bzw. risiko-, alters- und/oder geschlechtsstandardisierten Ergebnissen aller Leistungserbringer(anonym) vergleichend dargestellt werden. Die einzelnen Einrichtungen können somit Ihre Ergebnisse mit den aggregierten Ergebnissen aller Einrichtungen vergleichen. Der Datenhalter bereitet dafür einrichtungsspezifische Feedbackberichte auf. Die Berichte werden auf einer Web-Plattform (Reporting Plattform) zum Abruf durch die einzelnen Leistungserbringer bereitgestellt. Der Abruf des Feedbackberichts (Dokumentenformat) erfolgt aktiv und passwortgeschützt die Reporting Plattform- Der Abruf auf Einrichtungsebene ist durch unbefugten Zugriff im Rahmen der Rollen- und Benutzerverwaltung geschützt

10.2.8 Anlassbezogene Forschung im Forschungsverbund PriCare*net*

Zu Forschungswecken können seitens der teilnehmenden Standorte dezidierte Fragestellungen im Forschungsverbundeingebracht werden. Dazu wird ein Antrag zur Forschung an das DUAC gerichtet. Dem Antrag werden laut Konsortialvertrag folgende Unterlagen beigefügt:

- Studienprotokoll
    - Darstellung der Relevanz der Fragestellung
    - Reflexion ethischer Aspekte
    - Nennung erforderlicher Daten
    - Analyseplan, inkl. adäquate Darstellung der wissenschaftlichen Methoden
- Positives Votum einer Ethikkommission
- Angaben zur Verwertung und Veröffentlichung der Ergebnisse

Das DUAC prüft die Fragestellungen und das Vorhaben anhand vorab definierter Kriterien auf Machbarkeit, Relevanz, ethische Aspekte, Re-Identifizierungsrisiko und Vollständigkeit der

o.g. Unterlagen und spricht eine Empfehlung für oder gegen die Analyse aus. Unter Berücksichtigung dieser Empfehlung erfolgt eine Abstimmung über die Durchführung des jeweiligen Vorhabens auf dem Verbundtrefen. Im Falle einer positiven Bewertung erstellt das UniversitätsKlinikum Heidelberg ein R- Auswertungsskript und stellt dieses den Einrichtungen zur Verfügung. Die teilnehmenden Standorte des Netzwerks können sich eigenständig für oder gegen eine Teilnahme an der Forschungsfragestellung mit „ihren“ lokalen Daten entscheiden. Das Empfehlungs- und Teilnahmeverfahren erfolgt auf elektronischem Weg über die RefCare-Software.

Im Falle einer Teilnahme erfolgt analog der Import des zentral seitens der Universitätsklinik Heidelberg erstellten R-Skripts, die dezentrale automatisierte Analyse der lokalen Behandlungsdaten, die Erstellung eines oder mehrerer anonymer Kennzahlen sowie der Export derselben zu meta-analytischen Zwecken an die Universitätsklinik Heidelberg.

10.2.9 Löschung / Anonymisierung

Die anonymen Kennzahlen werden sowohl im Falle der Statistik (Surveillance) als auch Im Falle der Forschung im Verbund der teilnehmenden Standorte ohne Personenbezug auf den zentralen Surveillance-Server exportiert und dort gespeichert. Eine Löschung ist nicht erforderlich. Nach Auslaufen der Bundesförderung geht die Rechtsnachfolge in die Zuständiggkeit des Forschungsverbunds PriCare*net* und der darin festgelegten Verbundleitung über.

10.3 Informationsaustausch

Asylsuchende verlassen spätestens nach sechs Monaten Aufenthalt eine Erstaufnahmeeinrichtung der Länder. Bis zur kommunalen Anschlussunterbringung in Wohnungen der Kommunen erfolgt meist eine weitere Unterbringung in großen Gemeinschaftsunterkünften. Regional wird die Unterbringung sehr unterschiedlich gehandhabt. In einzelnen Fällen des Wechsels der Unterkunft zwischen Erstaufnahmeeinrichtungen- oder großen Gemeinschaftseinrichtungen erfolgt auch ein Wechsel der Leistungserbringer. Zum Zweck der medizinischen Weiterbehandlung können zwischen den an der Versorgung beteiligten Ärzten unterschiedlicher Leistungserbringer Behandlungsdaten auf informationstechnologischem Wege ausgetauscht werden.

10.3.1 Prozesse in der Versorgungssituation

10.3.1.1 Technische Voraussetzungen

Zum Zwecke des Informationsaustausches der Behandlungsdaten zwischen unterschiedlichen Leistungserbringern ist die jeweilige Nutzung der RefCare-Software sowie Kommunikationsschnittstellen (KTM = Kryptographie- und Transfermodul; HL-7, FIHR) Teil der Software notwendig.

10.3.1.2 Kommunikation mit medizinischen Leistungserbringern die **RefCare© nutzen**

Gibt ein einzelner Patient in einer versorgenden Einrichtung an, dass er bereits in einer anderen Versorgungseinrichtung von einem anderen Leistungserbringer medizinisch vorbehandelt wurde und dieser Leistungserbringer die RefCare© Software nutzt, können die Behandlungsdaten vom einen zum anderen Leistungserbringer über RefCare© transferiert werden. Der aktuell versorgende Leistungserbringer informiert den Patienten über diese Möglichkeit des Datenaustausches. Bei Zustimmung des Patienten zum Datenaustausch wird eine schriftliche Einverständniserklärung des Patienten eingeholt. Die Einwilligungserklärung kann anschließend eingescannt und mit einer Anfrage zum Datenaustausch über RefCare© an den vorversorgenden Leistungserbringer gesendet werden. Alternativ kann die Übermittlung der Einwilligungserklärung mittels Telefax erfolgen.

Nach Autorisierung des Patienten und bei Vorliegen der unterschriebenen Einverständniserklärung beim vorversorgenden Leistungserbringer wird die Anfrage zum Datenaustausch durch den vorversorgenden Leistungserbringer beantwortet und ein Datenexport mit Ziel des aktuell versorgenden Leistungserbringers angestoßen. Es wird davon ausgegangen, dass dieser Fall eher selten eintritt und der Nutzen für die Weiterbehandlung den Aufwand des Einholens einer schriftlichen Einwilligungserklärung überwiegt.

In Fällen, in denen die versorgende Einrichtung über die Verlegung eines Patienten in eine nachfolgende Unterkunft unterrichtet ist, kann die Einwilligungserklärung zur Datenweitergabe an die nachversorgenden Einrichtung schriftlich eingeholt und in RefCare© zusammen mit den Patientendaten vorausschauend an den nachversorgenden Leistungserbringer gesendet werden.

10.3.2 Kommunikationsprozesse

Der Datenexport einer Datenbank mit den medizinischen Behandlungsdaten erfolgt verschlüsselt („Ende-zu-Ende-Verschlüsselung“) über eine sichere Internetverbindung. Der Datenaustausch zwischen den beiden Leistungserbringern erfolgt äquivalent wie in Kapitel 10.2.4 beschrieben über das KTM-ZeDAC-Verfahren, allerdings ist hier das sogenannte "Ziel" der Kommunikation jeweils der andere Leistungserbringer. Die medizinischen Behandlungsdaten werden nach Autorisierung durch den Patienten einmalig übermittelt.

10.3.3 Zentrale Datenhaltung

Es erfolgt im Falle des Informationsaustausches zwischen versorgenden Leistungserbringer keine zentrale Datenhaltung.

10.3.4 Datennutzung und Auswertung

Die medizinischen Behandlungsdaten der Vorbehandlung werden nach Autorisierung durch den Patienten ausschließlich zur medizinischen Weiterbehandlung genutzt.

11 Risiko- und Schutzbedarfsanalyse

Die verarbeiteten Daten in diesem Verfahren zur medizinischen Versorgung von Asylsuchenden und geflüchteten Menschen sowie von Daten zur Sicherstellung der medizinischen Versorgung gehören laut DS-GVO Art. 9 Abs. 1 als Gesundheitsdaten zu einer besonderen Kategorie personenbezogener Daten, deren Verarbeitung grundsätzlich einem Erlaubnisvorbehalt unterliegt. Die umfangreiche Verarbeitung solcher Daten erfordert gemäß DS-GVO die Umsetzung einer Datenschutz-Folgenabschätzung (DSFA, DS-GVO Art. 35 Abs.3 lit b). Für eine angemessene Festlegung von technischen und organisatorischen Sicherheitsmaßnahmen ist zunächst der Schutzbedarf der Datensätze einzuschätzen. Auf der Grundlage dessen, dass zum einen die Behandlungsdaten der ärztlichen Schweigepflicht unterliegen und zum anderen extern verarbeitet und gespeichert werden (z.B. mit Personenbezug bei der Weiterbehandlung von Patienten, ohne Personenbezug für Forschung und Statistik (Anwendungsfall 2), besteht grundsätzlich ein hoher Schutzbedarf. Diese Einschätzung kann auch anhand des Standard-Datenschutzmodells (SDM, Version 2.0a) und im Schutzstufenkonzept der LfD Niedersachsen (Schutzstufe D) nachvollzogen werden. Demzufolge besteht in Bezug auf die Versorgungsdaten das Risiko, dass von der Datenverarbeitung betroffene Personen durch eine unsachgemäße Verarbeitung ggf. in ihren gesellschaftlichen und wirtschaftlichen Konstellationen erheblich beeinträchtigt werden könnten.

Infolgedessen werden alle datenverarbeitenden Prozesse einer Risikobewertung unterzogen. In diesem Zusammenhang wird eine Einteilung der Risiken nach Eintrittswahrscheinlichkeit und Schweregrad mithilfe der Einteilungsbegrifflichkeiten des Kurzpapiers Nr. 18 der Datenschutzkonferenz (DSK) vorgenommen. Dieser Vorgang zur Risikoeinschätzung wird einmal ohne Berücksichtigung risikobezogener technischer und organisatorischer Maßnahmen und einmal mit einer entsprechenden Berücksichtigung vorgenommen, so dass eine Wirksamkeitsprüfung der Maßnahmen möglich wird.

Folgende in Tabellenform dargestellte Auflistungen der Risiken pro Prozessschritt des Anwendungsfalls 1 (Tab. 3), des Anwendungsfalls 2 (Tab. 4) und des Anwenungsfalls 3 (Tab. 5) beruhen auf einer Analyse der in Kapitel 10 beschriebenen und in Abbildung 2 dargestellten datenbezogenen Prozessen und der in Kapitel 12 aufgeführten technischen und organisatorischen Maßnahmen.

Tab. 3: Auflistung der Risiken pro Prozessschritt für den Anwendungsfall 1. Die Einteilungen der Eintrittswahrscheinlichkeit (geringfügig, überschaubar, substanziell, groß) und des Schweregrads (geringfügig, überschaubar, substanziell, groß) wurden dem Kurzpapier Nr. 18 der (DSK) entnommen. Die Risikokategorien (normal, hoch, sehr hoch) entsprechen den Empfehlungen im SDM (Version 2.0a)

Prozessschritt	**Gefährdung**	**Bewertung**	
1. Ärztliche Primärdokumentation in der elektronischen Patientenakte (RefCare) in der Versorgungseinrichtung	**Unautorisierte Einsicht in Patientenakte RefCare**	Betroffene Schutzziele	Vertraulichkeit Integrität
		Risikoquelle/Angreifer	interne menschliche Quellen externe menschliche Quellen
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	überschaubar
		Schweregrad	substanziell
		Risikokategorie	hoch
		Maßnahmen: Ein Zugriff auf medizinische Behandlungsdaten ist nur möglich über ein Endgerät (Eingabegerät) in der leistungserbringenden Einrichtung, das gesichert mit dem lokalen RefCare-Server über LAN oder WLAN (WPA2) verbunden ist. Die Behandlungsdaten liegen in kryptographisch verschlüsselter Form auf dem lokalen RefCare-Server vor. Jedes Endgerät (Tablet, Laptop, PC) der Leistungserbringer greift per Browser auf die RefCare-Software zu (Vgl. Kap. 12.1.3.1). Als Schutz vor unerlaubtem Zugriff greift hier sowohl die Benutzerverwaltung des Betriebssystems, als auch die Benutzerverwaltung mit Zugangsdaten und rollenbasierten Rechten der RefCare-Software. Mit diesen Komponeten ist es möglich, dass nur der autorisierte medizinische Leistungserbringer Zugriff auf das browserbasierte RefCare und den Patientendaten hat. Die zugrundeliegenden TOMs sind in Kap. 12.1.2.1 beschrieben. Zudem wird der Zugang zu allen Räumen, in denen personenbezogenen Daten verarbeitet werden, durch entsprechende mechanische und elektronische Sicherheitsvorkehrungen geregelt(Vgl. Kap. 12.1.1.1).	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal
2. Einsicht des Patienten in seine Daten während der Behandlung	**Einsicht unbefugter Personen in die Behandlungsdaten**	Betroffene Schutzziele	Integrität Vertraulichkeit
		Risikoquelle/Angreifer	interne menschliche Quellen

		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	überschaubar
		Schweregrad	überschaubar
		Risikokategorie	hoch
		Maßnahmen: Für die Beantwortung von Fragebögen kann der Patient über ein Patienteninterface Daten mittels Umfragetool eingeben. Das Tool befindet sich in einem separaten Verzeichnis und erlaubt nicht den Zugriff auf Patientendaten. Dafür wird dem Patienten ein Tablet ausgehändigt, das im Intranet mit dem lokalen RefCare-Server kommunizieren kann. Die Tablets werden durch den behandelnden Arzt über RefCare für den jeweiligen Patienten und ausgewählten Fragebogen individuell freigeschaltet. Daraufhin wird in RefCare ein Code generiert, den der Arzt im vorgesehenen Tablet eingeben muss um dort den Eingabemodus zu öffnen. Das Tablet wird erst nach dieser Autorisierung an den Patienten ausgehändigt. Für weitere Fragebögen oder weitere Patienten muss der Arzt das Gerät neu autorisieren. Des Weiteren (Vgl. Kap. 10.1.1 und 12.1.5).	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal
3. Eingabe der medizinischen Versorgungsdaten mittels RefCare	**Eingabefehler in Patientenakte**	Betroffene Schutzziele	Integrität
		Risikoquelle/Angreifer	interne menschliche Quellen
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	substanziell
		Schweregrad	substanziell
		Risikokategorie	hoch
		Maßnahmen: Vor dem Speichern werden die vom medizinichen Leistungserbringer eingegebenen Daten von RefCare auf ihre Plausibilität hin überprüft (Vgl. Kap. 10.1.1).	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal

4. Regelmäßige Backups der RefCare-Datensätze	**Verlust oder unautorisierter Modifikation der Patientendaten**	Betroffene Schutzziele	Verfügbarkeit Integrität
		Risikoquelle/Angreifer	externe menschliche Quellen technische Quellen
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	überschaubar
		Schweregrad	groß
		Risikokategorie	hoch
		Maßnahmen: Es wird empfohlen regelmäßig - täglich und wöchentlich - automatisiert verschlüsselte Backups der RefCare-Daten auf einem NAS-Server der Einrichtung durchzuführen. (Vgl. Kap. 12.1.4)	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal
5. Speicherfrist der RefCare-Datensätze	**unautorisierte Einsichtnahme und Modifikation der Patientendaten**	Betroffene Schutzziele	Verfügbarkeit Integrität Vertraulichkeit
		Risikoquelle/Angreifer	externe menschliche Quellen technische Quellen
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	überschaubar
		Schweregrad	substanziell
		Risikokategorie	hoch
		Maßnahmen: Die personenbezogenen Daten der Primärdokumentation werden für mind.10 Jahre gespeichert und anschließend gelöscht. Des Weiteren wird in diesem Zeitraum jegliche Veränderung des RefCare-Datensatzes elektronisch dokumentiert. (Vgl. Kap. 10.1.4)	
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal

Tab. 4: Auflistung der Risiken pro Prozessschritt für den Anwenungsfall 2. Die Einteilungen der Eintrittswahrscheinlichkeit (geringfügig, überschaubar, substanziell, groß) und des Schweregrads (geringfügig, überschaubar, substanziell, groß) wurden dem Kurzpapier Nr. 18 der (DSK) entnommen. Die Risikokategorien (normal, hoch, sehr hoch) entsprechen den Empfehlungen im SDM (Version 2.0a)

Verortung	**Prozessschritt**	**Gefährdung**	**Bewertung**	
Leistungserbringende Einrichtung	1. Auslösen eines lokalen Exports zum Zweck der automatisierten lokalen Analyse der Patientendaten	**Unautorisierter Export von Patientendaten**	Betroffene Schutzziele	Vertraulichkeit Integrität
			Risikoquelle/Angreifer	interne menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substanziell
			Risikokategorie	hoch
			Maßnahmen: Der automatisierte Export der RefCare-Daten kann nur vom für die Software autorisierten medizinischen Leistungserbringer der jeweiligen Einrichtung ausgelöst werden (Vgl. Kap. 10.2.3 und 10.2.4; Abbildung 1).	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
	2. Zwischenspeicherung der exportierten Daten mit reduziertem Personenbezug im csv-Format	**Fehler in den exportierten Datensätzen**	Betroffene Schutzziele	Integrität
			Risikoquelle/Angreifer	technische Quellen interne menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substanziell
			Risikokategorie	hoch

			Maßnahmen: Im Laufe der lokalen automatisierten Analyse der RefCare-Daten werden dafür notwendige Zwischenergebnisse als csv-Dateien auf dem lokalen Server der leistungserbringenden Einrichtung temporär gespeichert und nach Erstellung der anonymen Kennzahl wiederum automatisiert gelöscht. Auf diese Weise kann die Qualität der exportierten Daten vom entsprechenden medizinischen Leistungserbringer kontrolliert werden. Dabei erfolgen z.B. Fallzahlprüfung und die Kontrolle auf Vollständigkeit der Daten (Vgl. Kap. 10.2.2 und Abbildung 1).	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
	3. Vollständige Anonymisierung und Kontrolle der lokalen anonymen Kennzahlen vor dem Export zum Surveillance-Server	**Export personenbeziehbarer medizinischer Daten zum Surveillance-Server**	Betroffene Schutzziele	Integrität Vertraulichkeit
			Risikoquelle/Angreifer	interne menschliche Quellen technische Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substanziell
			Risikokategorie	hoch
			Maßnahmen: Als Resultat der lokalen automatisierten Analyse werden anonyme Kennzahlen erhalten, die zunächst auf dem lokalen Server gespeichert. Der medizinische Leistungserbringer der jeweiligen Einrichtung sichtet die anonymen Kennzahlen, um zu kontrollieren, dass nicht aufgrund des automatischen Anaylseverfahrens personenbezogene Daten die leistungserbringende Einrichtung verlassen. Anschließend muss er den Export zum Surveillance-Server in der Software aktiv selbst auslösen. (Vgl. Abbildung 1 und Kap. 10.2.5)	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig

			Schweregrad	geringfügig
			Risikokategorie	normal
	4. Export der lokalen anonymen Kennzahlen zum Surveillance-Server	**unautorisierter Zugriff auf exportierte medizinische Daten**	Betroffene Schutzziele	Integrität Vertraulichkeit
			Risikoquelle/Angreifer	externe menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	substanziell
			Schweregrad	substanziell
			Risikokategorie	hoch
			Maßnahmen: Anschließend erfolgt der Export der kryptographisch verschlüsselten anonymen Kennzahlen aller Standorte auf dem Surveillance-Server des Universitätsklinikums Heidelberg mittels KTM(Krytopgraphie- und Transport-Modul)-ZeDAC(Zentraler Datenaustausch-Container)-Verfahrens zum Zwecke der zentralen Zusammenführung.(Vgl. Kap. 10.2.4 und Kap. 12.2.1)	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
Universitätsklinikum Heidelberg	5. Zentrale Datenzusammenführung der anonymen Kennzahlen und Metaanalyse auf dem Surveillance-Server	**unautorisierte Modifikation der Daten und Re-Identifikation von Patienten**	Betroffene Schutzziele	Vertraulichkeit Integrität
			Risikoquelle/Angreifer	externe menschliche Quellen nicht-menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	groß
			Risikokategorie	hoch

			Maßnahmen: Nur autorisiertes und technisch versiertes Personal (Rollenkonzept) des Universitätsklinikums Heidelberg, das einen Vertraulichkeritsvereinbarung zugestimmt hat, erhält Zugriff auf den Surveillance-Server (Vgl. Kap. 10.2.6 und Kap. 12.3.1).	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
	6. Feedbackbericht der Metaanalyse einzelne Leistungserbringer	**unautorisierte Einsichtnahme in Reporting-Daten**	Betroffene Schutzziele	Vertraulichkeit
			Risikoquelle/Angreifer	externe menschliche Quellen nicht-menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substantiell
			Risikokategorie	hoch
			Maßnahmen: Über ein Web-Portal wird den einzelnen medizinischen Leistungserbringern die Möglichkeit eingeräumt, Feedback-Reports abzufragen. Der Abruf dieser Berichte erfolgt passwortgeschützt. Der unbefugten Zugriff wird auf Einrichtungsebene im Rahmen der Rollen- und Benutzerverwaltung geschützt (Vgl. Kap. 12.1.2).	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
	7. Regelmäßige Backups des Surveillance-Servers	**Verlust oder unautorisierter Modifikation der gespeicherten Datensätze**	Betroffene Schutzziele	Verfügbarkeit Integrität
			Risikoquelle/Angreifer	externe menschliche Quellen technische Quellen

			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substantiell
			Risikokategorie	hoch
			Maßnahmen: Die Backups werden mindestens täglich, auf Datenspeicher innerhalb des Rechenzentrums der Universitätsklinik Heidelberg durchgeführt. Des Weiteren werden im Rechenzentrum des Universitätsklinikums Heidelberg Maßnahmen getroffen, um die Einsatzfähigkeit des Servers zu gewährleisten. Das betrifft u.a. die kontinuierliche Stromversorgung, den Harwareaustausch und die Installtuion einer Firewall (Vgl. Kap. 12.2.3.3 und 12.2.3.4).	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal
Forschungsverbund	8. Beantwortung von Forschungsfragen im Forschungsverbund PriCare*net*	**unautorisierte Einsichtnahme in die Datensätze des Surveillance-Servers**	Betroffene Schutzziele	Vertraulichkeit
			Risikoquelle/Angreifer	externe menschliche Quellen interne menschliche Quellen
			Bewertung vor Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	überschaubar
			Schweregrad	substantiell
			Risikokategorie	hoch

			Maßnahmen: Im Forschungsverbund können Fragestellungen eingebracht werden, die mithilfe der Surveillance-Datensätze beantwortet werden könnten. Eine Zustimmung dazu erfolgt erst nach Prüfung des entsprechenden Projektantrags auf u.a. datenschutzrechtliche Aspekte durch das Data-Use&Access-Committee (DUAC) und der Abstimmung im Verbundtreffen. Bei einem positivem Votum wird das infrage-kommende Projekt vom Verbund koordiniert. Des Weiteren steht es den einzelnen Standorten (Leistungserbringer) des Netzwerks frei, ob sie ihre Daten dem Projekt zur Verfügung stellen. (Vgl. Kap. 10.2.8)	
			Bewertung nach Eindämmung durch Maßnahme	
			Eintrittswahrscheinlichkeit	geringfügig
			Schweregrad	geringfügig
			Risikokategorie	normal

Tab. 5: Auflistung der Risiken pro Prozessschritt für den Anwenungsfall 3. Die Einteilungen der Eintrittswahrscheinlichkeit (geringfügig, überschaubar, substanziell, groß) und des Schweregrads (geringfügig, überschaubar, substanziell, groß) wurden dem Kurzpapier Nr. 18 der (DSK) entnommen. Die Risikokategorien (normal, hoch, sehr hoch) entsprechen den Empfehlungen im SDM (Version 2.0a)

Prozessschritt	**Gefährdung**	**Bewertung**	
1. Einrichtungs-übergreifende Weitergabe der Behandlungsdaten zum Zweck der Weiterbehandlung	**Widerrechtliche Weitergabe von und Einsicht unbefugter Personen in Behandlungsdaten**	Betroffene Schutzziele	Vertraulichkeit Integrität
		Risikoquelle/Angreifer	externe menschliche Quellen technische Quelle
		Bewertung vor Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	überschaubar
		Schweregrad	substanziell
		Risikokategorie	hoch
		Maßnahmen	Für den Zweck der inviduellen Weiterbehandlung könnten Behandlungsdaten zwischen Einrichtungen elektronisch übermittelt werden. Dieser Vorgang kann nur durch eine schriftliche Einwilligungserklärung des Patienten erfolgen. Auf der Grundlage dessen werden autorisiert durch den jeweiligen medizinischen Leistungserbringer die kryptographisch verschlüsselten Behandlungsdaten über das KTM(Krytopgraphie- und Transport-Modul)-ZeDAC(Zentraler Datenaustausch-Container)-Verfahren zur weiterbehandelnden Einrichtung transferiert(Vgl. Kap. 10.3.1 und 10.3.2)
		Bewertung nach Eindämmung durch Maßnahme	
		Eintrittswahrscheinlichkeit	geringfügig
		Schweregrad	geringfügig
		Risikokategorie	normal

12 Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen werden im Folgenden ausgehend von der Primärdatenerhebung zu Dokumentationszwecken, dem Datenfluss zum Surveillance-Server und dem Ziel des anschließenden Reporting beschrieben (Prozessperspektive).

12.1 Maßnahmen in den versorgenden Einrichtungen

Im Folgenden werden die Maßnahmen zum Betrieb und zur Nutzung der Software zur ärztlichen Primärdokumentation (RefCare) beschrieben. Die Leistungserbringer oder zuständigen Behörden sind datenverarbeitende und verantwortliche Stelle im Sinne des Datenschutzes. Die beschriebenen Maßnahmen werden den einzelnen datenschutzrechtlich verantwortlichen Stellen für einen sicheren IT-Betrieb und zur Wahrung des Datenschutzes empfohlen. Die Abteilung Allgemeinmedizin und Versorgungsforschung des Universitätsklinikums Heidelberg unterstützt als Konsortialführer des Projektes die Leistungserbringer bei der Umsetzung eines sicheren Betriebs der RefCare-Software. Verantwortlich für die Umsetzung und Wahrung der rechtlichen Bestimmungen sind allerdings die datenschutzrechtlich verantwortlichen Stellen selbst. Den Stellen wird empfohlen, die Umsetzung unter Beteiligung der IT-Verantwortlichen und zuständigen Datenschutzbeauftragten umzusetzen. Dadurch bedingte verbindliche Normen werden durch Rahmenverträge oder eine Betriebsvereinbarung geregelt.

12.1.1 Empfehlungen zu Zugriff-, Zutritt-, Zugang-, Weitergabe-, Eingabe-, Verfügbarkeitskontrolle

Im Folgenden werden Empfehlungen an technische, personelle und organisatorische Schutzmaßnahmen für die Leistungserbringer formuliert. Die erfolgte Information und die Kenntnisnahme dieser Empfehlungen werden durch die datenschutzrechtlich verantwortliche Stelle gegenüber dem Universitätsklinikum Heidelberg schriftlich bestätigt.

12.1.1.1 Zutrittskontrolle

Sichere Schließzylinder

Alle Räume, in welchen personenbezogene Daten verarbeitet werden, müssen mit Schließzylindern ausgestattet werden, deren Schlüssel man im Einzelhandel nicht duplizieren kann. Darüber hinaus sollten die Zylinder über einen Schutz vor aufbohren und abbrechen verfügen. Von entscheidender Bedeutung ist das Schließblech im Türrahmen. In vielen Fällen handelt es sich nur um ein normales Metall mit einer Stärke von 1 mm. Schon mit einem großen Schraubendreher lässt sich die Tür aufhebeln, indem das Schließblech zerstört wird. Abhilfe verschafft ein stabiles Schließblech.

Selbstschließende Bürotüren mit Knauf auf der Außenseite

Optimalerweise haben unbefugte Personen keinen physikalischen Zugriff auf die PCs der Mitarbeiter. Gerade im alltäglichen Bürobetrieb kann es immer wieder mal vorkommen, dass ein

PC unbeaufsichtigt bleibt. Möglicherweise ist der passwortgeschützte Bildschirmschoner noch nicht angesprungen oder vielleicht liegt das frisch erstellte Backup noch auf dem Schreibtisch. Auch der Karteikasten mit diversen personenbezogenen Daten wird nicht immer verschlossen. In diesen Fällen ist eine selbstschließende Bürotür eine einfache und effektive Maßnahme zum Schutz der Daten. Für geringe Kosten und einen kurzen Montageaufwand ist das Büro geschlossen. Eine fremde Person kann nicht ersehen, ob der Mitarbeiter am Arbeitsplatz sitzt. Soll die Bürotür im Alltag meistens offen stehen kann ein kleiner Keil die Tür offen halten. Verlässt der Mitarbeiter das Büro kurzfristig, so braucht er nur den Keil beim Hinausgehen entfernen um das Büro sicher zu verschließen.

Einen Schritt weiter geht die Installation eines Knaufes auf der Außenseite der Bürotür. Somit kann das Büro nur noch mit einem Schlüssel betreten werden.

Alarmanlage

Eine Alarmanlage signalisiert einen Einbruch mittels optischer und akustischer Signale. Sofern keine Schaltung zur Polizei oder einem Wachdienst vorgenommen wird, bleiben diese Signale oft unbeachtet. Nach Aussagen der Polizei wirkt eine Alarmanlage aber sehr oft abschreckend auf Gelegenheitseinbrecher. Auch bei der Anschaffung einer Alarmanlage sollte auf das „VdS"-Siegel geachtet werden.

Abschließbare Fenstergriffe

Alle Fenster, die nicht mindestens 3 Meter über dem Erdboden liegen, müssen mit abschließbaren Fenstergriffen versehen werden.

12.1.1.2 Zugriffskontrolle

Mitarbeiter melden Daten, die sie nicht sehen dürften

Die Mitarbeiter sollten schriftlich darauf verpflichtet werden, dass sie es dem Vorgesetzten unmittelbar melden, wenn sie (personenbezogene) Daten sehen, zu denen sie keine Berechtigung haben. Der Vorgesetzte kann darauf reagieren und möglicherweise ganz grundsätzliche Sicherheitsmängel beheben helfen.

Windows-Benutzerkonten möglichst restriktiv nutzen

Unter Windows können verschiedene Benutzer eingerichtet werden. Eine Sonderrolle hat der Benutzer „Administrator" (bzw. andere Benutzer, die den Rang eines Administrators zugewiesen bekommen haben). Der Administrator hat weitestgehende Rechte auf dem Computer; er kann beispielsweise Benutzer einrichten und Berechtigungen ändern. Daher sollten die alltäglichen Aufgaben von einem Benutzer mit „eingeschränkten Rechten" erledigt werden. Leider lässt sich auch bei eingeschränkten Rechten die Installation von (schädlicher) Software nicht verbieten, daher kann auch dieser Benutzer schädliche Programme installieren (Viren, Trojaner, Würmer, Rootkits). Die Auswirkung der schädlichen Programme ist bei einem Benutzer mit eingeschränkten Rechten aber sehr, sehr viel geringer. Als Beispiel dafür dient die hosts-Datei unter Windows; sie liegt im System-Verzeichnis und entscheidet darüber, wohin ein Internet-Browser surft, wenn eine www-Adresse eingegeben wird. Sollte diese Datei durch ein

Schadprogramm geändert werden, so surft der Browser zu einem anderen Ziel als manuell eingetippt wurde. Die Auswirkungen können verheerend sein. So nutzen viele Phishing-Webseiten diesen Mechanismus. Im Einzelfall muss ein normaler Benutzer auch Administrationsaufgaben wahrnehmen (Software installieren, Uhrzeit verändern, …); dies lässt sich unter Windows ohne größere Probleme realisieren, auch ohne dass sich der eingeschränkte Benutzer umständlich als Administrator anmelden muss. Für eine komfortable Rechteverwaltung existieren zahlreiche Spezialprogramme; als Beispiel dient die teilweise kostenlose Software „Privilege Manager“ (www.beyondtrust.com). Unnötige Benutzerkonten (die vielleicht einmal irrtümlich eingerichtet wurden) sollten gelöscht oder zumindest deaktiviert werden. Letzteres gilt auch für das „Gast“-Konto.

12.1.1.3 Zugangskontrolle

12.1.1.3.1 Richtlinien zur Erstellung von Passwörtern für die Rechner mit RefCare-Zugang in den Einrichtungen

Folgende Regelungen zum Passwortschutz und Passwortgebrauch, die sich an den Vorgaben des BSI zur Passwortvergabe orientieren, werden für die Handhabung mit den Rechnern empfohlen, mithilfe derer RefCare verwaltet wird[19].

1. Es sind individuelle Passwörter zu verwenden, die eine der folgenden Vergabeeigenschaften aufweisen sollten:
    - 20 bis 25 Zeichen lang → Nutzung zweier Zeichenarten (beispielsweise eine Folge von Wörtern). Es ist dann lang und weniger komplex.
    - 8 bis 12 Zeichen lang ist → Nutzung von vier Zeichenarten. Es ist dann kürzer und komplex.
    - 8 Zeichen lang → Nutzung von drei Zeichenarten und zusätzlicher Absicherung durch Mehr-Faktor-Authentisierung abgesichert ist (beispielsweise durch einen Fingerabdruck, eine Bestätigung per App oder eine PIN). Dies ist generell empfehlenswert.
2. Das Passwort darf keine personenidentifizierenden Merkmale (z.B. Namen, Vornamen) enthalten
3. Das Passwort muss geheim gehalten und nicht schriftlich unverschlüsselt festgehalten sowie öffentlich zugänglich abgelegt werden.
4. Das Passwort muss regelmäßig jedes Jahr geändert werden. Dabei ist zu beachten, dass es wichtiger ist, komplexe Passwörter zu führen, als diese oft zu ändern. Durch

[19] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

die Führung einer Passworthistorie, welche mindestens 6 Passwörter umfasst, wird verhindert, dass der Benutzer immer wieder das gleiche Passwort vergibt.

Für den Fall, dass das Passwort einer unbefugten Person zugänglich gemacht wurde, muss dieses Passwort umgehend geändert werden. Dies gilt auch bei Verdacht auf Passwortkenntnis unautorisierter Personen.

Passwörter unterwegs

Einige Passwort-Speicher-Programme können sich mit einem Pocket-PC abgleichen. Sowohl auf dem Computer, als auch auf dem Pocket-PC sind diese Daten verschlüsselt abgelegt. Dies ist sehr praktisch, da man auch im mobilen Einsatz alle Passwörter bei sich hat. Darüber hinaus ist der Pocket-PC auch noch eine „Sicherheitskopie" der Daten.

Speichern von Passwörtern mithilfe von Passwort-Managern

Passwörter sollten niemals unverschlüsselt auf dem Rechner abgelegt werden oder auf Notizzetteln am Arbeitsplatz hinterlegt werden. Wer sich Passwörter notieren will, sollte sie stattdessen gut unter Verschluss halten bzw. auf dem Rechner in einer verschlüsselten Datei ablegen. Das BSI empfiehlt hierzu die Verwendung von Passwortmanager-Software wie Keepass[20] für die sichere Speicherung von Passwörtern in Windows-Systemen. Darüber hinaus können derartige Programme auch starke Passwörter generieren.

Ausspionieren der Passwörter

Im Internet befinden sich zahlreiche Webseiten, die von sich behaupten, dass sie Passwörter ausspionieren können. Dabei werden die verschiedensten Mechanismen genutzt. Ob die angebotenen Programme wirklich das leisten, was sie versprechen, ist unklar. Ganz sicher ist jedoch, dass es sich um Schadsoftware handeln kann, die jeden denkbaren Schaden anrichten kann (zumal man unter Windows als Administrator angemeldet sein muss). Im Falle eines Angreifers, der auf einem fremden Computer spioniert, ist der anschließende Schaden im Betriebssystem allerdings kein wichtiges Gegenargument; er kann sogar gewollt sein.

Die Gefährdung der Passwörter lässt sich in verschiedene Kategorien einordnen:

- Bestehende Passwörter werden ausgelesen
    - Gespeicherte Passwörter werden entschlüsselt und angezeigt. Dies gilt für Windows, für geschützte Dateien, für Webseiten, für E-Mail-Passwörter, MS-Office-Dateien, für Remotedesktop und für VPN-Verbindungen.
    - Durch Sternchen verborgene Passwörter werden im Klartext angezeigt.
- Aktuell zu übertragende Passwörter werden ausgelesen

[20] https://keepass.info/download.html

- Mittels Keylogger (als Hard- oder Software) wird aufgenommen, was der Anwender aktuell eintippt.
- Der Datenverkehr der Netzwerkkarte wird abgehört.

Als Konsequenz lässt sich unmittelbar schließen, dass Passwörter auf keinen Fall gespeichert werden dürfen. Stattdessen muss der Benutzer die Mühe auf sich nehmen, die Passwörter jedes Mal manuell einzutippen.

Das Ausspionieren von Passwörtern (auch der Besitz der notwendigen Software) ist gemäß den „Hacker-Paragraphen“ (§202c StGB) durch das Strafgesetzbuch strafbar.

12.1.1.4 Weitergabe der Kennzahlen

Die Weitergabe der lokal generierten anonymen Kennzahlen erfolgt ausschließlich über den Softwareexport in verschlüsselter Form, wie unter Kapitel 10.2.4 beschrieben. Eine Weitergabe von Datenträgern ist nicht vorgesehen.

12.1.1.5 Eingabekontrolle

Jeder Mitarbeiter muss sich vor der Eingabe, Veränderung oder Löschung von Daten an die Software authentifizieren. Nach diesen Arbeiten ist ein Abmelden erforderlich.

12.1.1.6 Verfügbarkeitskontrolle

1) Mitarbeiter sollten sich schriftlich dazu verpflichten, dass sie keine Software am Computer installieren, ohne dies mit dem EDV-Verantwortlichen abzusprechen.
2) Die EDV-Verantwortlichen werden dazu verpflichtet, sicherheitskritische Updates für Betriebssystem und Anwendungsprogramme zeitnah zu installieren,

12.1.2 Benutzer/Zugriffskonzept

12.1.2.1 Rollenbasierte Zugriffskontrolle

Um den oben dargestellten Problemen entgegenzuwirken, kann die sogenannte rollenbasierte Zugriffskontrolle (engl. role-based access control, RBAC) eingesetzt werden. Statt jedem einzelnen Mitarbeiter einer Berufsgruppe Rechte auf Daten zuzuweisen, werden diese an eine bestimmte Rolle (engl. role) geknüpft, die dann dem Angestellten zugewiesen wird. Verändert sich seine Aufgabe innerhalb der Firma, so wird ihm lediglich eine neue Rolle zugewiesen, die über die erforderlichen Berechtigungen (engl. permissions) verfügt (siehe Abbildung 1). Der Aufwand für die Rechteverwaltung wird dadurch erheblich reduziert.

Berechtigungsmatrix

Es können unterschiedliche Berechtigungsstufen vergeben werden:

Stufe	Berechtigung
Keine	Benutzer dürfen Objekte weder erstellen, noch lesen oder ändern
Lesen	Benutzer können Objekte nur lesen
Erstellen	Benutzer können Dokumente verfassen
Ändern	Benutzer können Dokumente verfassen und/oder bearbeiten sowie löschen
Vollzugriff	Vollzugriff
Export	Benutzer kann den Export der anonymen Kennzahlen zum Surveillance Server auslösen
Assessment	Benutzer kann Assessmentbögen ausfüllen und exportieren (z.B. Strukturerhebungsbogen)

Einrichtungsspezifische Rollenmodelle mit unterschiedlichen Zugriffsrechten müssen durch die einzelnen Leistungserbringer entsprechend der lokalen Strukturen und Rollen auf Basis dieser Berechtigungsmatrix erstellt werden.

12.1.3 Absicherung der Kommunikationsprozesse seitens der datenschutzrechtlich verantwortlichen Stelle

12.1.3.1 Sicherheit Netzwerk LAN/WLAN

Die WLAN-Technik bietet verschiedene Möglichkeiten um Daten verschlüsselt zu übertragen: WEP, WPA und WPA2. Insbesondere die WEP-Technologie bietet jedoch praktisch keinerlei Schutz und sollte für die Übertragung sensibler Daten nicht eingesetzt werden, dies ist schon seit 2001 bekannt.

WPA benutzt einen 48 BIT großen Initialisierungsvektor (WEP 24 Bit) und dynamische Schlüssel für jedes versendete Paket, die Erzeugung dieser Schlüssel ist Aufgabe von TKIP. Zusätzlich zum Integrity Check Value (ICV) nach dem 802.11-IEEE-Standard wurde noch der sogenannte Message Integrity Check (MIC, auch Michael genannt) eingeführt, wodurch die Sicherheit der Datenintegrität erhöht wurde. Bei WPA2 steht das on der IEEE entwickelte Sicherheitsprotokoll CCMP (Counter CBC-MAC Protocol, RFC 3610) setzt auf AES auf und ermöglicht einen kombinierten Betriebsmodus, in dem der AES-Schlüssel sowohl für die Vertraulichkeit als auch zur Bildung einer kryptographisch sicheren ICV eingesetzt wird. Für die Authentifizierung stehen in WPA zwei verschiedene Modi zur Verfügung: WPA Personal (WPA-PSK, PSK = preshared key) und WPA Enterprise (WPA RADIUS). WPA-PSK ist identisch zur Preshared-Key-Authentisierung entsprechend dem Standard IEEE 802.11i und ist für den Heimbetrieb ausgelegt, daher wird diese Methode auch als SOHO- oder Home-Mode bezeichnet. Bei WPA-PSK wird der Preshared Key sowohl auf dem Access Point als auch auf den Clients eingetragen und der Access Point übernimmt de Authentisierung und das Key-Management ohne zusätzliche Komponenten.

12.1.4 Datensicherung

Datensicherung sollte durch die datenschutzrechtliche Stelle regelmäßig (täglich, automatisch) stattfinden. Zu empfehlen ist ein NAS Server, der automatisiert Daten im Zuwachsbackup sichert. Eine Vollsicherung ist 1x pro Woche zusätzlich zu empfehlen. Der NAS sollte im RAID Modus betrieben werden, um einem Verlust der Daten bei Ausfall einer Sicherungsfestplatte vorzubeugen. Eine einfache externe Festplatte ist weder in Hinsicht der Datensicherheit bei Ausfall noch hinsichtlich eines Datendiebstahls, Entfernens der Festplatte, empfehlenswert. Idealerweise können die Hot Swap fähigen Festplatten des NAS in regelmäßigen Abständen getauscht und sicher gelagert werden, sodass bei Brand, o.ä. zerstörenden Ereignissen eine Sicherungskopie erhalten bleibt.

12.1.5 Endgerät

Jedes Endgerät (Tablet, Laptop, PC) der Leistungserbringer greift per Browser auf die RefCare-Software zu. Als Schutz vor unerlaubtem Zugriff greift hier sowohl die Benutzerverwaltung des Betriebssystems, als auch die Benutzerverwaltung mit Zugangsdaten und rollenbasierten Rechten der Ref-Care-Software. Eine unerlaubte Nutzung ist somit vorgebeugt.

Einfügen: Patienteninterface

Ein Diebstahl eines Endgerätes hätte wegen der Datenspeicherung auf dem Server der Leistungserbringer keinen Datenverlust und somit Datenmissbrauch zur Folge.

12.1.6 Endgerät zu Server der datenschutzrechtlich verantwortlichen Stelle

Die Kommunikation zwischen Endgerät und Server des Leistungserbringers erfolgt, je nach technischer IT-Infrastruktur vor Ort, entweder über das lokale LAN-Netzwerk oder über ein WLAN mit dem aktuellen Verschlüsselungsstandard WPA2. Alternativ über eine sichere LTE-Datenverbindung.

12.1.7 Server der datenschutzrechtlich verantwortlichen Stelle

Als Schutz vor unerlaubtem Zugriff greift hier die Benutzerverwaltung des Betriebssystems. Desweiteren greifen die in Kapitel 12.1.1 empfohlenen Maßnahmen um den Server des Leistungserbringers effektiv zu schützen. Die Daten werden in der Datenbank des Leistungserbringers verschlüsselt abgelegt.

12.2 Prozess Server des Leistungserbringers zu Surveillance Server

In den folgenden Kapiteln werden Maßnahmen des Datenschutzes bezüglich des Prozesses des Datenflusses vom dezentralen, lokalen Server der Leistungserbringer zum zentralen Surveillance Server beschrieben

12.2.1 Server des Leistungserbringers zu ZeDAC und ZeDAC zu Surveillance-Server

Die Kommunikation vom Server des Leistungserbringers zum ZeDAC und "umgekehrt" wird mittels TLS-gesicherte Verbindung geschützt und zusätzlich durch das nachfolgende KTM-ZeDAC-Verfahren (Hybride Verschlüsselung mit RSA 4096 Bit und AES 256 Bit) gesichert.

12.2.1.1 Datenablage/Speichern

Zur Autorisierung des Senders (Server des Leistungserbringers) wird eine digitale Signierung durchgeführt (ähnlich der Prozedur einer Verschlüsselung). Dadurch wird verhindert, dass nicht-registrierte Teilnehmer Daten verschicken können. Bei einer digitalen Signierung wird normalerweise eine Nachricht signiert. Da hier keine Nachricht vorliegt, wird an dieser Stelle ein längerer Zufallsstring erzeugt und dem Sender durch das ZeDAC "aufgezwungen".

- KTM: die Daten der RefCare-Software werden durch das KTM komprimiert. Es wird beim ZeDAC der öffentliche Schlüssel des Ziels erfragt. Mit diesem öffentlichen Schlüssel werden die Daten verschlüsselt.
- ZeDAC: Diese Transportdatei wird nun auf dem ZeDAC in einen Quarantäne-Ordner gelegt. Das ZeDAC erzeugt einen zufälligen Autorisierungsstring und übermittelt diesen an das KTM des Senders.
- KTM: Erhält den Autorisierungsstring und verschlüsselt diesen mit dem privaten Schlüssel des Senders. Nun schickt das KTM den unverschlüsselten und verschlüsselten Autorisierungsstring ans ZeDAC. Der Transfer erfolgt auch unverschlüsselt, um die Kommunikation an dieser Stelle zuordnen zu können.
- ZeDAC: Der ZeDAC verschlüsselt mit dem Public-Key des Senders den Autorisierungsstring und autorisiert somit den Sender und verschiebt ggf. die Transportdatei vom Quarantäne-Ordner in den Container-Ordner.

12.2.1.2 Datenabholung / Anfrage

- KTM: Der Surveillance-Server schickt eine Anfrage an den ZeDAC, ob Daten vorhanden sind.
- ZeDAC: Signalisiert das Vorhandensein von Daten und schickt eine Liste ans KTM.
- KTM: Sendet Abholungsanfrage verschlüsselt mit dem privaten Schlüssel des Abholers.
- ZeDAC: Der ZeDAC verschlüsselt mit dem Public-Key des Abholers die Abholungsanfrage und autorisiert somit den Sender. Die Transportdatei wird dem KTM des Surveillance-Servers übermittelt.
- KTM: Das KTM entschlüsselt mit dem Private-Key die Transportdatei. Die Daten werden dekomprimiert und auf dem Surveillance-Server gespeichert.

12.2.2 Personelle Maßnahmen

Datenexport kann nur durch einen autorisierten Benutzer seitens des Leistungserbringers erfolgen.

12.2.3 Maßnahmen zur Sicherheit des zentralen Surveillance Server

Die anonymen Kennzahlen werden in der Datenbank des zentralen Surveillance-Servers verschlüsselt abgelegt. Darüber hinaus werden weitere technische und organisatorische Schutzmaßnahmen getroffen:

12.2.3.1 Zutrittskontrolle

Alle Server stehen in mit elektronischen Schlüsseln gesicherten Rechenzentren des Universitätsklinikums Heidelberg, zu denen nur auf den Datenschutz verpflichtete und autorisierte Mitarbeiter Zugang haben.

12.2.3.2 Zugangskontrolle

Alle Systembenutzer (Vgl. Kap. 12.3.1) müssen einen personalisierten Zugang zum Netzwerk des Universitätsklinikums Heidelberg besitzen. Zusätzlich erhalten sie einen personalisierten Zugang (Benutzeraccount), mit dem sie sich am Surveillance Server authentifizieren müssen.

12.2.3.3 Ausfallschutz

Im Folgenden werden Maßnahmen dargestellt, die die Wahrscheinlichkeit der Verfügbarkeit des Systems erhöhen und mögliche Ausfallzeiten minimieren. Dabei werden in der Spalte „Ursachen“ mögliche Ursachen für eine Nicht-Verfügbarkeit des Systems aufgeführt.

Tab. 6: Maßnahmen zum Ausfallschutz

Ursachen	Maßnahmen
Ausfall von Einzelkomponenten (Hardware)	Betrieb des Servers mit mindestens 2 Festplatten im RAID Modus
Ausfall von Server-Systemen (Hardware)	Bei Ausfall des gesamten Surveillance Servers -> Austausch der Hardware innerhalb von wenigen Tagen
Ausfall von Stromversorgung (Infrastruktur)	Die kontinuierliche Stromversorgung wird vom Rechenzentrum des Universitätsklinikums Heidelberg sichergestellt.
Angriff auf Server	Einsatz restriktiv konfigurierter Firewalls Umfassendes Monitoring von Authentifizierung- und ungewöhnlichen Datenanfragen

Zusätzlich zu den vorhergehend beschriebenen Maßnahmen wird sowohl bei ungeplanten Verfügbarkeitseinschränkungen als auch bei geplanten (z.B. Update mit Systemneustart) mit einer Nicht-Erreichbarkeit von mehr als 6 Stunden ein Ausfall-Bewertungsprozess gestartet. In einer grundlegenden Dokumentation werden dabei die Dauer der Verfügbarkeitseinschränkung, der Grund der Verfügbarkeitseinschränkung und die Einflüsse der

Verfügbarkeitseinschränkung auf die Nutzbarkeit des Systems festgehalten. Im Anschluss werden technische und organisatorische Maßnahmen erarbeitet, um die Verfügbarkeitseinschränkung in Zukunft zu verhindern oder früher zu erkennen und ggf. automatisiert zu beheben.

12.2.3.4 Datensicherung

Die Daten des Surveillance Servers werden regelmäßig, mindestens täglich, auf Datenspeicher innerhalb des Rechenzentrums der Universitätsklinik Heidelberg als Sicherungskopie gesichert.

12.3 Maßnahmen Surveillance Server und Reporting

Zu Zwecken der Berichterstattung der Ergebnisse werden durch wissenschaftliche Mitarbeiter der Abteilung Allgemeinmedizin und Versorgungsforschung des Universitätsklinikums Heidelberg (Wissenschaftler) Reports erstellt. Auf Grundlage der auf dem Surveillance Server zur Verfügung stehenden anonymen Kennzahlen werden von einem Mitarbeiter des IMBI (Statistiker) anhand von definierten Indikatorbeschreibungen Meta-analytische Analysen und Abbildungen (Forest-Plots) erstellt, die dem Wissenschaftler zur Berichterstattung zur Verfügung gestellt werden. Die Reporte dienen dem Zweck des Feedbacks an die einzelnen Leistungserbringer. Darüber hinaus wird während des Projektzeitraums die Relevanz und Machbarkeit einer öffentlichen Berichterstattung geprüft.

12.3.1 Funktionsbasiertes Zugriffskonzept Surveillance Server

Im Folgenden wird das Berechtigungskonzept für den Surveillance Server angeführt:

Berechtigungsstufen

Stufe	Berechtigung
Keine	Benutzer dürfen Objekte weder erstellen, noch lesen oder ändern
Lesen	Benutzer können zentrale Daten einsehen
Ändern	Benutzer können zentral zusammengeführte Rohdaten ändern
Erstellen	Benutzer können k-anonymisierte Reports verfassen
Löschen	Benutzer können Daten löschen, sofern unzulässiger Weise personenbezogene Daten gespeichert wurden oder bspw. ältere Sicherheitskopien nicht weiter notwendig sind.
Vollzugriff	Vollzugriff
Export	Benutzer kann den Datenexport zum Reporting-Server auslösen

Berechtigungsmatrix

Funktion	Keine	Lesen	Ändern	Erstellen	Löschen	Export	Vollzugriff
Wissenschaftler[1]		x	x	x		x	
Biometriker[2]		x	x	x		x	
IT-Datenmanager[3]		x	x		x	x	
Datenschutzbeauftragter[4]					x		

Wissenschaftler[1] (Abt. Allgemeinmedizin und Versorgungsforschung, Universitätsklinikum Heidelberg)

Biometriker[2] (Abt. Biometrie, Institut für Medizinische Biometrie und Informatik, Universitätsklinikum Heidelberg)

IT-Datenmanagerr[3] (Abt. Allgemeinmedizin und Versorgungsforschung, Universitätsklinikum Heidelberg)

Datenschutzbeauftragter[4] (Universitätsklinikum Heidelberg)

13 Fristen und Ausblick

Das Datenschutzkonzept der Version 1 galt für die beschriebenen, mit Blick auf die Machbarkeit eingeschränkten Versorgungssettings.

Die Förderung des Projektvorhabens endet unter Berücksichtigung einer bereits bewilligten, kostenneutralen Verlängerung am 31.12.2020.

Das Datenschutzkonzept der Version 2 dient der nachhaltigen Nutzung in den bereits beteiligten Standorten sowie für neue Standorte in diesen oder weiteren Bundesländern. Die Zuständigkeiten der Nutzung der anonymisierten Daten sind über den Forschungsverbund PriCare*net* geregelt (vgl. Kapitel 10.2.8).

Die langfristige Weiternutzung der Dokumentationssoftware RefCare© sowie der dafür notwendige technische Support und ggfs. erforderliche Dienstleistungen (z.B. Wartung und Aktualisierung der Software) sind über einen Lizenzvertrag geregelt Im Rahmen des Lizenzvertrags sind ebenso Verantwortlichkeiten zur Haltung und Speicherung der mediznischen Primärdaten festgelegt.

Das Datenschutzkonzept behält seine Gültigkeit sofern keine relevanten Änderungen der rechtlichen Grundlagen erfolgen. Sollte dieser Fall eintreten, wird das Datenschutzkonzept entsprechend aktualisiert.

14 Abkürzungsverzeichnis

AES Advanced Encryption Standard: symmetrisches Verschlüsselungsverfahren

AIS Arztinformationssystem

ATC Anatomisch-Therapeutisch-Chemische Klassifikation: Klassifikation von Arzneimittelwirkstoffen entsprechend dem Organ oder Organsystem, auf das sie einwirken, und nach ihren chemischen, pharmakologischen und therapeutischen Eigenschaften

BDSG Bundesdatenschutzgesetz

BGB Bürgerliches Gesetzbuch

DSGVO Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)

EG Europäische Gemeinschaft

ICD International Statistical Classification of Diseases and Related Health Problems

ICD-10 International Statistical Classification of Diseases and Related Health Problems,

ID Identifikationsnummer

IEEE International non-profit organization and professional association for the advancement of technology, ursprgl.: Institute of Electrical and Electronics Engineers (www.ieee.org)

ISO International Organization for Standardization (www.iso.org)

k-Anonymisierung Verfahren zur Anonymisierung einer Datensammlung, so dass jede Merkmalskombination, die potentiell für einen reidentifizierenden Abgleich genutzt werden könnte, in mindestens k Datensätzen vorkommt

KBV Kassenärztliche Bundesvereinigung (www.kbv.de)

KV Kassenärztliche Vereinigung

LAN Local Area Network

LANR Lebenslange Arztnummer: Von der KBV vergebene, eindeutige neunstellige Nummer, die im Rahmen der vertragsärztlichen Versorgung lebenslang eindeutig einen Arzt und seine Fachgruppenzugehörigkeit identifiziert

LDSG Landesdatenschutzgesetz

LKHG Landeskrankenhausgesetz

MBO Musterberufsordnung für Ärzte

MS Multiple Sklerose

NAS Network Attached Storage

ÖGD Öffentlicher Gesundheitsdienst

PZN Pharmazentralnummer

RAID Redundant Array of Inexpensive / Independent Disks: Einheit aus Controller und mehreren Festplatten für erhöhte Geschwindigkeit und/oder Sicherheit

RBAC Role Based Access Control

RFC Request for Comments: Technische Dokumente zur Standardisierung im Internet (www.ietf.org/rfc)

RKI Robert Koch-Institut (www.rki.de)

RSA Asymmetrischer Verschlüsselungsalgorithmus nach Ronald L. (R)ivest, Adi (S)hamir und Leonard (A)dleman

SGB Sozialgesetzbuch

StGB Strafgesetzbuch

TLS Transport Layer Security

TMF TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (www.tmf-ev.de)

VPN Virtual Private Network

WHO World Health Organization (www.who.org)

WLAN Wireless LAN