

# CovidCare – Überwachung und Betreuung von Patienten mit COVID-19 in der Hausarztpraxis

Datenschutzkonzept

## Dokumentation

Status: in progress

### Verantwortliche

#### Initiierung

Joachim Szecsenyi

#### Erstellung

Markus Qreini

Version 0.12(H)

23.12.2021

# Inhaltsverzeichnis

Dokumenteninformation .....	1
Einleitung .....	5
<b>1. Ziele</b> .....	5
<b>2. Teilnehmende medizinische Leistungserbringer</b> .....	6
<b>3. Anwendungsfälle und Zweckbestimmung</b> .....	6
3.1. Fall 1: Ärztliche Primärdokumentation (Softwaremodul CovidCare) .....	7
3.2. Fall 2: Statistik (Surveillance) und Forschung .....	8
3.2.1. Primäre Ergebnisse .....	8
3.2.2. Sekundäre Ergebnisse .....	9
3.3. Fall 3: begleitende Prozessevaluation .....	9
3.3.1. Ergebnisse der Prozessevaluation .....	9
3.4. Datenquellen .....	9
<b>4. Verantwortlichkeiten</b> .....	10
4.1. Verantwortlichkeiten im Anwendungsfall „Ärztliche Primärdokumentation“ .....	10
4.2. Verantwortlichkeiten im Anwendungsfall „Statistik (Surveillance) und Forschung“ .....	10
4.3. Verantwortlichkeiten im Anwendungsfall und „Prozessevaluation“ .....	11
<b>5. Rechtsgrundlagen</b> .....	11
5.1. Primärnutzung von medizinischen Daten .....	11
5.1.1. Datenerhebung und Dokumentation auf Arztrechner zu Monitoringzwecken (Anwendungsfall 1) .....	11
<b>6. Daten und Datenkategorien</b> .....	12
6.1. Lokale Behandlungsdaten der Leistungserbringer (Datenquelle) .....	12
6.2. Daten Ärztliche Primärdokumentation (Software CovidCare) .....	13
6.2.1. Identitätsdaten und medizinische Basisdaten Patienten .....	13
6.2.2. Medizinische Gesundheits- und Versorgungsdaten Patienten .....	15
6.3. Lokal gespeicherte Daten zur Surveillance (Indikatoren) .....	19
6.4. Auflistung der Exportvariablen .....	19
<b>7. Beschreibung der datenbezogenen Prozesse</b> .....	20
7.1. Ärztliche Primärdokumentation (Software CovidCare) .....	20
7.1.1. Prozesse in der Versorgungssituation .....	20
7.1.2. Kommunikationsprozesse und dezentrale Datenhaltung durch die Leistungserbringer 21	
7.1.3. Datennutzung und Auswertung .....	21
7.1.4. Löschung/Anonymisierung .....	22

7.2.	Statistik (Surveillance) und Forschung.....	22
7.2.1.	Automatisierte Analyse lokaler Daten durch die einzelnen Leistungserbringer.....	22
7.2.2.	Schritte des automatisierten Auswertungsprozesses .....	22
7.2.3.	Grundlage der automatisierten Auswertung: Programmierung eines Skriptes und Transfer auf den lokalen Server der Leistungserbringer.....	23
7.2.4.	Zentrales Zusammenführen der anonymen Kennzahlen (KTM-ZeDAC-Verfahren) .....	23
7.2.5.	Organisatorische Sicherheitsmaßnahmen bezüglich der automatisierten Auswertung:	24
7.2.6.	Zentrale Speicherung anonymer Kennzahlen .....	24
7.2.7.	Datennutzung der zentral gespeicherten Daten für ein Reporting (Surveillance) .....	25
7.2.8.	Löschung / Anonymisierung.....	25
<b>8.</b>	<b>Schutzbedarfsanalyse</b> .....	<b>25</b>
8.1.	Ärztliche Primärdokumentation (CovidCare) .....	25
8.1.1.	Unerlaubter Zugriff auf medizinische Daten in der versorgenden Einrichtung.....	26
8.1.2.	Unerlaubtes Kopieren .....	26
8.1.3.	Unerlaubtes Löschen .....	26
8.1.4.	Unerlaubtes Einstellen von Daten.....	26
8.1.5.	Surveillance .....	26
8.1.6.	Unerlaubter Zugriff auf den Surveillance-Server.....	26
8.1.7.	Gefahr der Re-Identifikation von Patienten .....	27
<b>9.</b>	<b>Technische und organisatorische Maßnahmen</b> .....	<b>27</b>
9.1.	Maßnahmen in den versorgenden Einrichtungen.....	27
9.1.1.	Empfehlungen zu Zugriff-, Zutritt-, Zugang-, Weitergabe-, Eingabe-, Verfügbarkeitskontrolle .....	27
9.1.2.	Benutzer/Zugriffskonzept.....	30
9.1.3.	Absicherung der Kommunikationsprozesse seitens der Leistungserbringer .....	31
9.1.4.	Datensicherung .....	31
9.1.5.	Endgerät.....	31
9.1.6.	Endgerät zu Server des Leistungserbringers .....	32
9.1.7.	Server des Leistungserbringers.....	32
9.2.	Prozess Leistungserbringer zu Surveillance Server .....	32
9.2.1.	Server des Leistungserbringers zu ZeDAC und ZeDAC zu Surveillance-Server.....	32
9.2.2.	Personelle Maßnahmen .....	33
9.2.3.	Maßnahmen zur Sicherheit des zentralen Surveillance Server .....	33
9.3.	Maßnahmen Surveillance Server und Reporting .....	34

9.3.1. Funktionsbasiertes Zugriffskonzept Surveillance Server .....	34
<b>10. Fristen und Ausblick.....</b>	<b>34</b>
<b>11. Abkürzungsverzeichnis.....</b>	<b>35</b>
<b>12. Exportvariablen der Schnittstelle.....</b>	<b>36</b>
Modul "CovidCare" (Projekt).....	36
Modul "CovidCare" (Studie) .....	39
Modul "UlcusCrurisCare" .....	52

## Einleitung

**Hintergrund:** Seit Ende Dezember 2019 breitet sich das neue Coronavirus SARS-CoV-2 über den Globus aus und verursacht die Lungenkrankheit COVID-19. SARS-CoV-2 verursacht Krankheitssymptome in den Atemwegen und kann in einem dynamischen Verlauf innerhalb weniger Tage milde, schwere und auch lebensgefährliche Krankheitsverläufe verursachen. Patienten mit schweren Verläufen werden in Kliniken behandelt. Hausärzte sind jedoch die erste Anlaufstelle im Gesundheitswesen für die Mehrheit der Patienten. Es ist noch wenig bekannt über den Einfluss von Risikofaktoren auf den Verlauf der Krankheit. Aus diesem Grund wird ein Surveillance und Care Modul in den Hausarztpraxen eingesetzt, mit dem und durch das die ambulante Versorgung der Hochrisikopatienten unterstützt wird.

**Ziele:** Das Ziel des CovidCare-Moduls ist, die Hausarztpraxen bei der Überwachung und Betreuung von COVID-19-Patienten zu unterstützen. Das Ziel der CovidCare-Studie ist die Entwicklung, Implementierung und Evaluation eines softwaregestützten COVID-19 Surveillance- und Behandlungs-Instruments in Hausarztpraxen. Die Evaluation hat das Ziel Erkenntnisse über die Effekte von Risikofaktoren auf den Verlauf der Krankheit zu erlangen. Eine begleitende Prozessanalyse zielt darauf ab die Implementierung der Software und deren Attraktivität unter Mitarbeitern der Hausarztpraxen sowie die Betreuung über das CovidCare-Modul aus Sicht der Patienten zu verstehen.

**Methoden:** Ein softwaregestütztes COVID-19 Surveillance- und Behandlungs-Instrument wird in Hausarztpraxen eingeführt. Es beinhaltet ein initiales Assessment von Risikofaktoren und Symptomen, sowie ein fortlaufendes Telefon-Monitoring zu Krankheitszeichen und Symptomen.

Die Zielgruppe sind bestätigte COVID-19 Patienten, die einer Risikogruppe angehören und mindestens 18 Jahre alt sind,.

Dies ist eine multizentrische, prospektive, nicht-kontrollierte, longitudinale Beobachtungsstudie, die die Effekte unterschiedlicher Risikofaktoren auf den Krankheitsverlauf von COVID-19 Patienten erforscht, mit einer begleiteten Prozessevaluation.

Die Prozessevaluation besteht aus qualitativen Interviews und quantitativen Befragungen der Praxisteams und Studienpatienten.

**Analyse:** Die Evaluation basiert auf Daten, die über das CovidCare Software Modul erhoben wurden. Der Hauptfokus der Analyse liegt auf der Präsentation von validen deskriptiven Ergebnissen. Darüber hinaus werden gemischte Regressionsmodelle benutzt, um die hierarchische Struktur zu berücksichtigen, da es pro Patienten mehrere Aufnahmen/Einweisungen geben und eine Praxis auch viele Patienten hat. Die Regressionsmodelle konzentrieren sich auf die Erkennung von den Hauptfaktoren, die COVID-19-Verursachte Risiken beeinflussen, insbesondere Hospitalisierung und Tod.

Die Analyse in der Prozessevaluation ist deskriptiv und explorativ.

### 1. Ziele

Das CovidCare-Modul ist eine Software-gestütztes COVID-19 Surveillance- und Behandlungsinstruments für Hausarztpraxen. Die Software soll dem Team der Hausarztpraxis helfen den Verlauf der Krankheit zu dokumentieren, um dem Patienten das Eigen-Monitoring zu

erleichtern und eine Verschlechterung zeitnah zu erkennen. Das Ziel der Studie ist die Entwicklung, Implementierung und Evaluation eines softwaregestützten COVID-19 Surveillance- und Behandlungsinstruments in Hausarztpraxen. Die Evaluation hat das Ziel Erkenntnisse über die Effekte von Risikofaktoren auf den Verlauf der Krankheit zu erlangen.

Die begleitende Prozessevaluation zielt darauf ab die Implementierung der Software und deren Attraktivität unter Mitarbeitern der Hausarztpraxen und die Wahrnehmung der Versorgung aus Sicht der Patienten zu verstehen.

## **2. Teilnehmende medizinische Leistungserbringer**

Die Dokumentation der Behandlungsdaten erfolgt als „Ärztliche Primärdokumentation“ mittels der Elektronischen Patientenakte CovidCare in der Case Management Software CareCockpit browserbasiert via Endgeräte durch die Leistungserbringer in den der HZV AOK-Baden-Württemberg angeschlossenen Hausarztpraxen.

Die Datenspeicherung erfolgt in Datenbanken auf dem jeweiligen Rechner / (virtuellen) Server, der in einer sicheren Umgebung in Verantwortung des jeweiligen Leistungserbringers betrieben wird. Die Daten zwischen Client und Server werden über eine sichere Verbindung via LAN ausgetauscht. Die personenbezogenen Behandlungsdaten verbleiben durchgehend in der Hand des jeweiligen Leistungserbringers.

Die medizinische Versorgungseinrichtung bzw. der niedergelassene Arzt (im Folgenden: die medizinischen Leistungserbringer) werden als verantwortliche Stelle für die Datenverarbeitung von medizinischen Behandlungsdaten betrachtet, die zu Zwecken der Statistik (Surveillance) und Forschung mit dem Universitätsklinikum Heidelberg kooperiert.

## **3. Anwendungsfälle und Zweckbestimmung**

Ausgehend von den Zielen des Projektes wird im Modul „CovidCare“ in der elektronischen Dokumentationssoftware „CareCockpit“ die ärztliche Primärdokumentation der medizinischen Beobachtung von an COVID-19 Erkrankten ermöglicht. Weiter sollen automatisiert Sekundärdatenanalysen lokaler Behandlungsdaten erfolgen. Aus den lokalen anonymisierten Datensätzen wird eine praxisübergreifende Statistik zur Surveillance der Krankheitsverläufe von COVID-19 und des Infektions-, bzw. Ausbruchsgeschehens von SARS-CoV-2 erstellt.

Lokale Daten aus der Primärdokumentation der Leistungserbringer unterschiedlicher Hausarztpraxen werden in regelmäßigen Abständen lokal seitens der behandelnden Ärzte durch ein automatisiertes Verfahren in der Software CareCockpit ausgewertet. Die hierdurch generierten anonymen Kennzahlen werden zu statistischen Zwecken (Surveillance) zusammengeführt um in der Population Trends und Änderungen des Morbiditäts-, bzw. des Infektionsgeschehens erkennen zu können. Diese Evaluation zielt darauf ab Einsichten auf den Effekt von Risikofaktoren auf den Verlauf der Krankheit zu gewinnen.

Die begleitende Prozessevaluation möchte Einsicht gewinnen in den Prozess der Implementierung des Tools zur Surveillance und Patientendokumentation und seine Attraktivität und Akzeptanz bei den Teams der Hausarztpraxen und Patienten.

Ausgehend von diesen Vorhaben können daher drei Anwendungsfälle unterschieden werden:

### 3.1. Fall 1: Ärztliche Primärdokumentation (Softwaremodul CovidCare)

Ärztliche Dokumentation der primärmedizinischen, individuellen Behandlung durch medizinische Leistungserbringer. (Primärnutzung medizinischer Daten zum Zweck des Patientenmonitorings)

Ziel der Software ist es, den Hausärzteteams darin zu helfen den Verlauf der Infektion zu überwachen, um den Patienten bei der Eigenkontrolle zu unterstützen und zeitnah eine Verschlechterung zu erkennen. Beteiligte Leistungserbringer nutzen das Modul „CovidCare“ im CareCockpit zur Primärdokumentation des medizinischen Monitorings und können auf diesem Wege der Dokumentation ihrer Arbeit nach § 630f BGB (Dokumentation der Behandlung) nachkommen. Das Modul „CovidCare“ ermöglicht eine auf die Dauer des Monitorings ausgerichtete, zielgruppen- und settingspezifische Infektion mit SARS-CoV-2 und Heimquarantäne) Dokumentation des Infektionsverlaufs unter Berücksichtigung der dafür erforderlichen Software-Funktionalität. Nach initialem Assessment des Patienten werden in flexiblen, vom Behandler festgelegten Intervallen Telefonmonitorings durchgeführt und dokumentiert, die die Symptome und Vitalwerte des Patienten abfragen. Durch die Fokussierung auf das Wesentliche der für eine SARS-CoV-2 Dokumentation erforderlichen Datenerhebung und die settingpezifisch 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):

In den Stammdaten:

- Vorname, Name
- Geburtsdatum
- Geschlecht
- Adresse
- Kontaktmöglichkeiten wie Telefon und Erreichbarkeit
- Einverständniserklärung, Einwilligungen und Aufklärungen
- Versichertennummer
- Teststatus auf Coronavirus (getestet (ja, nein), Testergebnis (positiv, negativ, ausstehend))
- Einverständniserklärung (mündliche oder schriftlich)
- Datum der Einverständniserklärung (mündlich oder schriftlich)
- Erreichbarkeit (Abwesenheitsstatus wenn im Krankenhaus oder im Urlaub)
- Krankenversicherung oder Kostenträger
- Status als Hausbesuchspatient

Im Assessment:

- die medizinischen Befunde und Risikofaktoren wie chronische Erkrankungen (Diabetes, Herz-Kreislauf-Erkrankungen, Lungenerkrankungen, Lebererkrankungen, Nierenerkrankungen)
- Immunschwäche
- Krebserkrankung
- Weitere Erkrankungen, wenn ja welche

- Informationen über 8teil-) Stationäre Behandlungen
- Größe
- Gewicht
- BMI
- Raucher (ja, nein), wenn ja seit wann
- der Impfstatus auf Pneumokokken und/oder Influenza
- Medikamentenplan (ja, nein)
- Wohnstatus (allein lebend (ja, nein, Pflegeheim)
- Bezugsperson (ja, nein)
- Krankheitssymptome
- Weitere Beschwerden oder Symptome
- Messwerte Eigenmessung (Fieber, Blutdruck, Puls)
- Gesundheitsvollmacht oder Patientenverfügung (ja, nein)
- Terminierung für die Telefonmonitorings (Termin und Durchführende Person)
- Krankheitssymptombeginn
- Überwachungsparameter (Blutdruck Puls, Atemfrequenz, Sauerstoffsättigung, Körpertemperatur, Gesicht, Trinkmenge, Weitere (freiwillige angabe)

Im Telefonmonitoring:

- Auflistung der Risiken
- Krankheitssymptome
- Schwierigkeiten bei der Durchführung der Überwachungsparameter (siehe Assessment)
- Aussagen über die Probleme und Schwierigkeiten
- Teststatus auf Coronavirus
- Medikamentenstatus
- Probleme bei der Medikamenteneinnahme (welche, Verträglichkeit)
- Angaben zu Ängsten
- Weitere freiwillige Angeben
- der weitere Behandlungsverlauf
- Kuriert ( ja, nein)
- Einweisungstatus (Krankenhaus)

Im Abschlussmonitoring:

- Aktueller Zustand (COVID auskuriert oder verstorben)

### 3.2. Fall 2: Statistik (Surveillance) und Forschung

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

Das Ziel dieses Anwendungsfalles ist der Gewinn von Erkenntnissen über die Effekte von Risikofaktoren auf den Verlauf der Erkrankung.

#### 3.2.1. Primäre Ergebnisse

Wichtigstes Ergebnis ist die Hospitalisierung aufgrund COVID-19.



### 3.2.2. Sekundäre Ergebnisse

Die folgenden Indikatoren wurden als Sekundärergebnisse identifiziert:

1. Diagnose Pneumonie (Crb-65 Index) bei bestätigten COVID-19 Patienten.
2. Palliativbehandlung bei bestätigten COVID-19 Patienten.
3. Mortalitätsrate bei bestätigten COVID-19 Patienten.
4. Angst bei bestätigten COVID-19 Patienten, gemessen unter Verwendung von Generalized Anxiety Disorder Index (GAD-2)
5. Identifizierung von prädiktiven Risikofaktoren auf die Ergebnisse, wie Hospitalisierung, Intensivpflege und Sterblichkeit.

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 Sekundärdatennutzung datenschutzkonform zu gestalten erfolgt lokal, durch die Leistungserbringer selbst ausgelöst, eine automatisierte Anonymisierung der medizinischen Behandlungsdaten. Aus den dadurch generierten Kennzahlen ist kein Personenbezug mehr ableitbar (absolute Anonymisierung). Die anonymen Kennzahlen werden im folgenden Schritt praxisübergreifend auf einem Surveillance-Server zentral zusammengeführt, metaanalytisch ausgewertet und aus den Analyseergebnissen Statistiken erstellt.

Zur Umsetzung der automatisierten Anonymisierung wird durch das Universitätsklinikum Heidelberg ein Skript (Algorithmus) programmiert. Das Skript führt bei aktivem Initiieren durch den Hausarzt (push-Verfahren) innerhalb der eigenen IT Infrastruktur den lokalen Export der erforderlichen Behandlungsdaten aus der elektronischen Patientenakte CovidCare, die statistischen Berechnungen, die automatisierte Löschung temporär gespeicherter Daten sowie die lokale Speicherung der anonymen Kennzahlen durch.

### 3.3. Fall 3: begleitende Prozessevaluation

Die begleitende Prozessanalyse will die Implementierung der Software beobachten und deren Attraktivität und Akzeptanz unter Mitarbeitern der Hausarztpraxen und Patienten erforschen.

#### 3.3.1. Ergebnisse der Prozessevaluation

Folgende Ziele wurden als Ergebnisse der Prozessevaluation festgelegt:

1. Interventionstreue: Anzahl der Kontakte pro Patienten
2. Anzahl der Kontakte pro Patienten in der kritischen Phase, nach Definition des Robert-Koch-Institut (RKI) als Maß dafür, ob Hausärzte ihre Patienten nach Richtlinie behandeln.
3. Attraktivität und Akzeptanz von CovidCare bei Hausärzten und VERAHs sowie Patienten
4. Determinanten für die Implementierung des CovidCare Surveillance and Dokumentations-Tools aus Sicht der Hausärzte, VERAHs und Patienten

### 3.4. Datenquellen

Basis der Datenquelle für die „Surveillance“ sind die Daten, die in den Hausarztpraxen in Baden-Württemberg mit der Software CareCockpit im Modul CovidCare im Anwendungsfall „Ärztliche Primärdokumentation“ dokumentiert wurden. CareCockpit und der Vorgänger PraCMan Cockpit sind Softwarepakete für das Case Management und werden in ca. 800 Hausarztpraxen in Baden-Württemberg angewendet.

Datenquelle für die Prozessevaluation sind sowohl qualitative Telefoninterviews und Befragungen von Hausärzten und VERAHs sowie Patienten nach selbstentwickelten semi-strukturierten Interview-Richtlinien und eigens entwickelte quantitative Fragebögen als auch anonymisierte Daten aus dem CovidCare Modul des Leistungserbringers.

#### 4. Verantwortlichkeiten

Die verantwortliche Stelle im Sinne des §3 Abs. 7 BDSG gewährt die datenschutzkonforme Verarbeitung personenbezogener Daten. An die verantwortliche Stelle können sich Betroffene zur Wahrnehmung ihrer Rechte wenden und ggfs. bei einem eingetretenen Schaden der Stelle gegenüber Schadenersatzansprüche geltend machen.

Hinsichtlich der Zuständigkeiten für den Datenschutz kooperieren für die genannten Anwendungsfälle die Hausarztpraxen, das Universitätsklinikum Heidelberg und die AOK.

Die Hausarztpraxen sind als verantwortliche Stelle für die datenschutzkonforme Primärdokumentation und lokale Datenverarbeitung bis zur Erstellung der anonymen Kennzahlen verantwortlich. Die Zuständigkeit des Universitätsklinikums Heidelberg bezieht sich dabei auf die datenschutzkonforme Formulierung der Prozesse der Statistiken und Forschungsfragen und der Verarbeitung der anonymen Kennzahlen.

Im Folgenden werden die Verantwortlichkeiten im datenschutzrechtlichen Sinne nach Anwendungsfällen differenziert angeführt.

##### 4.1. Verantwortlichkeiten im Anwendungsfall „Ärztliche Primärdokumentation“

Die verantwortliche Stelle im datenschutzrechtlichen Sinne im Falle der ärztlichen Primärdokumentation mittels der CovidCare-Software sind die jeweiligen Leistungserbringer (Hausarztpraxen). Die Leistungserbringer haben die datenschutzkonforme lokale Verarbeitung der Patientendaten zu gewährleisten. Hierzu gehört der sichere Betrieb der IT-Infrastruktur sowie die Vorbeugung unberechtigten Zugreifens auf die gespeicherten Patientendaten. Dies beinhaltet explizit auch das Einhalten der gesetzlichen Speicherfristen, die Gewährung eines Auskunfts- und Einsichtsrechts, die Sicherstellung der Umsetzung eines Berechtigungskonzeptes mit Protokollierung der Zugriffe auf die Patientenakte, Maßnahmen der Revisionsicherheit sowie die Sicherstellung technischer und organisatorischer Maßnahmen. Das Universitätsklinikum Heidelberg ist dabei zuständig für die Bereitstellung und Aktualisierung der CovidCare-Software, die Einweisung in die Nutzung der Software und die Formulierung von Empfehlungen zu technischen und organisatorischen Maßnahmen zur IT-Sicherheit.

##### 4.2. Verantwortlichkeiten im Anwendungsfall „Statistik (Surveillance) und Forschung“

Die Leistungserbringer (Hausarztpraxis) sind 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. 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. Die Zuständigkeit des Universitätsklinikums Heidelberg im datenschutzrechtlichen Sinne für den Anwendungsfall Statistik (Surveillance) und Forschung bezieht sich auf die

Formulierung der Prozesse der Datenverarbeitung (Sekundärdatenanalyse), die Programmierung und Aktualisierung des Algorithmus und die Datenhaltung und Datenverarbeitung der zentral zusammengeführten, anonymen Kennzahlen.

### 4.3. Verantwortlichkeiten im Anwendungsfall und „Prozessevaluation“

Die Prozessevaluation liegt im Verantwortungsbereich des Universitätsklinikum Heidelberg. Formulare, Fragebögen und anonymisierte, aggregierte Daten aus der Surveillance (siehe Punkt 5.2) sind Forschungsdaten und werden nach den Grundsätzen der medizinischen Forschung datenschutzrechtlich behandelt.

## 5. Rechtsgrundlagen

Ausgehend von den im vorigen Kapitel beschriebenen Anwendungsfällen werden im Folgenden die Rechtsgrundlagen für die Fälle der Primärnutzung (Ärztliche Primärdokumentation mit CovidCare) und die Sekundärnutzung (Surveillance und Forschung) der Daten beschrieben.

Die Dokumentation in CovidCare und die Weitergabe von Prozessdaten geschieht auf Basis der Hausarztzentrierten Versorgung der AOK Baden-Württemberg für diejenigen Patienten, die im Rahmen der AOK versichert sind und an der HZV teilnehmen. Der Patient wird im Vorfeld des Einschlusses in CovidCare über die Datenspeicherung und Weitergabe seiner Daten für Forschungszwecke informiert und gibt sein Einverständnis schriftlich. Außerdem sind folgende Rechtsnormen anwendbar:

### 5.1. Primärnutzung von medizinischen Daten

Im Folgenden werden die Rechtsgrundlagen zur Speicherung und Weiterverarbeitung der primär erhobenen Patientendaten zu Behandlungszwecken durch niedergelassene Ärzte und des zugrunde gelegten BDSG angeführt.

#### 5.1.1. Datenerhebung und Dokumentation auf Arztrechner zu Monitoringzwecken (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 (§ 4 Abs. 1 BDSG). Die vorliegende Bewertung geht von der Annahme aus, dass die Behandlung und Dokumentation durch niedergelassene Ärzte erfolgt. Diese fallen als sog. nicht-öffentliche Stelle in den Anwendungsbereich des BDSG (§ 1 Abs. 2 Nr. 3 BDSG). Als legitimierende Vorschrift für den Einsatz eines AIS zur Erhebung und Verarbeitung von Patientendaten kommt §28 BDSG in Betracht. Sofern davon ausgegangen wird, dass die Patientendaten auf dem PC oder Tablet gespeichert und genutzt werden, stellt dies eine Datenerhebung und -speicherung für eigene geschäftliche Zwecke dar. Dabei ist zu unterscheiden, ob es sich bei den Daten um identifizierende Daten, wie Name, Anschrift oder Geburtsdatum oder um medizinische Daten des Patienten handelt. Die Erhebung von identifizierenden Daten ist gemäß § 28 Abs. 1 Nr. 1 zulässig, soweit es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Vertragsverhältnisses notwendig ist, was beispielsweise bei einem Behandlungsvertrag der Fall ist. Demgegenüber bemisst sich die Zulässigkeit der medizinischen Datenverarbeitung nach § 28 Abs. 6-8 BDSG. Ärztliche Behandlungs- und Befunddaten stellen besondere Arten personenbezogener Daten dar (§ 3 Abs. 9 BDSG). Eine Erhebung und Speicherung solcher sensibler Daten ist zulässig, wenn dies zu Zwecken der Gesundheitsvorsorge, Diagnostik oder Behandlung erforderlich ist (§ 28 Abs. 7 BDSG).

In Abgrenzung zu einer zulässigen Datenverarbeitung nach § 28 Abs. 1, Abs. 7 BDSG stellen die Regelungen der § 630f BGB, § 10 Abs. 1 MBO, § 57 Abs. 3 BMV-Ä keine datenschutzrechtliche Gestattungsnorm im Sinne von § 4 Abs. 1 BDSG dar. Diese Normen statuieren lediglich vertragliche und berufsrechtliche Verfahrens- und Dokumentationspflichten im Rahmen der ärztlichen Behandlung.

## 5.2. Nutzung von Patientendaten in anonymisierter Form zur Surveillance und Forschung (Anwendungsfall 2)

In diesem Anwendungsfall werden die im Umfeld von Hausarztpraxen entstehenden medizinischen Behandlungsdaten von COVID-19 Patienten für wissenschaftliche Forschungsfragen und statistische Auswertung (Surveillance) vor Ort anonymisiert. Die Daten aus den Monitorings sind in der speziellen CovidCare Software gespeichert (vgl. 4.1) und werden durch die automatisierte Auswertung anonymisiert. Die auf diesem Weg generierten anonymen Fallzahlen werden durch die Leistungserbringer an das Universitätsklinikum Heidelberg übermittelt. Der Patient gibt im Vorfeld des Einschlusses in CovidCare nach Aufklärung sein Einverständnis.

## 6. 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:

- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische Daten,
- biometrische Daten,
- Gesundheitsdaten,
- Sexualeben sowie sexuelle Orientierung.

In CovidCare werden aus oben genannter Liste ausschließlich Gesundheitsdaten und biometrische Daten erfasst und beachtet. Bei den personenbezogenen Daten, die im Zuge einer ärztlichen Primärversorgung zu Monitoringzwecken dokumentiert werden, handelt es sich sowohl um Identitäts- und Basisdaten des Patienten als auch um medizinische Daten, die im Zuge der Diagnostik und des Monitorings anfallen. Zum Zweck der Qualitätssicherung werden Daten sekundär genutzt, lokal anonymisiert abgelegt und diese Daten 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.

### 6.1. Lokale Behandlungsdaten der Leistungserbringer (Datenquelle)

Die Darstellung der Daten wird anhand der Anwendungsfälle differenziert.

## 6.2. Daten Ärztliche Primärdokumentation (Software CovidCare)

Im Rahmen der ärztlichen Primärdokumentation werden im Rahmen einer medizinischen Konsultation durch die Leistungserbringer alle für die medizinische Versorgung notwendigen Daten der Patient\*innen erhoben und gespeichert. Welche der Daten als Pflichtfelder dokumentiert werden, entscheiden die Ärztinnen und Ärzte in den Praxen.

### 6.2.1. Identitätsdaten und medizinische Basisdaten Patienten

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

Im Intake:

Lfd.Nr. [automatisch]

Einschlusskriterien\*

COVID-19-Patient ab 18 Jahren  
[Ja; Nein]

Datum der Testdurchführung:

Wurde ein Test durchgeführt? [Ja;  
Nein]

Datum der  
Testdurchführung: [Datum]

Ergebnis: [Positiv, Negativ,  
ausstehend]

Mind. 1 weiteres Risiko\* [Ja;  
Nein]

Alter > 50 Jahre [Ja; Nein]

Einverständniserklärung\*

Liegt MÜNDLICH vor [Ja; Nein]

Wann erhalten? [Datum]

Einverständniserklärung zur  
Studie zugesandt

Liegt SCHRIFTLICH vor [Ja; Nein]

Aktiv	Ja; Nein
Status	Erreichbar; Im Krankenhaus; Im Urlaub; Sonstiges
Status, Historie / Bemerkungen	[Freitext]

#### Basisdaten

Geschlecht*	Männlich; Weiblich; Divers
Vorname*	[Freitext]
Nachname*	[Freitext]
Geburtsdatum*	[TT.MM.JJJJ]
Versichertennummer*	[Freitext]
Patienten-ID der Praxis	[Freitext]

#### Krankenversicherung

Krankenkasse	[Freitext]
Kostenträgerkennung	[Freitext]

Ist Patient ein Hausbesuchspatient?*	[Ja; Nein ]
---	-------------

#### Anschrift

Adresszusatz	[Freitext]
Straße	[Freitext]
PLZ	[Freitext]
Ort	[Freitext]

#### Kontakt

Telefon, privat	[Freitext]
Telefon, dienstlich	[Freitext]
Telefon, mobil	[Freitext]
Erreichbarkeit	[Freitext]

#### Weiteres

Kommentar [Freitext]

Beendet Ja; Nein

Speicher-Historie [Datum; Uhrzeit; Kürzel; Behandler][Datum; Uhrzeit; Kürzel; Behandler]

Erzeugt / Geändert [Datum; Uhrzeit] / [Datum; Uhrzeit]

\*Pflichtfelder

### 6.2.2. 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.

Während des Telefon-Monitorings:

Datum des Telefonmonitorings: [Datum]

Start des Monitorings [Uhrzeit]

Beginn Monit. [Datum]

Assessment vom [Datum]

**Symptome und Messungen [automatisch aus Anamnese]:**

Husten

Dyspnoe

Hals

Körpertemperatur

Gliederschmerzen

Riech-/Geschmacksverlust

Schnupfen

Kopfschmerzen

Übelkeit/Erbrechen

Durchfall

Sonstige  
RR Systolisch  
RR Diastolisch  
Herzfrequenz/Puls  
Sauerstoff  
Atemfrequenz  
Gewicht  
Trinkmenge  
Sonstiges

### **Symptombeginn**

Krankheitsgefühl (Allgemeine Abgeschlagenheit / Müdigkeit, Schwächegefühl) [Nein; Ja]  
Wann hat dieses Krankheitsgefühl begonnen? [Datum]  
Wie stark ist dieses Krankheitsgefühl HEUTE? [Keine; Leicht; Mittel; Stark; Auswurf]  
Husten (jeder Art) [Nein; Ja]  
Wann hat der Husten begonnen? [Datum]  
Wie stark ist dieser Husten HEUTE? [Keine; Leicht; Mittel; Stark]  
Atemschwierigkeiten (Kurzatmigkeit? Oder das Gefühl schlecht Luft zu bekommen) [Nein; Ja]  
Wann haben die Atemschwierigkeiten begonnen? [Datum]  
Wie stark sind diese Atemschwierigkeiten HEUTE?  
[Keine; Leicht; Mittel; Stark]  
Fühlen Sie sich in der Lage Ihre eigenen Atemzüge über eine Minute lang zu zählen? [Ja, sicher;  
Ja, unsicher; Nein]  
Halsbeschwerden [Nein; Ja]  
Wann haben die Halsbeschwerden begonnen? [Datum]  
Wie stark sind diese Halsbeschwerden HEUTE?  
[Keine; Leicht; Mittel; Stark]

### **Körpertemperatur**

Haben Sie Ihre Körpertemperatur in den letzten Tagen gemessen? [Nein; Ja]  
Bitte nennen Sie mir Ihre max. Körpertemperatur: [° C]  
Wann war der Wert das erste Mal über 37.2°C? [Datum]  
Haben Sie HEUTE Ihre Körpertemperatur gemessen?  
Bitte nennen Sie mir Ihre max. Körpertemperatur: [° C]  
Wann gemessen? [Datum]

### **Weitere Symptome / Beschwerden zum heutigen Zeitpunkt?**

Muskel- / Gelenk- oder Gliederschmerzen [Nein; Ja]  
Riech- oder Geschmacksstörung [Nein; Ja]  
Schnupfen [Nein; Ja]  
Kopfschmerzen [Nein; Ja]  
Übelkeit / Erbrechen [Nein; Ja]  
Durchfall [Nein; Ja]  
Sonstige, und zwar: [Freitext]

### **Messwerte heute**

Haben Sie heute Ihren Blutdruck gemessen? [Nein; Ja]  
Bitte nennen Sie mir Ihre Messung in Ruhe:  
Systolisch: mmHG [Numerisch]



Diastolisch: mmHG [Numerisch]

Haben Sie heute Ihre Herzfrequenz / Ihren Puls gemessen? [Nein; Ja]

Bitte nennen Sie mir Ihre max. Messung: [Numerisch]

Sauerstoffsättigung; [Nein; Ja]

Bitte nennen Sie mir Ihre max. Messung: [Numerisch]

### **Corona-Virus (SARS-CoV-2)**

Sind Sie auf das Corona-Virus (SARS-CoV-2) getestet worden?  [Nein; Ja]

Datum der Testdurchführung: [Datum]

Ergebnis: [Positiv; Negativ; Noch ausstehend]

Sind Sie alleine lebend? [Nein; Ja; Alten- oder Pflegeheim]

Wie viele Personen (inkl. Ihnen) leben in Ihrem Haushalt? [numerisch]

Ist eine Person aus Ihrem Haushalt positiv auf das Corona-Virus (SARS-CoV-2) getestet worden?  
[Nein; Ja]

Wann getestet? [Datum]

### **Medikamente**

Nehmen Sie weitere Medikamente zu ihrem aktuellen Medikamentenplan ein?

[Nein; Ja]

Welche? [Freitext]

Gibt es generell Schwierigkeiten bei der Medikamenteneinnahme (Vergessen, Weglassen, Handhabung, Verträglichkeit)? [Nein; Ja]

Welche? [Freitext]

### **Vereinbarung Termin(e) für das Telefonmonitoring**

Nächster Termin: [Datum]

Uhrzeit [Uhrzeit]

Ende des Monitorings

Monitoring wurde durchgeführt: [Per Telefon; In der Praxis; Zu Hause]

Monitoring komplett ausgefüllt? [Nein; Ja]

Zeitpunkt Ende: [Uhrzeit]

Zeitpunkt Start: [Uhrzeit]

Dauer: [Stunden:Minuten]

Während des Telefon-Assessments:

haben Sie Diabetes (Zuckerkrankheit)? [Nein; Ja]

Haben Sie eine Herz-Kreislaufkrankung? [Nein; Ja]

wenn ja:

Hypertonie, Koronare Herzerkrankung (KHK), Herzinsuffizienz, Vorhofflimmern (jede Form), pAVK, z. n. Apoplex/Folgen eines Schlaganfalls, Sonstige, und zwar [Freitext]

Haben Sie eine Lungenerkrankung? [Nein; Ja]

Haben Sie eine chronische Lebererkrankung? [Nein; Ja]

Haben Sie eine chronische Nierenerkrankung? [Nein; Ja]

Haben Sie ein geschwächtes Immunsystem (aufgrund einer Erkrankung die mit einer Immunschwäche einhergeht) beziehungsweise nehmen Sie Medikamente ein, welche die Immunabwehr schwächen können? [Nein; Ja]

Befinden Sie sich derzeit in Behandlung wegen einer Krebserkrankung mit Immunschwäche?  
(Ausgenommen z.B. lokal begrenzter Hautkrebs wie Plattenepithelkarzinom oder Basalzellkarzinom) [Nein; Ja]

Haben Sie noch weitere chronische Erkrankungen, die sie nennen möchten? [Nein; Ja]

Waren Sie in den letzten 4 Wochen in (teil-) stationärer Behandlung? [Nein; Ja]

Alter des Patienten aus Intake

Adipositas errechnet aus Intake

BMI errechnet aus Intake

Rauchen Sie? [Nein; Ja]; Nie-Raucher; Nichtraucher seit < 6 Monaten; Nichtraucher seit  $\geq$  6 Monaten]

Sind Sie geimpft gegen...? [Pneumokokken;Influenza]

Ist Ihr Medikamentenplan aktuell? [Nein; Ja]

Teststatus aus Intake

Sind Sie alleine lebend? [Nein; Ja];Pflegeheim]

Haben Sie mind. eine Bezugsperson die täglich zu ihnen Kontakt hat? [Nein; Ja]

Krankheitsgefühl (Allgemeine Abgeschlagenheit / Müdigkeit, Schwächegefühl) [Nein; Ja; Datum; keine;leicht;

Haben Sie HEUTE Ihre Körpertemperatur gemessen?mittel;stark]

Husten (jeder Art) [Nein; Ja; Datum; keine;leicht; mittel;stark, Auswurf ja nein]

Atemschwierigkeiten (Kurzatmigkeit? Oder das Gefühl schlecht Luft zu bekommen) ) [Nein; Ja; Datum; keine;mittel;stark]

Fühlen Sie sich in der Lage Ihre eigenen Atemzüge über eine Minute lang zu zählen? [Nein; Ja unsicher; ja sicher]

Halsbeschwerden (auch leichte) [Nein; Ja; Datum; keine; leicht;mittel;stark]

Körpertemperatur gemessen[Nein; Ja]

Haben Sie Ihre Körpertemperatur in den letzten Tagen gemessen? [Nein; Ja]

Haben Sie HEUTE Ihre Körpertemperatur gemessen? ? [Nein; Ja]

Weitere Symptome / Beschwerden zum heutigen Zeitpunkt? [Muskel- / Gelenk- oder Gliederschmerzen; Riech- oder Geschmacksstörung; Schnupfen; Kopfschmerzen; Übelkeit/Erbrechen; Durchfall;Sonstige, und zwar: Freitext]

Haben Sie heute Ihren Blutdruck gemessen? [Nein; Ja; Werte]

Haben Sie heute Ihre Herzfrequenz / Ihren Puls gemessen? [Nein; Ja]

Haben Sie eine Gesundheitsvollmacht? [Nein; Ja]

Haben Sie eine Patientenverfügung? [Nein; Ja]

Planung des Telefonmonitorings: Festlegung von Zeitpunkt(en) und Ausmaß[Person. Datum]

Überwachungsparameter [Blutdruckmessung (RR); Atemfrequenz; Herzfrequenzmessung (HF); Sauerstoffsättigung SpO2 (Messung der O2-Sättigung mittels Pulsoxymeter);

Universitätsklinikum Heidelberg – Abteilung Allgemeinmedizin und Versorgungsforschung

CovidCare - Datenschutzkonzept - Version 0.12 23.12.2021

Seite 18 von 71

Körpertemperatur messen; Gewicht;  
Trinkmenge protokollieren (innerhalb von 24 Stunden); Weitere]  
Termin Telefonmonitoring [Datum nächster Termin;Intervall]

### 6.3. 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 folgenden Domänen:

- Hospitalisierung aufgrund COVID-19
- Diagnose Pneumonie (Crb-65 Index) bei bestätigten COVID-19 Patienten
- Palliativbehandlung bei bestätigten COVID-19 Patienten
- Mortalitätsrate bei bestätigten COVID-19 Patienten.  
Angst bei bestätigten COVID-19 Patienten, gemessen unter Verwendung von Generalized Anxiety Disorder Index (GAD-2)
- Identifizierung von prädiktiven Risikofaktoren auf die Ergebnisse, wie Hospitalisierung, Intensivpflege und Sterblichkeit

Der lokal gespeicherte Datensatz wird anhand des abgestimmten Analyseplans ausgewertet, die dabei generierten Kennzahlen werden zentral zusammengeführt und meta-analytisch seitens der Universitätsklinik Heidelberg ausgewertet.

### 6.4. Auflistung der Exportvariablen

Nachfolgend finden Sie einen Link zu einem Dokument, welches die aktuellen Exportvariablen auflistet: 1212.

Sofern die mündliche Einwilligung der Patienten (Bestätigung des Feld „Einverständniserklärung zur Teilnahme“) vorliegt, werden folgende Variablen exportiert: **siehe Kapitel 12**

## 7. Beschreibung der datenbezogenen Prozesse

Die datenschutzbezogenen Prozesse werden im Folgenden anhand der in Kapitel 4 beschriebenen Anwendungsszenarien beschrieben.

### 7.1. Ärztliche Primärdokumentation (Software CovidCare)

#### 7.1.1. Prozesse in der Versorgungssituation

Bei der CareCockpit-Software handelt es sich um eine Intranet-Lösung, d.h. der Webserver und die Datenbank liegen auf einem eigenen, lokalen Server der dafür verantwortlichen Leistungserbringer (dezentral). Der Zugriff zu Zwecken der ärztlichen Primärdokumentation erfolgt mittels Endgeräts (Laptop/Tablet/PC) per Browser über ein Netzwerk (LAN) in der Verantwortung der leistungserbringenden Versorgungseinrichtung. Alternativ kann ein Zugriff auf den Server über ein LTE-Datennetz über VPN erfolgen.

#### **Zugriff, Dateneingabe, Benutzerverwaltung**

Der behandelnde Arzt/die VERAH loggt sich mit seinen/ihren Benutzerdaten (Benutzername und Passwort) in die CareCockpit-Software ein und öffnet die Patientenakte des Patienten. Er/sie gibt Daten, die zum Zweck des medizinischen Monitorings dokumentiert werden, über die Tastatur ein und speichert diese. Die Datenhaltung erfolgt dezentral durch die Leistungserbringer. 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 Hausarztpraxis, von einem Administrator durchgeführt. Nur ein Administrator ist berechtigt, Rollen zu ändern und Passwörter zu setzen.

#### **Plausibilität und Vollständigkeit**

Die CareCockpit-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 Leistungserbringer gespeichert. Es werden keine behandlungsrelevanten Dokumente (z.B. Arztbriefe, externe Befunde) patientenbezogen als Dokumente abgelegt. Die in den Monitorings

erzeugten Arztberichte werden bei jedem Aufruf dynamisch generiert und können lediglich ausgedruckt werden. Das aufkommende Datenvolumen für jede einzelne leistungserbringende Versorgungseinrichtung ist abhängig von der Anzahl der Patienten und Monitorings, ist aber insgesamt betrachtet als gering 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 Monitoringverlauf über Zeit dargestellt werden. Die Patienten-ID (Patientenliste) wird ausschließlich zu Monitoringzwecken lokal in der Datenbank der Leistungserbringer gespeichert und ist durch die Benutzerverwaltung vor nicht-autorisiertem Zugriff geschützt.

## Technische Voraussetzungen der ärztlichen Primärdokumentation mittels CovidCare

Die technischen Voraussetzungen für die Umsetzung der unter Kapitel 4.1 beschriebenen ärztlichen Primärdokumentation sind abhängig von den Anforderungen der Dokumentation mittels der CovidCare Software. Standortseitig muss auf eine bereits vorhandene EDV Infrastruktur zurückgegriffen werden. Die Datenschutzkonformität und Datensicherheit einer Arztpraxis wird vorausgesetzt. Daher wird das Thema IT Sicherheit und firewall in diesem Dokument nicht behandelt. Für die Installation von CareCockpit kann ein handelsüblicher, aktueller Windows Rechner mit Betriebssystem ab Windows 10 oder Windows Server ab Version 2012 genutzt werden. Bei Leistungserbringern, die gleichzeitig mehrere Dokumentationsplätze betreiben, kommen Endgeräte zur ärztlichen Dokumentation zum Einsatz, die über LAN oder alternativ VPN / LTE mit dem lokalen Server der Leistungserbringer verbunden sind.

### 7.1.2. Kommunikationsprozesse und dezentrale Datenhaltung durch die Leistungserbringer

Die Endgeräte (Laptop/Tablet/PC) übertragen die über eine Browseranwendung eingegebenen Daten der medizinischen Behandlung zu Dokumentationszwecken direkt zum lokalen Server des Leistungserbringers. Die Daten werden dort in einer relationalen Datenbank gespeichert. Die Daten (vgl. Kapitel 8.1.1), 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 Monitoring- und Primärdokumentationszwecken außerhalb der Zuständigkeit des Leistungserbringers gespeichert.**

### 7.1.3. Datennutzung und Auswertung

Die dezentral gespeicherten Daten werden im Rahmen der ärztlichen Primärdokumentation zum Zweck des medizinisches Monitorings, eventuell der medizinischen Behandlung seitens der Leistungserbringer genutzt.

#### 7.1.4. 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 der Leistungserbringer zuständig.

### 7.2. Statistik (Surveillance) und Forschung

Zweck der Surveillance ist eine regelmäßige, über mehrere Standorte hinweg harmonisierte Erstellung von Statistiken zum Gesundheitszustand der Population, die Hospitalisierungsprävalenz aufgrund COVID-19 und Effekte von Risikofaktoren auf den Verlauf der Erkrankung. Basierend auf relevanten medizinischen Monitoringdaten erfolgt eine indikatorbasierte, automatisierte und lokal durchgeführte Sekundärdatenanalyse (vgl. 7.2). Die dadurch generierten anonymen Kennzahlen werden auf einen zentralen Surveillance-Server exportiert zur praxisübergreifenden Metaanalyse und Berichterstattung. Technisch analog zu diesem Verfahren erfolgt die Forschung (siehe 4.2).

#### 7.2.1. 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 Analyseplans automatisiert und innerhalb der lokalen Server-Strukturen der Leistungserbringer ausgewertet, mit dem Ziel der Erstellung anonymer Kennzahlen. Die dafür notwendigen Zwischenergebnisse werden im Zuge des automatisierten Auswertungsprozesses als xml-Datei auf dem lokalen Server der Leistungserbringer temporär gespeichert und nach Erstellung der anonymen Kennzahl wiederum automatisiert gelöscht. Aus dem Ergebnis der anonymen Kennzahl ist kein Personenbezug mehr herstellbar.

#### 7.2.2. 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 CovidCare-Software (Push-Verfahren).
- ii. Der Export der Daten erfolgt in Form einer XML-Datei mit den zur Berechnung der Indikatoren erforderlichen Daten. Diese XML-Datei beinhaltet keine eindeutig personenidentifizierenden Merkmale wie bspw. Namen oder Geburtsdatum. Die XML-Datei wird temporär auf dem Server der

Leistungserbringer 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 Regressionsverfahren).

iv. Die dadurch generierten anonymen Kennzahlen (Output) werden lokal gespeichert.

v. Alle temporär gespeicherten Exporte aus den Datenbanken der Primärdokumentation (xml-Dateien) werden automatisiert gelöscht.

### 7.2.3. Grundlage der automatisierten Auswertung: Programmierung eines Skriptes und Transfer auf den lokalen Server der Leistungserbringer

Zur automatisierten Auswertung wird durch das Universitätsklinikum ein Skript (Algorithmus) programmiert. Das Skript führt bei aktivem Initiieren eines autorisierten Arztes (1.) die lokalen Exporte der XML-Datei, (2.) die statistischen Berechnungen, (3.) die automatisierte Löschung der temporär gespeicherten XML-Dateien sowie (4.) die lokale Speicherung der anonymen Kennzahlen durch. Das Skript ist Teil des CovidCare Moduls und wird den Leistungserbringern mit der Software zur Verfügung gestellt.

### 7.2.4. Zentrales Zusammenführen der anonymen Kennzahlen (KTM-ZeDAC-Verfahren)

Die anonymen Kennzahlen (anonymisiertes Ergebnis der lokalen, automatisierten Auswertung) werden in regelmäßigen Abständen mittels der CareCockpit-Software von den Servern der Leistungserbringer auf einen zentralen Surveillance-Server des Universitätsklinikums Heidelberg exportiert. Die Zeitintervalle des Exports sind variabel und werden den Leistungserbringern mitgeteilt. Bei neu hinzugekommenen Studiendaten ist 1 Export/Woche, vorgesehen, andernfalls ist der Export von Prozessdaten zum Quartalsende ausreichend. Im Projektzeitraum werden die geeigneten Zeitintervalle für den Export der Surveillance-Daten in Abhängigkeit der einzelnen Indikatoren geprüft und ggf. adaptiert. Der verantwortliche, behandelnde Arzt / eine VERAH einer Praxis (Leistungserbringer) stößt den Prozess des Datenexports aktiv an, in dem er zu definierten Zeitpunkten die Export-Schaltfläche aktiviert (Push-Verfahren). Der autorisierte Arzt / die autorisierte VERAH erhält zu den definierten Zeitpunkten ggf. über die Software eine Erinnerung, mit der Bitte eines Datenexports der pseudonymisierte Daten. Diese Erinnerung kann durch den Nutzer in den Einstellungen deaktiviert werden. Durch die Aktivierung der Exportschaltfläche werden die anonymen Kennzahlen von dem lokalen Server der Leistungserbringer 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 ausschließlich Textdateien übermittelt werden. Die Kennzahlen ohne Personenbezug werden nach dem folgenden KTM-ZeDAC-Verfahren von dem dezentralen, lokalen Server der Leistungserbringer zu dem zentralen Surveillance Server übertragen:

- Der nach dem Rollenkonzept autorisierte Benutzer (i.d.R. ein behandelnder Arzt oder eine VERAH) startet den Export der Daten zur Surveillance innerhalb der CareCockpit-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 CareCockpit-Software übergibt die anonymen Daten an das KTM (Kryptographie- 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.

### 7.2.5. Organisatorische Sicherheitsmaßnahmen bezüglich der automatisierten Auswertung:

Da nicht in jedem Fall davon ausgegangen werden kann, dass die Praxen das Exportskript prüfen können, werden folgende organisatorischen Sicherheitsmaßnahmen implementiert:

- a. Zur Prüfung, dass durch das automatische Verfahren keine personenbezogenen Daten die Arztpraxis verlassen, wird der Export der anonymen Kennzahlen von dem Server der Leistungserbringer auf den zentralen Surveillance-Server nur aktiv durch einen autorisierten, behandelnden Arzt / eine VERAH ermöglicht (Push-Verfahren).
- b. Nach aktivem Auslösen des Exports durch den autorisierten Arzt / VERAH werden die Daten übertragen.
- c. In der Exporthistorie erscheint sodann ein Eintrag mit dem aktuellen Datum. Das exportierte XML-File kann durch Klicken auf den Eintrag geöffnet werden, sodass der Arzt / die VERAH die übertragenen Daten einsehen kann.

### 7.2.6. 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:

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



### 7.2.7. Datennutzung der zentral gespeicherten Daten für ein Reporting (Surveillance)

Die zentral von unterschiedlichen Praxen aus unterschiedlichen Standorten zusammengeführten, anonymen Kennzahlen werden (1.) mittels Metaanalyse zu Surveillance-Zwecken ausgewertet sowie (2.) einer Berichterstellung unterzogen. Die anonymen Ergebnisse der Metaanalysen werden über alle Einrichtungen hinweg (Ergebnisse der Metanalyse) berichtet.

#### 7.2.7.1. Report über alle Einrichtungen hinweg

Zum Zwecke einer Berichterstattung über alle Einrichtungen hinweg werden von dem Biometriker oder Datenanalyst, der lt. Zugriffskonzept autorisierten Zugriff auf den Surveillance Server hat, Metaanalysen der anonymen Kennzahlen durchgeführt und die Ergebnisse in einer noch festzulegenden Form an einen Wissenschaftler der Abt. Allgemeinmedizin und Versorgungsforschung des Universitätsklinikum Heidelberg ausgehändigt.

### 7.2.8. Löschung / Anonymisierung

Die anonymen Kennzahlen werden sowohl im Falle der Statistik (Surveillance) als auch im Falle der ohne Personenbezug auf den zentralen Surveillance-Server exportiert und dort gespeichert. Eine Löschung ist nicht erforderlich. Sofern während des Projektzeitraums die Rechtsnachfolge für den Weiterbetrieb nicht geklärt werden kann, wird die zentrale Zusammenführung der Kennzahlen zu Zwecken der Surveillance und Forschung eingestellt. Für einen von diesen sekundäranalytischen Anwendungszwecken unabhängigen, etwaigen Weiterbetrieb der Software CareCockpit / CovidCare zu Zwecken der ärztlichen Dokumentation, werden gemeinsam mit den beteiligten Leistungserbringern während der Projektlaufzeit ein tragfähiges Konzept für den technischen Support entwickelt.

## 8. Schutzbedarfsanalyse

Die IT-Grundschutz-Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) empfiehlt drei Schutzbedarfskategorien:

- normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
- hoch: Die Schadensauswirkungen können beträchtlich sein.
- sehr hoch: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

### 8.1. Ärztliche Primärdokumentation (CovidCare)

Im Zuge der ärztlichen Primärdokumentation werden personenbezogene Daten besonderer Art zu medizinischen Behandlungszwecken erhoben. Hinsichtlich des datenschutzrechtlichen Grundwerts „Vertraulichkeit“ haben diese Daten einen **hohen bis sehr hohen Schutzbedarf**.

Im Folgenden werden mögliche Risikoszenarien angeführt. Entsprechende Schutzmaßnahmen dagegen werden in Kapitel 10.1 angeführt.

### 8.1.1. Unerlaubter Zugriff auf medizinische Daten in der versorgenden Einrichtung

Ein Zugriff auf medizinische Behandlungsdaten ist nur möglich über

- ein Tablet oder einen Laptop innerhalb der leistungserbringenden Einrichtung mittels Browser,
- ein Tablet oder einen Laptop innerhalb der leistungserbringenden Einrichtung von einem Remote-Standort über VPN mittels Browser,
- den Server des Leistungserbringers auf Datenbankebene.

Die Übermittlung der Behandlungsdaten erfolgt über verschlüsselte Kanäle. Die Daten werden nur auf dem lokalen Server der Leistungserbringer verschlüsselt gespeichert. Der Zugriff innerhalb der leistungserbringenden Einrichtung wird durch ein rollenbasiertes Berechtigungskonzept auf einen engen und definierten Personenkreis eingeschränkt sowie durch passwortgeschützte Authentifizierung sichergestellt. Das Risiko eines unerlaubten Zugriffs ist somit als gering einzustufen.

### 8.1.2. Unerlaubtes Kopieren

Dokumente können aufgrund der Tatsache, dass sie in einem Browser angezeigt werden, heruntergeladen und damit kopiert werden. Da zum Zugriff auf ein Dokument eine explizite Zugriffsberechtigung des Benutzers vorliegen muss, kann damit das Risiko des unerlaubten Kopierens reduziert werden. Das Risiko ist daher als mittel einzustufen.

### 8.1.3. Unerlaubtes Löschen

Dokumente lassen sich nur von Benutzern löschen, die eine explizite Zugriffsberechtigung haben. Das Risiko eines unerlaubten Löschens ist als gering einzustufen.

### 8.1.4. Unerlaubtes Einstellen von Daten

Dokumente lassen sich nur von Benutzer einstellen, die eine explizite Zugriffsberechtigung haben. Das Risiko eines unerlaubten Einstellens von Daten ist als gering einzustufen.

### 8.1.5. Surveillance

Zu Zwecken der Surveillance werden anonyme Kennzahlen exportiert und gespeichert. Hinsichtlich des datenschutzrechtlichen Grundwerts „Vertraulichkeit“ haben diese Daten einen **normalen Schutzbedarf**. Im Folgenden werden mögliche Risikoszenarien angeführt. Entsprechende Schutzmaßnahmen dagegen werden in Kapitel 10.2 und 10.3 angeführt.

### 8.1.6. Unerlaubter Zugriff auf den Surveillance-Server

Ein Zugriff auf Surveillance-Daten ist nur über den im Universitätsklinikum Heidelberg stehenden Surveillance-Server auf Datenbankebene möglich. Die Server (Surveillance-Server und ZeDAC-Server) stehen in einer geschützten, demilitarisierten Zone (DMZ) des Universitätsklinikum Heidelberg. Der Zugriff ist auf einen engen Personenkreis beschränkt. Das Risiko eines unerlaubten Zugriffs ist somit als **sehr gering einzustufen**. Ein Transfer der anonymen Kennzahlen geschieht nur über das in Kapitel 8.2.4 beschriebene ZeDAC-KTM-Verfahren. Die Daten werden immer vorab verschlüsselt und jede Übermittlung erfolgt ausschließlich über verschlüsselte Kanäle. Der Zugriff auf den Datentransfer ist als **gering einzustufen**.

### 8.1.7. Gefahr der Re-Identifikation von Patienten

Auf dem Surveillance-Server besteht aufgrund der Anonymisierung der Kennzahlen sowie unter Berücksichtigung der zusätzlichen Schutzmaßnahmen theoretisch kein Restrisiko zur Re-Identifikation der Patienten. Das Risiko der Re-Identifikation ist daher als **sehr gering einzustufen**.

## 9. 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).

### 9.1. Maßnahmen in den versorgenden Einrichtungen

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

#### 9.1.1. 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 Leistungserbringer gegenüber dem Universitätsklinikum Heidelberg schriftlich bestätigt.

##### 9.1.1.1. 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.

#### 9.1.1.2. 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](http://www.beyondtrust.com)). Unnötige Benutzerkonten (die vielleicht einmal irrtümlich eingerichtet wurden) sollten gelöscht oder zumindest deaktiviert werden. Letzteres gilt auch für das „Gast“-Konto.

### 9.1.1.3. Zugangskontrolle

#### 9.1.1.3.1. Qualität und Vertraulichkeit von Passwörtern

Zur Kontrolle des Zugangs werden häufig Passwörtern verwendet. Hierzu gibt es eine Reihe von wichtigen Anmerkungen.

##### ***Qualität von Passwörtern***

Um eine effektive Sicherheit zu gewährleisten, müssen die Passwörter einigen Mindestkriterien genügen. So sollte ein Passwort mindestens acht Zeichen lang sein. Es sollte Groß- und Kleinbuchstaben beinhalten und möglichst auch Zahlen und Sonderzeichen.

##### ***Individualität von Passwörtern***

Ein weiteres Sicherheitskriterium von Passwörtern ist die Individualität. Für jedes Programm und jede Webseite muss ein eigenes Passwort erfunden werden. Andernfalls könnte ein Angreifer (oder neugieriger Kollege) durch das Wissen eines Passwortes an verschiedensten Stellen Schaden anrichten. Dieser Forderung liegt die Beobachtung zugrunde, dass Hacker ein bekanntes Passwort (optimalerweise in Verbindung mit einer E-Mail-Adresse) sofort an verschiedensten Stellen im Internet ausprobieren: ebay, Paypal und ähnliche Seiten sind ein lohnenswertes Ziel. Diese Forderung hat fast zwangsläufig zur Folge, dass man sich die Passwörter schriftlich notieren muss. An dieser Stelle bieten sich spezielle Computerprogramme an, die Passwörter verwalten können.

##### ***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.

##### ***Automatisches Speichern von Passwörtern***

Viele Programme bieten ein automatisches Speichern von Passwörtern an. Dies ist beispielsweise beim Internet-Explorer von Microsoft der Fall. Diese Option sollte man niemals nutzen, denn

- 1) vergisst man im Laufe der Zeit die Passwörter und im Falle eines Datenverlustes ist man hilflos,
- 2) nutzen auch Angreifer oder neugierige Kollegen diese gespeicherten Passwörter,
- 3) könnten die Passwörter durch ein Schadprogramm möglicherweise ausgelesen werden.

Aktuelle Schadprogramme lesen die Passwörter auf einer manipulierten Webseite aus und drücken automatisch auf den „OK-Knopf“. Aktuelle Forschungen haben ergeben, dass alle Browser extreme Sicherheitslücken in den Passwort-Managern aufweisen.

##### ***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, MSOffice-Dateien, für Remotedesktop und für VPN-Verbindungen.
- Durch Sternchen verborgene Passwörter werden im Klartext angezeigt.
- Aktuell zu übertragende Passwörter werden ausgelesen
- 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-Paragrafen“ (§202c StGB) durch das Strafgesetzbuch strafbar.

#### 9.1.1.4. Weitergabe der Kennzahlen

Die Weitergabe der lokal generierten anonymen Kennzahlen erfolgt ausschließlich über den Softwareexport in verschlüsselter Form, wie unter Kapitel 8.2.4 beschrieben. Eine Weitergabe von Datenträgern ist nicht vorgesehen.

#### 9.1.1.5. Eingabekontrolle

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

#### 9.1.1.6. 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.

### 9.1.2. Benutzer/Zugriffskonzept

#### 9.1.2.1. 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. Strukturhebungsbogen)

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

### 9.1.3. Absicherung der Kommunikationsprozesse seitens der Leistungserbringer

#### 9.1.3.1. Sicherheit Netzwerk LAN

Grundsätzlich empfehlen wir Clients **NICHT** per WLAN im Netzwerk zu betreiben, sondern das Intranet immer Kabelbasiert aufzubauen. Dennoch der Vollständigkeit halber eine Übersicht über die Entwicklungen in der WLAN Technik.

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 die Authentisierung und das Key-Management ohne zusätzliche Komponenten.

#### 9.1.4. Datensicherung

Datensicherung sollte durch die Leistungserbringer 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.

#### 9.1.5. Endgerät

Jedes Endgerät (Tablet, Laptop, PC) der Leistungserbringer greift per Browser auf die CovidCare-Software zu. Als Schutz vor unerlaubtem Zugriff greift hier die Benutzerverwaltung des Betriebssystems, als auch die Benutzerverwaltung mit Zugangsdaten und rollenbasierten Rechten der CareCockpit-Software. Einer unerlaubten Nutzung wird somit vorgebeugt. Ein Diebstahl eines

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

#### 9.1.6. Endgerät zu Server des Leistungserbringers

Die Kommunikation zwischen Endgerät und Server des Leistungserbringers erfolgt, je nach technischer IT-Infrastruktur vor Ort, entweder über das lokale LAN-Netzwerk oder über eine sichere LTE-Datenverbindung über VPN.

#### 9.1.7. Server des Leistungserbringers

Als Schutz vor unerlaubtem Zugriff greift hier die Benutzerverwaltung des Betriebssystems. Des Weiteren greifen die in Kapitel 10.1.1 empfohlenen Maßnahmen um den Server des Leistungserbringers effektiv zu schützen. Die Daten werden in der Datenbank des Leistungserbringers verschlüsselt abgelegt.

### 9.2. Prozess Leistungserbringer 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.

#### 9.2.1. 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 KTMZeDAC-Verfahren (Hybride Verschlüsselung mit RSA 4096 Bit und AES 256 Bit) gesichert.

##### 9.2.1.1. 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 CovidCare-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.

##### 9.2.1.2. 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.

### 9.2.2. Personelle Maßnahmen

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

### 9.2.3. 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:

#### 9.2.3.1. Zutrittskontrolle

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

#### 9.2.3.2. Zugangskontrolle

Alle Systembenutzer (vgl. 9.3.1 Zugriffskonzept) müssen einen personalisierten Zugang zum Netzwerk des Universitätsklinikum Heidelberg besitzen. Zusätzlich erhalten sie einen personalisierten Zugang (Benutzeraccount), mit dem sie sich am Surveillance Server authentifizieren müssen.

#### 9.2.3.3. 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.

#### 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.

#### 9.2.3.4. Datensicherung

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

### 9.3. Maßnahmen Surveillance Server und Reporting

Zu Zwecken der Berichterstattung der Ergebnisse werden durch wissenschaftliche Mitarbeiter der Abteilung Allgemeinmedizin und Versorgungsforschung des Universitätsklinikum Heidelberg (Wissenschaftler) Reports erstellt. Auf Grundlage der auf dem Surveillance Server zur Verfügung stehenden anonymen Kennzahlen werden von einem Mitarbeiter des Instituts für Medizinische Biometrie und Informatik des Universitätsklinikum Heidelberg (Statistiker) anhand von definierten Indikatorbeschreibungen Metaanalysen und Abbildungen 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.

#### 9.3.1. 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 <sup>1</sup>		x	x	x		x	
Biometriker <sup>2</sup>		x	x	x		x	
IT-Datenmanager <sup>3</sup>		x	x		x	x	
Datenschutzbeauftragter <sup>4</sup>					x		

Wissenschaftler<sup>1</sup> (Abt. Allgemeinmedizin und Versorgungsforschung, Universitätsklinikum Heidelberg)

Biometriker<sup>2</sup> (Abt. Allgemeinmedizin und Versorgungsforschung, Universitätsklinikum Heidelberg)

IT/Datenmanager<sup>3</sup> (Abt. Allgemeinmedizin und Versorgungsforschung, Universitätsklinikum Heidelberg)

Datenschutzbeauftragter<sup>4</sup> (Universitätsklinikum Heidelberg)

## 10. Fristen und Ausblick

Die Laufzeit der CovidCare-Studie endet am 31.12.2021, das CovidCare-Modul läuft noch bis einschließlich 31.12.2022 mit Option auf Verlängerung bei Andauern der Pandemie. Nach dem 31.12.2021 ist ein Studieneinschluss nicht mehr möglich. Datenexporte sind momentan

wöchentlich geplant. Die Exportzeitpunkte werden bei Bedarf dem Pandemiegesehen angepasst.

## 11. 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](http://www.ieee.org))  
ISO International Organization for Standardization ([www.iso.org](http://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](http://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](http://www.ietf.org/rfc))  
RKI Robert Koch-Institut ([www.rki.de](http://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  
VPN Virtual Private Network  
WHO World Health Organization ([www.who.org](http://www.who.org))  
WLAN Wireless LAN

## 12. Exportvariablen der Schnittstelle

### Modul "CovidCare" (Projekt)

<content version="P">

Praxis

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME

lastmodified	Zeitstempel der letzten Änderung	DATETIME
--------------	----------------------------------	----------

### Patient

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
geschlecht		CHAR(1) [M,W,I]
<i>geburtsjahr</i>	Aus geburtsdatum extrahiert	CHAR(4), YYYY
beendet		CHAR(1) [J,N]
beendetDatum		DATE, YYYY-MM-DD
beendetGrund		CHAR(1) [A:Arzt, P:Patient, D:Tod]
beendetGrundPatientDatenLoeschen	Daten löschen	CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

### Assessment

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
o_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

<b>Monitoring Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
o_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
o_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

## Modul "CovidCare" (Studie)

<content version="S">

(rot markierte Variablen werden ab der Version 3.4.0 neu exportiert)

### Praxis

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

### Patient

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
geschlecht		CHAR(1) [M,W,I]
einverstaendnisSchriftlichDatum		DATE, YYYY-MM-DD
beendet		CHAR(1) [J,N]
beendetDatum		DATE, YYYY-MM-DD
beendetGrund		CHAR(1) [A:Arzt, P:Patient, D:Tod]
beendetGrundPatientDatenLoeschen	Daten löschen	CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

### Assessment

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT

o_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
durchfuehrendeVerah_id	referenziert auf das Feld id der Tabelle Verah, welche aktuell nicht exportiert wird	INT
o_corona_id	referenziert auf das Feld id der Tabelle Corona	INT
o_symptome_id	referenziert auf das Feld id der Tabelle Symptome	INT
o_werte_id	referenziert auf das Feld id der Tabelle Werte	INT
o_ueberwachung_id	referenziert auf das Feld id der Tabelle Ueberwachung	INT
aktuellesAlter		INT
zucker		CHAR(1) [J,N]
zuckerDiabetes2		CHAR(1) [J,N]
zuckerDiabetes1		CHAR(1) [J,N]
herzkreislauf		CHAR(1) [J,N]
herzkreislaufHypertonie		CHAR(1) [J,N]
herzkreislaufKhk		CHAR(1) [J,N]
herzkreislaufHerzinsuffizienz		CHAR(1) [J,N]
herzkreislaufVorhofflimmern		CHAR(1) [J,N]
herzkreislaufPavk		CHAR(1) [J,N]
herzkreislaufApoplex		CHAR(1) [J,N]
herzkreislaufSonstig		CHAR(1) [J,N]
herzkreislaufSonstigText		CHAR(200)
lungenerkrankung		CHAR(1) [J,N]
lungenerkrankungCopd		CHAR(1) [J,N]
lungenerkrankungAsthma		CHAR(1) [J,N]



lungenerkrankungSonstig	CHAR(1) [J,N]
lungenerkrankungSonstigText	CHAR(200)
lebererkrankung	CHAR(1) [J,N]
lebererkrankungLeberzirrhose	CHAR(1) [J,N]
lebererkrankungSonstig	CHAR(1) [J,N]
lebererkrankungSonstigText	CHAR(200)
nierenerkrankung	CHAR(1) [J,N]
nierenerkrankungText	CHAR(200)
nierenerkrankungGrad	CHAR(1)
immunsystem	CHAR(1) [J,N]
immunsystemMaligne	CHAR(1) [J,N]
immunsystemLeukozytopenie	CHAR(1) [J,N]
immunsystemTransplantation	CHAR(1) [J,N]
immunsystemSonstig	CHAR(1) [J,N]
immunsystemSonstigText	CHAR(200)
medikamenteGlukokortikoide	CHAR(1) [J,N]
medikamenteImmunsuppressiva	CHAR(1) [J,N]
medikamenteImmunmodulatoren	CHAR(1) [J,N]
medikamenteZytostatika	CHAR(1) [J,N]
medikamenteSonstig	CHAR(1) [J,N]
medikamenteSonstigText	CHAR(200)
krebserkrankung	CHAR(1) [J,N]
erkrankungWeitere	CHAR(1) [J,N]
erkrankungWeitereSonstig	CHAR(1) [J,N]
erkrankungWeitereSonstigText	CHAR(200)
stationaer	CHAR(1) [J,N]
stationaerText	CHAR(200)

adipositasGewicht		FLOAT
adipositasGroesse		FLOAT
adipositasBmi		INT
rauchen		CHAR(1) [J,N]
rauchenSeit		INT
rauchenMenge		INT
rauchenNein		CHAR(1) [J,N]
pneumokokken		CHAR(1) [J,N]
pneumokokkenJahr		CHAR(4), YYYY
influenza		CHAR(1) [J,N]
medikamentenplan		CHAR(1) [J,N]
gesundheitsvollmacht		CHAR(1) [J,N]
patientenverfuegung		CHAR(1) [J,N]
durchfuehrung		CHAR(1) [J,N]
durchfuehrungWeiterZeit		TIME, HH:MM
coronaSymptomeBeginnDatum		DATE, YYYY-MM-DD
coronaSymptomeBeginnDatumNicht		CHAR(1) [J,N]
zeitstrahl	In Wochen	INT
monitoringIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
monitoringDatum		DATE, YYYY-MM-DD
monitoringZeit		TIME, HH:MM
assessmentOrt		CHAR(1) [T:Telefon, P:Praxis, H:Hausbesuch]
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

<b>Monitoring Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
o_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
o_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
durchfuehrendeVerah_id	referenziert auf das Feld id der Tabelle Verah, welche aktuell nicht exportiert wird	INT
o_corona_id	referenziert auf das Feld id der Tabelle Corona	INT
o_symptome_id	referenziert auf das Feld id der Tabelle Symptome	INT
o_werte_id	referenziert auf das Feld id der Tabelle Werte	INT
o_ueberwachung_id	referenziert auf das Feld id der Tabelle Ueberwachung	INT
abschluss		CHAR(1) [J,N]
abschlussZustand		CHAR(1) [K:Kuriert, V:Verstorben]
abschlussZustandKuriertDatum		DATE, YYYY-MM-DD
abschlussZustandKuriertVerlauf		CHAR(1) [1:Leicht, 2:Moderat, 3:Schwer, 4:Kritisch]
abschlussZustandKuriertVerlaufKkh		CHAR(1) [J,N]
abschlussZustandKuriertVerlaufKkhEin weisungDatum		DATE, YYYY-MM-DD

abschlussZustandKuriertVerlaufKkhIntensiv	CHAR(1) [J,N]
abschlussZustandKuriertVerlaufKkhBeatmet	CHAR(1) [J,N]
abschlussZustandKuriertVerlaufKkhEntlassungDatum	DATE, YYYY-MM-DD
abschlussZustandKuriertSymptome	CHAR(1) [N:Nein, T:Teilweise, J:Ja]
abschlussZustandKuriertSymptomeText	CHAR(200)
abschlussZustandKuriertZustand	INT [0:sehr schlecht...10:sehr gut]
abschlussZustandKuriertTestPositiv	CHAR(1) [J,N]
abschlussZustandKuriertHilfreich	CHAR(1) [1:Sehr, 2:Hilfreich, 3:Unentschieden, 4:Wenig, 5:Nicht]
abschlussZustandVerstorbenDatum	DATE, YYYY-MM-DD
abschlussZustandVerstorbenOrt	CHAR(1) [K:Krankenhaus, H:Häuslich]
abschlussZustandVerstorbenOrtKkhEinweisungDatum	DATE, YYYY-MM-DD
abschlussZustandVerstorbenOrtKkhIntensiv	CHAR(1) [J,N]
abschlussZustandVerstorbenOrtKkhIntensivTage	INT
abschlussZustandVerstorbenOrtHausePalliativ	CHAR(1) [J,N]
abschlussZustandVerstorbenOrtHausePalliativBetreuung	CHAR(1) [H:Hausarzt, S:SAPV]
vordergrundText	CHAR(200)
schwierigkeiten	CHAR(1) [J,N]
schwierigkeitenText	CHAR(200)
dokumentiert	CHAR(1) [J,N]

dokumentiertText		CHAR(200)
besonderheiten		CHAR(1) [J,N]
besonderheitenText		CHAR(200)
medikamenteWeitere		CHAR(1) [J,N]
medikamenteWeitereText		CHAR(2000)
medikamenteSchwierigkeiten		CHAR(1) [J,N]
medikamenteSchwierigkeitenText		CHAR(2000)
angst		CHAR(1) [J,N]
anspannung		CHAR(1) [0:Nicht, 1:Einzel, 2:Mehr, 3:Jeden]
sorgen		CHAR(1) [0:Nicht, 1:Einzel, 2:Mehr, 3:Jeden]
monitoringDatum		DATE, YYYY-MM-DD
monitoringZeit		TIME, HH:MM
verwirrt		CHAR(1) [J,N]
monitoringOrt		CHAR(1) [T:Telefon, P:Praxis, H:Hausbesuch]
komplett		CHAR(1) [J,N]
dauer		TIME, HH:MM
konsequenzIntervall		CHAR(1) [J,N]
monitoringIntervall		CHAR(1) [Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
o_ueberwachung_id_konsequenz	referenziert auf das Feld id der Tabelle Ueberwachung	INT
konsequenzAbschluss		CHAR(1) [J,N]
monitoringAbschlussDatum		DATE, YYYY-MM-DD
monitoringAbschlussZeit		TIME, HH:MM

created	Zeitstempel der Erstellung des Datensatzes	DATETIME
---------	--	----------

lastmodified	Zeitstempel der letzten Änderung	DATETIME
--------------	----------------------------------	----------

## Corona

Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
----------	-----------	----------------------------------

id	Autoinkrementelle, interne ID	INT
----	-------------------------------	-----

test		CHAR(1) [J,N]
------	--	---------------

testDatum		DATE, YYYY-MM-DD
-----------	--	------------------

testErgebnis		CHAR(1) [P:Positiv, N:Negativ, U:Ausstehend]
--------------	--	--

testVeranlasst		CHAR(1) [J,N]
----------------	--	---------------

testVeranlasstDatum		DATE, YYYY-MM-DD
---------------------	--	------------------

haushaltAlleine		CHAR(1) [J:Ja, N:Nein, H:Heim]
-----------------	--	--------------------------------

haushaltAlleineBezugsperson		CHAR(1) [J,N]
-----------------------------	--	---------------

haushaltPersonen		INT
------------------	--	-----

haushaltPersonenPositiv		CHAR(1) [J,N]
-------------------------	--	---------------

haushaltPersonenPositivAnzahl		INT
-------------------------------	--	-----

haushaltPersonenPositivDatum		DATE, YYYY-MM-DD
------------------------------	--	------------------

haushaltPersonenBezugsperson		CHAR(1) [J,N]
------------------------------	--	---------------

haushaltHeimPositiv		CHAR(1) [J,N]
---------------------	--	---------------

haushaltHeimPositivDatum		DATE, YYYY-MM-DD
--------------------------	--	------------------

created	Zeitstempel der Erstellung des Datensatzes	DATETIME
---------	--	----------

lastmodified	Zeitstempel der letzten Änderung	DATETIME
--------------	----------------------------------	----------

## Symptome

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
allgemein		CHAR(1) [J,N]
allgemeinDatum		DATE, YYYY-MM-DD
allgemeinHeuteWert		CHAR(1) [1:Keine, 2:Leicht, 3:Mittel, 4:Stark]
husten		CHAR(1) [J,N]
hustenDatum		DATE, YYYY-MM-DD
hustenHeuteWert		CHAR(1) [1:Keine, 2:Leicht, 3:Mittel, 4:Stark]
hustenAuswurf		CHAR(1) [J,N]
atem		CHAR(1) [J,N]
atemDatum		DATE, YYYY-MM-DD
atemHeuteWert		CHAR(1) [1:Keine, 2:Leicht, 3:Mittel, 4:Stark]
atemHeuteVerlauf		CHAR(1) [1:Gleich, 3:Schlechter, 4:Deutlich schlechter]
atemZaehlen		CHAR(1) [J:Ja, U:Unsicher, N:Nein]
hals		CHAR(1) [J,N]
halsDatum		DATE, YYYY-MM-DD
halsHeuteWert		CHAR(1) [1:Keine, 2:Leicht, 3:Mittel, 4:Stark]
fieber		CHAR(1) [J,N]
fieberWert		FLOAT
fieberDatum		DATE, YYYY-MM-DD
fieberHeute		CHAR(1) [J,N]
fieberHeuteWert		FLOAT

feiberHeuteZeit		TIME, HH:MM
weitereGliederschmerzen		CHAR(1) [J,N]
weitereGliederschmerzenDatum		DATE, YYYY-MM-DD
weitereGeschmacksstoerung		CHAR(1) [J,N]
weitereGeschmacksstoerungDatum		DATE, YYYY-MM-DD
weitereSchnupfen		CHAR(1) [J,N]
weitereSchnupfenDatum		DATE, YYYY-MM-DD
weitereKopfschmerzen		CHAR(1) [J,N]
weitereKopfschmerzenDatum		DATE, YYYY-MM-DD
weitereErbrechen		CHAR(1) [J,N]
weitereErbrechenDatum		DATE, YYYY-MM-DD
weitereDurchfall		CHAR(1) [J,N]
weitereDurchfallDatum		DATE, YYYY-MM-DD
weitereSonstig		CHAR(1) [J,N]
weitereSonstigText		CHAR(200)
weitereSonstigDatum		DATE, YYYY-MM-DD
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Werte</b>		
<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
blutdruck		CHAR(1) [J,N]
blutdruckSys		INT
blutdruckDia		INT
atem		CHAR(1) [J,N]



atemWert		INT
herz		CHAR(1) [J,N]
herzWert		INT
sauerstoff		CHAR(1) [J,N]
sauerstoffWert		INT
fieber		CHAR(1) [J,N]
fieberWert		FLOAT
gewicht		CHAR(1) [J,N]
gewichtWert		FLOAT
trinken		CHAR(1) [J,N]
trinkenWert		FLOAT
sonstig		CHAR(1) [J,N]
sonstigText		CHAR(200)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Überwachung</b>		
<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
blutdruck		CHAR(1) [J,N]
blutdruckIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
blutdruckSysOben		INT
blutdruckDiaOben		INT
blutdruckSysObenRot		INT
blutdruckDiaObenRot		INT

blutdruckSysUnten		INT
blutdruckSysUntenRot		INT
blutdruckDiaUntenRot		INT
blutdruckDiaUnten		INT
atem		CHAR(1) [J,N]
atemIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
atemOben		INT
atemObenRot		INT
atemUnten		INT
atemUntenRot		INT
herz		CHAR(1) [J,N]
herzIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
herzOben		INT
herzObenRot		INT
herzUnten		INT
herzUntenRot		INT
sauerstoff		CHAR(1) [J,N]
sauerstoffIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
sauerstoffUnten		INT
sauerstoffUntenRot		INT
fieber		CHAR(1) [J,N]
fieberIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]

feiberOben		FLOAT
feiberObenRot		FLOAT
feiberUnten		FLOAT
feiberUntenRot		FLOAT
gewicht		CHAR(1) [J,N]
gewichtIntervall	Pro Tag bzw. alle X Tage	CHAR(1) [D:Dreimal, Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
gewichtZiel		FLOAT
trinken		CHAR(1) [J,N]
trinkenEmpfohlen		FLOAT
sonstig		CHAR(1) [J,N]
sonstigText		CHAR(200)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

## Modul "UlcusCrurisCare"

### Praxis

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
bsnr	Betriebsstättennummer	CHAR(9)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

### Patient

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
geschlecht		CHAR(1) [M,W,I]
einverstaendnisSchriftlichDatum		DATE, YYYY-MM-DD
beendet		CHAR(1) [J,N]
beendetDatum		DATE, YYYY-MM-DD
beendetGrund		CHAR(1) [A:Arzt, P:Patient, D:Tod]
beendetGrundPatientDatenLoeschen	Daten löschen	CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

### Assessment

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT

datum	Durchführungsdatum	DATE, YYYY-MM-DD
durchfuehrendeVerah_id	referenziert auf das Feld id der Tabelle Verah, welche aktuell nicht exportiert wird	INT
venoesBesenreiser		CHAR(1) [J,N]
venoesVarikosis		CHAR(1) [J,N]
venoesOedem		CHAR(1) [J,N]
venoesPigmentierung		CHAR(1) [J,N]
venoesEkzem		CHAR(1) [J,N]
venoesDermatoliposklerose		CHAR(1) [J,N]
venoesAtrophie		CHAR(1) [J,N]
u_phq9_id	referenziert auf das Feld id der Tabelle Phq9	INT
u_eq5d_id	referenziert auf das Feld id der Tabelle Eq5d	INT
patientenaufklaerung		CHAR(1) [J,N]
patientenaufklaerungNeinText		CHAR(200)
patientenaufklaerungKrankheitsbild		CHAR(1) [J,N]
patientenaufklaerungKompressionstherapie		CHAR(1) [J,N]
patientenaufklaerungWundbehandlung		CHAR(1) [J,N]
patientenaufklaerungBewegung		CHAR(1) [J,N]
patientenaufklaerungAllgemeinmassnahmen		CHAR(1) [J,N]
u_kompression_id	referenziert auf das Feld id der Tabelle Phq9	INT
allgemein		CHAR(2000)
monitoringIntervall	Pro Tag bzw. alle X Tage	CHAR(2) [1:1, 2:2, 3:3, 4:4, 5:5, 7:7, 10:10, 14:14]
monitoringDatum		DATE, YYYY-MM-DD

monitoringZeit		TIME, HH:MM
studienvisite1Datum		DATE, YYYY-MM-DD
studienvisite1Zeit		TIME, HH:MM
studienvisite2Datum		DATE, YYYY-MM-DD
studienvisite2Zeit		TIME, HH:MM
assessmentOrt		CHAR(1) [P:Praxis, H:Hausbesuch]
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### DiagnoseDesAssessments

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
icd10		CHAR(7)
text		CHAR(260)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### WundeDesAssessments

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT

u_wunde_id	referenziert auf das Feld id der Tabelle Wunde	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### Monitoring Feldname

Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
durchfuehrendeVerah_id	referenziert auf das Feld id der Tabelle Verah, welche aktuell nicht exportiert wird	INT
studienvisite		CHAR(1) [,,“(leer = Monitoring),1,2]
patientenaufklaerungKrankheitsbild		CHAR(1) [J,N]
patientenaufklaerungKompressionstherapie		CHAR(1) [J,N]
patientenaufklaerungWundbehandlung		CHAR(1) [J,N]
patientenaufklaerungBewegung		CHAR(1) [J,N]
patientenaufklaerungAllgemeinmassnahmen		CHAR(1) [J,N]
u_kompression_id	referenziert auf das Feld id der Tabelle Kompression	INT
allgemein		CHAR(2000)
adhaerenzTermine		INT [0-100]
adhaerenzBehandlungsmassnahmen		INT [0-100]
u_phq9_id	referenziert auf das Feld id der Tabelle Phq9	INT

u_eq5d_id	referenziert auf das Feld id der Tabelle Eq5d	INT
u_fima_id	referenziert auf das Feld id der Tabelle Fima	INT
pacicAusgehaendigt		CHAR(1) [J,N]
monitoringOrt		CHAR(1) [P:Praxis, H:Hausbesuch]
monitoringDatum		DATE, YYYY-MM-DD
monitoringZeit		TIME, HH:MM
konsequenzIntervall		CHAR(1) [J,N]
monitoringIntervall		CHAR(1) [Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
u_gesundheitsoekonomischeAnalyse_id	referenziert auf das Feld id der Tabelle GesundheitsoekonomischeAnalyse	INT
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### WundeDesMonitorings

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
u_wunde_id	referenziert auf das Feld id der Tabelle Wunde	INT



ref_assessment_wunde_id	referenziert auf das Feld id der Tabelle Wunde des bezugnehmenden Assessments	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### GesundheitsoekonomischeAnalyse

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
wundkontrollen		INT [0-100]
kontakte		INT [0-100]
abstrichuntersuchungen		INT [0-30]
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### Ueberweisung

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_gesundheitsoekonomischeAnalyse_id	referenziert auf das Feld id der Tabelle GesundheitsoekonomischeAnalyse	INT
facharztGruppe		CHAR(200)

datum	Durchführungsdatum	DATE, YYYY-MM-DD
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Einweisung Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_gesundheitsoekonomischeAnalyse_id	referenziert auf das Feld id der Tabelle GesundheitsoekonomischeAnalyse	INT
stationaerGruppe		CHAR(200)
datum	Durchführungsdatum	DATE, YYYY-MM-DD
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Arzneimittel Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_gesundheitsoekonomischeAnalyse_id	referenziert auf das Feld id der Tabelle GesundheitsoekonomischeAnalyse	INT
art		CHAR(2) [WA:Wundauflage, VM:Verbandsmittel, WS:Wundspüllösung, AB:Antibiotika, AM:Sonstige Arzneimittel, HM:Hilfsmittel]

name		CHAR(200)
laenge		FLOAT
breite		FLOAT
flaeche		FLOAT
anzahl		INT
pzn		CHAR(8)
datum	Durchführungsdatum	DATE, YYYY-MM-DD
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### Fima

<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
ambulantChirurg		CHAR(1) [J,N]
ambulantChirurgAnzahl		INT
ambulantChirurgWunde		CHAR(1) [J,N]
ambulantOrthopaede		CHAR(1) [J,N]
ambulantOrthopaedeAnzahl		INT
ambulantOrthopaedeWunde		CHAR(1) [J,N]
ambulantPsychiater		CHAR(1) [J,N]
ambulantPsychiaterAnzahl		INT
ambulantPsychiaterWunde		CHAR(1) [J,N]
ambulantDermatologe		CHAR(1) [J,N]

ambulantDermatologeAnzahl	INT
ambulantDermatologeWunde	CHAR(1) [J,N]
ambulantKardiologe	CHAR(1) [J,N]
ambulantKardiologeAnzahl	INT
ambulantKardiologeWunde	CHAR(1) [J,N]
ambulantAngiologe	CHAR(1) [J,N]
ambulantAngiologeAnzahl	INT
ambulantAngiologeWunde	CHAR(1) [J,N]
ambulantPhlebologe	CHAR(1) [J,N]
ambulantPhlebologeAnzahl	INT
ambulantPhlebologeWunde	CHAR(1) [J,N]
ambulantKkhWunde	CHAR(1) [J,N]
ambulantKkhWundeAnzahl	INT
ambulantKkhAnderer	CHAR(1) [J,N]
ambulantKkhAndererAnzahl	INT
stationaerKkhWunde	CHAR(1) [J,N]
stationaerKkhWundeAnzahl	INT
stationaerKkhWundeTage	INT
stationaerKkhAnderer	CHAR(1) [J,N]
stationaerKkhAndererAnzahl	INT
stationaerKkhAndererTage	INT
operation	CHAR(1) [J,N]
psychotherapie	CHAR(1) [J,N]
psychotherapieAnzahl	INT
wohnen	CHAR(1) [J,N]
wohnenPrivatPflegedienst	CHAR(1) [J,N]
wohnenPrivatPflegedienstAnzahl	INT

wohnenPrivatPflagedienstStunden	INT
wohnenPrivatKurzzeitpflege	CHAR(1) [J,N]
wohnenPrivatTagespflege	CHAR(1) [J,N]
pflegeversicherung	CHAR(1) [J,N]
pflegeversicherungGrad	INT
pflegeversicherungGeld	INT
behandlungsmittel	CHAR(1) [J,N]
behandlungsmittelChirurg	CHAR(1) [J,N]
behandlungsmittelDermatologe	CHAR(1) [J,N]
behandlungsmittelAngiologe	CHAR(1) [J,N]
behandlungsmittelPhlebologe	CHAR(1) [J,N]
behandlungsmittelAndere	CHAR(1) [J,N]
heilmittelKrankengymnastik	CHAR(1) [J,N]
heilmittelKrankengymnastikAnzahl	INT
heilmittelLymphdrainage	CHAR(1) [J,N]
heilmittelLymphdrainageAnzahl	INT
heilmittelErgotherapie	CHAR(1) [J,N]
heilmittelErgotherapieAnzahl	INT
heilmittelMedizinischeFusspflege	CHAR(1) [J,N]
heilmittelMedizinischeFusspflegeAnzahl	INT
heilmittelHeilpraktiker	CHAR(1) [J,N]
heilmittelHeilpraktikerAnzahl	INT
hilfe	CHAR(1) [J,N]
hilfeTaeglich	CHAR(1) [J,N]
hilfeAnzahl	INT
hilfeStunden	INT
hilfeMinuten	INT

haushaltshilfe		CHAR(1) [J,N]
haushaltshilfeTaeglich		CHAR(1) [J,N]
haushaltshilfeAnzahl		INT
haushaltshilfeStunden		INT
haushaltshilfeMinuten		INT
anreiseFuss		CHAR(1) [J,N]
anreiseFahrrad		CHAR(1) [J,N]
anreisePkw		CHAR(1) [J,N]
anreiseOeffentliche		CHAR(1) [J,N]
anreiseTaxi		CHAR(1) [J,N]
anreiseMinuten		INT
anreiseKilometer		INT
anreiseKosten		INT
berufstaetig		CHAR(1) [J,N]
berufstaetigAnzahl		INT
berufstaetigReduziert		CHAR(1) [J,N]
berufstaetigReduziertAnzahl		INT
berufstaetigKrankgeschriebenWunde		CHAR(1) [J,N]
berufstaetigKrankgeschriebenWundeAnzahl		INT
berufstaetigKrankgeschriebenAndere		CHAR(1) [J,N]
berufstaetigKrankgeschriebenAndereAnzahl		INT
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

## Phq9

Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
----------	-----------	----------------------------------

id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
interesse		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
schwermut		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
schlaf		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
energie		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
appetit		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
meinung		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
schwierigkeiten		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
bewegung		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
gedanken		CHAR(1) [N:Nicht, T:Tagen, H:Hälfte, B:Beinahe]
ergebnis		INT
ergebnisText		CHAR(200)
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME

#### Eq5d

Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
----------	-----------	----------------------------------

id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
datum	Durchführungsdatum	DATE, YYYY-MM-DD
beweglichkeit		CHAR(1) [0:Nicht, 1:Wenig, 2:Mäßig, 3:Sehr, 4:Extrem]
selbstsorgen		CHAR(1) [0:Nicht, 1:Wenig, 2:Mäßig, 3:Sehr, 4:Extrem]
allgemein		CHAR(1) [0:Nicht, 1:Wenig, 2:Mäßig, 3:Sehr, 4:Extrem]
schmerzen		CHAR(1) [0:Nicht, 1:Wenig, 2:Mäßig, 3:Sehr, 4:Extrem]
angst		CHAR(1) [0:Nicht, 1:Wenig, 2:Mäßig, 3:Sehr, 4:Extrem]
zustand		INT [0-100]
ergebnisText		CHAR(500)
komplett		CHAR(1) [J,N]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Kompression</b>		
<b>Feldname</b>	<b>Bemerkung</b>	<b>Datentyp, Format [Gültige Werte]</b>
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT



u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
kompression		CHAR(1) [J,N]
klasse		CHAR(1) [2:2-lagig, 4:4-lagig, A:MAK, U:Ulcusstrumpf, M:Med. Kompressionsstrumpf, S:Anderes]
klasseAnderes		CHAR(200)
klasseAnderesBegrueundungText		CHAR(200)
beinLinks		CHAR(1) [J,N]
beinRechts		CHAR(1) [J,N]
taeglichNeu		CHAR(1) [J,N]
kompressionsmittelNeuAnzahl		INT
kompressionsmittelNachts		CHAR(1) [J,N]
kompressionsmittelAnlegender		CHAR(1) [P:Praxis, D:Pflegedienst, S:Selbst, A:Angehörige]
zufriedenheit		CHAR(1) [J,N]
zufriedenheitNeinText		CHAR(200)
entstaut		CHAR(1) [J,N]
beinumfangFuss		FLOAT
beinumfangKnoechel		FLOAT
beinumfangWade		FLOAT
ruheschmerzen		CHAR(1) [J,N]
taubheitsgefuehl		CHAR(1) [J,N]
durchblutungsstoerungen		CHAR(1) [J,N]
druckstellen		CHAR(1) [J,N]

druckstellenLaenge		FLOAT
druckstellenBreite		FLOAT
druckstellenFlaeche		FLOAT
druckstellenGrad		CHAR(1) [1:Rötung, 2:Epidermale, 3:Alle, 4:Nekrose]
druckstellenLokalisation		CHAR(200)
kompressionNeinText		CHAR(200)
kompressionNeinAlternative		CHAR(1) [J,N]
kompressionNeinAlternativeKlasse		CHAR(1) [U:Ulcusstrumpf, K:Kompr.strumpf, S:Anderes]
kompressionNeinAlternativeKlasseAnderes		CHAR(200)
kompressionNeinAlternativeNeinText		CHAR(200)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Wunde</b>		
Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
abgeheilt		CHAR(1) [J,N]
abgeheiltDatum		DATE, YYYY-MM-DD
bezeichnung		CHAR(200)

wundenMatrix	Wundenfelder	CHAR(5000)
seitMonaten		INT [0-60]
schmerzenRuhe		INT [0-10]
schmerzenAlltag		INT [0-10]
schmerzenSpazieren		INT [0-10]
wundLaenge		FLOAT
wundBreite		FLOAT
wundFlaeche		FLOAT
wundbodenGranulation		CHAR(1) [0:Nicht, 1:Wenig, 3:Mäßig, 6:Mehrheitlich, 8:Ganze]
wundbodenFibrin		CHAR(1) [0:Nicht, 1:Wenig, 3:Mäßig, 6:Mehrheitlich, 8:Ganze]
wundbodenAvital		CHAR(1) [0:Nicht, 1:Wenig, 3:Mäßig, 6:Mehrheitlich, 8:Ganze]
wundbodenStrukturMuskel		CHAR(1) [J,N]
wundbodenStrukturKnochen		CHAR(1) [J,N]
wundbodenStrukturSehne		CHAR(1) [J,N]
wundrandReizlos		CHAR(1) [J,N]
wundrandMazeriert		CHAR(1) [J,N]
wundrandLivide		CHAR(1) [J,N]
wundrandNekrotisch		CHAR(1) [J,N]
wundrandSchuppend		CHAR(1) [J,N]
wundumgebungReizlos		CHAR(1) [J,N]
wundumgebungMazeriert		CHAR(1) [J,N]
wundumgebungLivide		CHAR(1) [J,N]
wundumgebungNekrotisch		CHAR(1) [J,N]
wundumgebungSchuppend		CHAR(1) [J,N]

sekretion		CHAR(1) [0:Keine, 1:Wenig, 2:Mäßig, 3:Stark]
sekretionQualitaet		CHAR(1) [0:Nicht, 1:1-50, 5:51-100, X:Gelöst]
wundauflageBelegt		CHAR(1) [K:Serös, S:Blutig-serös, B:Blutig, F:Fibrinös, E:Eitrig]
wundgeruch		CHAR(1) [J,N]
wundinfekt		CHAR(1) [J,N, V:Verdacht]
abstrich		CHAR(1) [J,N]
abstrich1Keim		CHAR(200)
abstrich1Ergebnis		CHAR(200)
abstrich1Wachstum		CHAR(1) [0:Gering, 1:Mäßig, 2:Stark, 3:Massenhaft]
abstrich2Keim		CHAR(200)
abstrich2Ergebnis		CHAR(200)
abstrich2Wachstum		CHAR(1) [0:Gering, 1:Mäßig, 2:Stark, 3:Massenhaft]
abstrich3Keim		CHAR(200)
abstrich3Ergebnis		CHAR(200)
abstrich3Wachstum		CHAR(1) [0:Gering, 1:Mäßig, 2:Stark, 3:Massenhaft]
bild1		CHAR(1) [J]
bild2		CHAR(1) [J]
bild3		CHAR(1) [J]
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
Therapieplan Feldname	Bemerkung	Datentyp, Format [Gültige Werte]

id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
u_wunde_id	referenziert auf das Feld id der Tabelle Wunde	INT
verbandswechsel		CHAR(1) [Z:Zweimal, 1:1, 2:2, 3:3, 4:4, 5:5, 7:7]
verbandswechselDurchfuehrender		CHAR(1) [P:Praxis, D:Pflegedienst, A:Patient/Angehörige]
wundspuelloesung		CHAR(1) [N:NaCl, H:Hypochlorsäure, O:Octenidindihydrochlorid, P:Polyhexanid, S:Sonstige]
wundspuelloesungSonstigText		CHAR(200)
spuelmenge		INT
wundreinigungText		CHAR(2000)
wundauflageBezeichnung		CHAR(200)
wundauflageLaenge		FLOAT
wundauflageBreite		FLOAT
wundauflageFlaeche		FLOAT
wundauflageTyp		CHAR(2) [KO:Kompressen, GA:Gaze, SA:Saugkompressen, AK:Aktivkohlekompressen, AL:Alginate, HY:Hydrofaser, HG:Hydrogel, HK:Hydrokolloide, SS:Schaumstoff, SI:Silberhaltige, SU:Superabsorber]

wundauflageSekundaer		CHAR(1) [J,N]
wundauflageSekundaerText		CHAR(200)
lokalbehandlung		CHAR(1) [J,N]
lokalbehandlungText		CHAR(2000)
antibiotisch		CHAR(1) [J,N]
antibiotischDatum		DATE, YYYY-MM-DD
antibiotischEndeDatum		DATE, YYYY-MM-DD
antibiotischUeberlaengeText		CHAR(200)
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME
<b>Praeparat</b>		
Feldname	Bemerkung	Datentyp, Format [Gültige Werte]
id	Autoinkrementelle, interne ID	INT
u_patient_id	referenziert auf das Feld id der Tabelle Patient	INT
u_assessment_id	referenziert auf das Feld id der Tabelle Assessment	INT
u_monitoring_id	referenziert auf das Feld id der Tabelle Monitoring	INT
u_wunde_id	referenziert auf das Feld id der Tabelle Wunde	INT
u_therapieplan_id	referenziert auf das Feld id der Tabelle Therapieplan	INT
name		CHAR(200)
dosis		FLOAT
einnahmeschema1	Morgens	INT
einnahmeschema2	Mittags	INT

einnahmeschema3	Abends	INT
einnahmeschema4	Nachts	INT
created	Zeitstempel der Erstellung des Datensatzes	DATETIME
lastmodified	Zeitstempel der letzten Änderung	DATETIME