Projektspezifisches

DATENSCHUTZKONZEPT

STATAMED

Kurzstationäre Allgemeinmedizin

Gefördert durch den Innovationsfonds des G-BA
Förderkennzeichen 01NVF22103

Version vom 10.04.2024

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

0. Präambel

Die neue Versorgungsform "STATAMED“ – Transformation des Patientenpfades durch ein sektorenübergreifendes kurzstationäres allgemeinmedizinisch-orientiertes Versorgungmodell" wird durch den Innovationsausschuss beim Gemeinsamen Bundesausschuss (G-BA) vom 01.07.2024 bis 31.03.2027 gefördert (Förderkennzeichen: 04NVF22103) [1].

Bei der Umsetzung von Forschungsprojekten im medizinischen Kontext werden sensible Daten verarbeitet. Auch für die Durchführung des Projekts STATAMED sind gesundheitsbezogene personenbezogene Daten unerlässlich. Um den Schutz dieser hochsensiblen Daten und die Einhaltung der Datenschutzgrundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) für das Projektvorhaben gewährleisten und nachweislich einhalten zu können, beschäftigt sich dieses Datenschutzkonzept mit dem Schutz, der Sicherung und dem Datentransfer der pseudonymisierten und personenbezogenen Daten im STATAMED-Projekt. Dabei werden gezielt die Aspekte Integrität, Vertraulichkeit und Verfügbarkeit der Daten berücksichtigt, und es werden Sicherheitsmaßnahmen als Mindestanforderungen formuliert.

Die neue Versorgungsform wird sektorenübergreifend an sechs Standorten in Nordrhein-Westfalen, Hamburg und Niedersachsen ab dem 01. April 2024 umgesetzt und umfassend evaluiert.

Bei diesem Datenschutzkonzept handelt es sich um eine vorläufige Version.

1. Darstellung des Forschungsvorhabens

1.1. Allgemeine Kurzbeschreibung

Im Zuge des STATAMED-Projekts wird eine sektorenübergreifende, kurzstationäre und allgemeinmedizinische Versorgung für Menschen mit (sub-)akuten gesundheitlichen Beschwerden und ärztlichem Hilfebedarf etabliert. Damit sollen vor allem unnötige Einsätze des Rettungsdienstes mit anschließender Behandlung in einer Notfallambulanz und gegebenenfalls längeren stationären Aufenthalten vermieden werden. Stattdessen wird eine gezielte, sorgsam geplante kurzstationäre Behandlung in einer STATAMED-Einrichtung geboten, eine möglichst zügige Entlassung und bedarfsorientierte Nachbetreuung in gewohntem Umfeld.

Das neue Versorgungsform STATAMED soll den ambulanten und stationären Bereich sinnvoll verbinden und regionale, berufsgruppenübergreifende Gesundheitsnetzwerke unter Einbeziehung von Ärztinnen und Ärzten, Patientenlotsen und „Flying Nurses“ für das neue Versorgungsangebot an zunächst sechs Standorten aufbauen, die durch das Projekt neue Perspektiven für die stationäre Versorgung gewinnen.

1.2. Zielsetzung des STATAMED-Forschungsprojekt

Ziel ist es, die Wirkung und Wirksamkeit auf Populations- und Organisationsebene wissenschaftlich zu evaluieren. Zudem findet eine wissenschaftliche Projektbegleitung zur weiteren Optimierung der Versorgungspraxis sowie für die Entwicklung von nachhaltigen Vergütungsmodellen statt. Das STATAMED-Forschungsprojekt umfasst mehrere Teilstudien.

1.3. Evaluierende Institute

Folgende Institutionen sind verantwortlich für die unabhängige Evaluation und wissenschaftliche Projektbegleitung für die STATAMED-Teilstudien:

Unabhängige Evaluation:

- Hamburg Center for Health Economics (HCHE), Universität Hamburg: Summative Evaluation, formative Evaluation, gesundheitsökonomische Evaluation und SEIA

- Medizinische Hochschule Hannover (MHH) – Institut für Allgemeinmedizin und Palliativmedizin: Formative Evaluation und qualitative Prozessevaluation

Wissenschaftliche Projektbegleitung:

- Universitätsklinikum Hamburg-Eppendorf (UKE): Qualitätssicherung und Operationalisierung des kontinuierlichen Verbesserungsprozesses
- Institute for Health Care Business GmbH (hcb): Wirtschaftliche Bewertung und Beurteilung der Rahmenbedingungen für eine erfolgreiche Überführung in die Regelversorgung

1.4. Zielparameter, Studiendesign und Methodik

Der primäre kombinierte Zielparameter für die Wirksamkeitsuntersuchung ist:

- die Rehospitalisierungsrate innerhalb von 30 Tagen nach Entlassung aus einer STATAMED-Klinik und
- die durchschnittliche stationäre Verweildauer für eine initiale Hospitalisierung von behandlungsbedürftigen Menschen (welche die Einschlusskriterien erfüllen) im Vergleich zur bisherigen Regelversorgung.

Weitere zu untersuchende sekundäre Zielparameter ergeben sich aus einer Reihe von unterschiedlichen wissenschaftlichen Fragestellungen. Sie sollen im Versorgungsalltag bewertet werden und sind für den Gesamterfolg von STATAMED und damit auch für eine etwaige Aufnahme in die Regelversorgung bedeutsam. Diese umfassen im Einzelnen folgende Aspekte:

- Verringerung der Inanspruchnahme der ambulanten Notfallversorgung und des Rettungsdienstes
- Verbesserung der allgemeinen krankheitsübergreifenden Lebensqualität der betroffenen Patientinnen und Patienten
- Höhere Patientenzufriedenheit
- Fähigkeiten der Betroffenen zu einem verbesserten Gesundheitsmanagement
- Verbesserung der Arbeitszufriedenheit der am Behandlungsprozess beteiligten Leistungserbringer im sektorenübergreifenden Gesundheitsnetzwerk
- Kosteneffektivität von STATAMED im Vergleich zur bestehenden Regelversorgung

- Feststellen potenzieller Faktoren, die das Implementieren der neuen Versorgungsform beeinflussen könnten
- Gewinnen von Erkenntnissen und Bewertung von sozioökonomischen Faktoren (auf Politik-, Versorgungs-, Individual-/Organisationsebene) zur Unterstützung des angestrebten Übergangs von STATAMED vom Projekt in die Regelversorgung
- Wissenschaftliche Projektbegleitung im kontinuierlichen Verbesserungsprozess zur Qualitätssicherung und -optimierung von STATAMED
- Konzeptionelle Weiterentwicklung im Hinblick auf Leistungsspektrum, Standortkonzeption, Ausstattung und Mindestgröße für die kurzstationäre allgemeinmedizinische Behandlung
- Wirtschaftliche Bewertung und Untersuchung regulatorischer Fragestellungen zur Finanzierung und Vergütung von STATAMED

Für die Untersuchung zum kombinierten primären Zielparameter wird eine prospektive, cluster-randomisierte, kontrollierte Studie (C-RCT) im Stepped-Wedge-Design angewendet. Das Einzugsgebiet der Zielregionen wird in separate Gebiete (Cluster) aufgeteilt.

Jedes Cluster fängt in einer Kontrollgruppe an, das heißt, die Behandlung erfolgt entsprechend der Regelversorgung und wird randomisiert zeitversetzt der Interventionsgruppe zugeordnet. Die stufenweise Einführung der neuen Versorgungsform STATAMED erlaubt die Erfassung und den Vergleich von zeitlichen Effekten sowie eine Prozessevaluation. Die Cluster werden regional aus unterschiedlichen Zuweisenden (hausärztliche und fachärztliche Praxen, Rettungsdienste, ambulante Pflegedienste und stationäre Pflegeeinrichtungen) über die sechs Standorte gebildet.

Für die Untersuchung der sekundären Fragestellungen werden unterschiedlichen Methoden angewendet.

Zur Analyse der Kosteneffektivität der neuen Versorgungsform wird eine gesundheitsökonomische Evaluation durchgeführt. Sie erfolgt anhand einer Kosten-Effektivitäts-Analyse aus Perspektive der gesetzlichen Krankenkasse. Die wissenschaftliche Begleitung der Intervention über die Dauer der geplanten C-RCT (s. oben) hinweg erfolgt über eine formative und qualitative Prozessevaluation – mithilfe von Fragebogenbefragungen (quantitativ) und Einzelinterviews sowie Fokusgruppen (qualitativ) mit am Projekt beteiligten Leistungserbringern, mit teilnehmenden Patientinnen und Patienten sowie Angehörigen.

Zur Unterstützung der Nachhaltigkeitsplanung für den Transfer des neuen Versorgungskonzeptes in die Regelversorgung wird zudem ein Sozioökonomisches Impact Assessment (SEIA) durchgeführt.

Im Rahmen der wissenschaftlichen Projektbegleitung werden Strukturen, Prozesse und Ergebnisse mittels Qualitätszirkeln an den Standorten im Sinne der kontinuierlichen Verbesserung überprüft, analysiert, gemessen und weiterentwickelt. Für die wirtschaftliche Bewertung wird eine Kostenarten-, Kostenstellen- und Kostenträgerrechnung und Simulation der Wirtschaftlichkeit bei alternativen Vergütungsansätzen angewendet.

1.5. Beteiligte Konsortial-, Kooperations- und Projektpartner

Folgende Institutionen, sind an der Projektumsetzung als Konsortialpartner und Projektpartner beteiligt:

Tabelle 1: Übersicht der beteiligten Organisationen

Name der Organisationen	Abkürzungen	Verantwortlichkeit /Rolle
AOK Rheinland/Hamburg	AOK RH	**Konsortialführung:** Projektmanagement, Vertragsgestaltung, Bereitstellung der GKV-Routinedaten
AOK Niedersachsen	AOK NDS	**Konsortialpartner:** Standort-Management NDS, Vertragsgestaltung, Bereitstellung der GKV-Routinedaten
Institute for Health Care Business GmbH	hcb	**Konsortialpartner:** Wissenschaftliche Projektbegleitung: Wirtschaftliche Bewertung der Intervention, Erarbeitung eines Vergütungsmodells und Rahmenbedingungen für die Überführung in die Regelversorgung
Hamburg Center for Health Economics (HCHE), Universität Hamburg	HCHE	**Konsortialpartner:** Externe Evaluation: Summative Evaluation, Formative Evaluation, Gesundheitsökonomische Evaluation, SEIA
Medizinische Hochschule Hannover, Institut für Allgemeinmedizin und Palliativmedizin	MHHJ	**Konsortialpartner:** Externe Evaluation: Formative Evaluation, Qualitative Prozessevaluation
Universitätsklinikum Hamburg-Eppendorf	UKE	**Konsortialpartner:** Standard Operating Procedures, Wissenschaftliche Projektbegleitung: Qualitätssicherung und Operationalisierung

Name der Organisationen	Abkürzungen	Verantwortlichkeit /Rolle
		des kontinuierlichen Verbesserungsprozesses
Stadtteilklinik Hamburg	Klinikstandort SKH	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
Wilhelmsburger Krankenhaus Groß-Sand	Klinikstandort Groß-Sand	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
Klinik Sulingen Landkreis Diepholz	Klinikstandort Sulingen	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
BürgerGesundheitsPark Bad Gandersheim	Klinikstandort Bad Gandersheim	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
Ubbo-Emmius Klinik Norden	Klinikstandort Norden	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
Gesundheitszentrum St. Vincenz gGmbH“, Essen-Stoppenberg	Klinikstandort Essen	**Konsortialpartner:** Interventionsstandort, Bereitstellung der 21er Krankenhausdaten (§ 21 KHEntg) und klinikinternen Statistiken
gevko GmbH, Bonn	gevko	**Projektpartner:** HealthPortal, Registrierungstool, Bereitstellung der Daten der Studiendokumentation aus dem HealthPortal
Kassenärztliche Vereinigung Nordrhein	KV NO	**Kooperationspartner:** Versorgungsvertrag, Bereitstellung der KV-Statistik
Abrechnungsdienstleister N.N.		**Projektpartner externer Dienstleister**
Vertrauensstelle N.N.		**Projektpartner externer Dienstleister**

Weitere Kooperationspartner (Stadt Essen, Ärztenetz Billstedt-Horn e.V.) wirken am STATAMED-Projekt mit und unterstützen in der Umsetzung.

1.6. Ethikantrag

Folgende Ethikanträge wurden erstellt und von den zuständigen Ethikkommissionen für die STATAMED-Teilstudien begutachtet:

Tabelle 2: Übersicht der Ethikvoten der Teilstudien

Teilstudie	Konsortialpartner	Ethikkommission	Ethikvotum

Mit der Studienumsetzung wird erst bei Vorliegen eines positiven Ethikvotums der genannten Institutionen begonnen.

1.7. Finanzierung

Das Projektvorhaben wird aus Mitteln des Innovationsfonds des GBA zur Förderung von neuen Versorgungsformen (§ 92a Absatz 1 Satz SGB V) finanziert. Der offizielle Förderbescheid mit dem Förderkennzeichen 01NVF22103

1.8. Rechtsgrundlage

Als Rechtsgrundlage für die neue Versorgungsform der teilnehmenden STATMED-Krankenkassen dient der Versorgungsvertrag der „Besonderen Versorgung“ nach § 140a SGB V. Gesetzliche Krankenkassen, die nicht dem Versorgungsvertrag nach § 140a SGB V beitreten, gilt für ihre Versicherten der Behandlungsvertrag nach § 630a BGB. Für die Forschung gelten des Weiteren § 92a und b SGB V in Verbindung mit § 67b SGB X sowie Artikel 6 Abs. 1a DSGVO, Artikel 9 DSGVO und 67c Abs. 5 SGB X in Verbindung mit § 75 SGB X.

1.9. Projektabschluss und Fortführung nach Ende

Die umfangreichen Arbeiten am Indikationsprofil, den Qualifikationsanforderungen der Leistungserbringenden und die einfach vorzuhaltende apparative Mindestausstattung des STATAMED-Konzepts ermöglichen eine Übertragbarkeit auf eine Vielzahl von Regionen und Versorgungssettings. Langfristig kann dieses Modell in der Fläche dazu führen, dass kleine Kreiskrankenhäuser durch STATAMED in der Regelversorgung abgelöst

werden. Insbesondere wenn in strukturschwachen Regionen Kommunen ein strukturpolitisches Interesse an dem „Erhalt“ des regionalen Krankenhauses haben, müsste dieses nicht komplett geschlossen, sondern das medizinische Angebot verändert und regional neu eingebunden werden. Das erhöht auch die Akzeptanz in der Bevölkerung.

2. Beschreibung der Datenverarbeitung

2.1. Datenschutzmanagement

Die Verantwortliche sind nach EU-DSGVO (unter anderem Art. 5 und Art. 25 EU-DSGVO) verpflichtet, im Rahmen des STATAMED-Projekts ein System zum Datenschutzmanagement einzuführen. Das Datenschutz-Managementsystem beinhaltet die Gesamtheit der Datenschutzinstrumente und -prozesse.

Die Projektbeteiligten und ihre jeweilige Verantwortlichkeit im STATAMED-Projekt wurden bereits kurz eingeführt (Abschnitt 1.5). Im Folgenden werden die Akteure im Zusammenhang mit ihrer jeweiligen zentralen Aufgabe bei der Datenverarbeitung und dem Datenaustausch beschrieben.

Tabelle 3: Aufgaben der Datenverarbeitung

Akteure	Aufgaben	Standort	Datenart
Klinikstandorte	Aufklärung, Rekrutierung, Versorgung, Primärdatenerhebung	SKH Hamburg, Wilhelmsburger Krankenhaus Groß Sand, Ubbo-Emmius Klinik Norden, Klinik Sulingen Landkreis Diepholz Sulingen, Bürger-GesundheitsPark Bad Gandersheim, Gesundheitszentrum St. Vincenz gGmbH, Essen-Stoppenberg	Personenbezogen: Erhebung der Einwilligungsdaten, Primärdateneingabe von Leistungs- und Versorgungsdaten (HealthPortal) Pseudonymisiert: Extraktion der Krankenhausdaten (§ 21 KHEntg) Anonymisiert/Pseudonymsiert: Extraktion der standortbezogene Finanz-, Personal- und Leistungsdaten

Akteure	Aufgaben	Standort	Datenart
Krankenkasse, AOK RH	Bereitstellung spezifischer GKV-Routinedaten im Rahmen der Besonderen Versorgung nach § 140a SGB-V gemäß Zustimmung nach § 75 SGB X, Pseudonymisierung (Kassenpseudonym, FORM-ID der KG) Projektcontrolling	AOK Rheinland/Hamburg, Düsseldorf	Pseudonymisiert: Extraktion der GKV-Routinedaten Personenbezogen: Kontaktdaten der teilnehmenden Zuweiser zur Projektdokumentation im Rahmen der Aufgaben als Konsortialführung Abrechnungsstatistik der KV-NO und Abrechnungsdienstleister zur Projektdokumentation im Rahmen der Aufgaben als Konsortialführung
Krankenkasse, AOK NDS	Bereitstellung spezifischer GKV-Routinedaten im Rahmen der Besonderen Versorgung nach § 140a SGB-V gemäß Zustimmung nach § 75 SGB X, Pseudonymisierung (Kassenpseudonym, FORM-ID der KG)	AOK Niedersachsen, Hannover	Pseudonymisiert: Extraktion der GKV-Routinedaten
gevko	Entwicklung HealthPortal, Entwicklung Registrierungstool, Pseudonymisierung (Studien-ID,FORM-ID der IG)	gevko GmbH	Personenbezogen: Verarbeitung der Einwilligungsunterlagen der Patientinnen und Patienten, Verarbeitung der Kontaktdaten der zuweisenden Leistungserbringer, Verarbeitung der Studiendaten der Leistungs- und Versorgungsdaten

Akteure	Aufgaben	Standort	Datenart
Abrechnung, N.N., KV-NO		N.N., KV-Nordrhein	Personenbezogen: Verarbeitung der Abrechnungsdaten der teilnehmenden niedergelassenen Ärzte
Unabhängige Evaluation, HCHE		HCHE, Universität Hamburg	
Unabhängige Evaluation, MHH		MHH, Medizinische Hochschule Hannover	
Wissenschaftliche Projektbegleitung, UKE		UKE, Uniklinik Eppendorf	
Wissenschaftliche Projektbegleitung, hcb		hcb, Essen	
Vertrauensstelle, N.N.	Datenannahme, Qualitätskontrolle, Entgegennahme und Aufbewahrung der Schlüssellisten (Zuordnungslisten) Datenlinkage, Datenweiterleitung	N.N.	Personenbezogen: Studiendaten aus dem HealthPortal, Datenexporte der Kontaktdaten der teilnehmenden Zuweiser aus dem Registrierungstool, Abrechnungs-/KV-Statistik Pseudonymisiert: GKV-Routinedaten, Krankenhausdaten (§ 21 KHEntg) Standortbezogene Finanz-, Personal- und Leistungsdaten Schlüssellisten: Zuordnungslisten zur Pseudonymisierung der Daten für den Datentransfer an die Evaluation

2.2. Vertrauensstelle

Die Vertrauensstelle ist eine unabhängige Treuhandstelle, welche institutionell, räumlich, personell getrennt ist. Sie fungiert als Schnittstelle zwischen Datengeber/-erheber und Datenempfänger. Die Vertrauensstelle umfasst das Trust Center mit Datenmanagementstelle, eingerichtet an externer Dienstleister.

Die wesentlichen Aufgaben und Verantwortlichkeiten der Vertrauensstelle sind:

- Datenschutzrechtlich angemessene Lösung und treuhänderische Verwahrung der Schlüssellisten für die Zuordnung der Pseudonyme
- Speicherung und Übergabe des Teilnahmeverzeichnisses der Kontrollgruppe (Form-ID-Teilnahmeverzeichnis) für die GKV-Routinedatenlieferung
- Datenannahme der pseudonymisierten GKV-Routinedaten
- Datenannahme der Datenexporte über das Dokumentationssystem des Health-Portals. Die Daten des digitalen Einschreibe- und Teilnahmeprozess sind davon ausgeschlossen.
- Datenannahme der Datenexporte des Registrierungstools der Zuweiserkontaktdaten
- Datenannahme der Krankenhausdaten des 21er Datensatzes (§ 21 KHEntgG)
- Datenannahme der KV-Statistiken bzw. Abrechnungsstatistik
- Datenannahme der Schlüssellisten
- Datenannahme der standortbezogenen Finanz-, Personaleinsatz- und Leistungsdaten
- Pseudonymisierung und Datenlinkage der Studiendaten (personen- bzw. institutionsidentifizierende Merkmale werden mit einem Pseudonym versehen)
- Weiterleitung der pseudonymisierten Daten an die externe Evalation HCHE, MHH und wissenschaftliche Projektbegleitung UKE, hcb.
- Weiterleitung der Zuweiserkontaktdaten an die HCHE, MHH.

Nach Abschluss der STATAMED-Teilstudien werden die Schlüssellisten (Zuordnungsschlüssel) datenschutzkonform vernichtet bzw. gelöscht.

2.3. Health-Plattform

Allgemeine Beschreibung des HealthPortals

Das HealthPortal, entwickelt von der gevko GmbH – einem auf IT-Lösungen im Gesundheitswesen spezialisierten Tochterunternehmen der AOK – ist eine benutzerfreundliche Webanwendung, die über gängige Web-Browser wie Chrome, Edge und Firefox genutzt werden kann. Es dient der Kommunikation zwischen den Vertragspartnern unter Nutzung der Telematik-Infrastruktur. Die Nutzer sind das STATAMED-Klinikpersonal an den sechs Klinikstandorten, darunter die ärztliche STATAMED-Leitung, Flying Nurse, Patientenlotsen, diensthabende Ärztinnen/Ärzte und Pflegekräfte. Im Rahmen des STATAMED Projekts werden die folgenden Funktionen des HealthPortals genutzt:

i. Digitaler Einschreibe- und Teilnahmeprozess (Behandlungsvertrag) für die STATAMED-Klinikstandorte und für die Versicherten, mit nahtloser Integration in die Krankenkassen-Software der teilnehmenden Krankenkassen AOK Rheinland/Hamburg und AOK Niedersachsen.
ii. Elektronische, strukturierte Versorgungs- und Leistungsdokumentation während der Interventionsphase für Studienzwecke durch das STATAMED-Klinikpersonal.
iii. Export der pseudonymisierten Daten der Dokumentationsbögen aus dem Dokumentationssystem für die Evaluatoren.
iv. Bereitstellung von Evaluationsfragebögen mit pseudonymisierter Form-ID (Evaluations-ID für den Behandlungsfall) für die Versicherten nach Abschluss der Behandlung. Die Funktion soll den Patientenlotsen bei der Studienkoordination unterstützen.

Funktionalität des HealthPortals

Die STATAMED-Kliniken wird durch das HealthPortal mit einem vollständig digitalen Registrierungsverfahren unterstützt. Nach erfolgreicher Registrierung der STATATMED-Standorte im HealthPortal wird die Teilnahmeerklärung elektronisch automatisch an die AOK Rheinland/Hamburg oder AOK Niedersachsen übermittelt und dort im Backendsystem hinterlegt. Der Teilnahmestatus wird dann über ein Teilnehmerverzeichnis für Leistungserbringer an das HealthPortal zurückübermittelt.

Die zugewiesenen Patientinnen und Patienten werden von der ärztlichen STATAMED-Leitung im HealthPortal erfasst. Neben der manuellen Anlage und Bearbeitung der Patientenstammdaten besteht die Möglichkeit, diese optional über die elektronische Gesundheitskarte einzulesen. In den Patientenstammdaten können Zusatzparameter wie DMP-

Kennzeichen, interne AIS-ID, E-Mail, Telefon, Mobilfunknummer und Zuzahlungsstatus erfasst werden. Anschließend können die Patientinnen und Patienten, abhängig von ihrer gesetzlichen Krankenversicherung nach § 140a SGB V oder nach § 630a BGB, elektronisch in den Versorgungsvertrag eingeschrieben werden. Die Teilnahmeerklärung nach § 140a SGB V wird digital an die AOK Rheinland/Hamburg oder AOK Niedersachsen übermittelt und automatisch im Backendsystem hinterlegt. Nach einer automatischen Prüfung im Backendsystem wird der Teilnahmestatus der Patientinnen und Patienten im Vertrag digital an das HealthPortal zurückübermittelt, wo die ärztliche STATAMED-Leitung ihn einsehen kann. Für die Teilnahmeerklärung nach § 630a BGB wird eine Teilnahmestatistik (Anzahl der Versicherten der gesetzlichen Krankenversicherungen, Information zum Zuweiser, gruppiert nach STATAMED-Klinikstandort) generiert und digital an die AOK Rheinland/Hamburg verschlüsselt übermittelt. Die Teilnahmestatistik wird ausschließlich für Zwecke der Abrechnungsprüfung mit den teilnehmenden kassenärztlichen Vereinigungen und zur Projektdokumentation im Rahmen des STATAMED-Innovationsfondsprojektes verwendet.

Das HealthPortal (Dokumentationssystem) stellt den Nutzern der STATAMED-Klinikstandorte eine digitale Patientenkarteikarte zur Verfügung. Alle Dokumentationen werden in der Karteikarte angezeigt und können nach verschiedenen Kriterien gefiltert werden. Es besteht auch die Möglichkeit, alle Aktivitäten über einen Schnellzugriff zu erfassen. Alle im Rahmen der STATAMED-Evaluation zu erfassenden Dokumente werden digital im HealthPortal bereitgestellt. Die Stammdaten der Patienten werden automatisch vom HealthPortal übernommen. Weitere Felder der Dokumente können einfach und schnell von den STATAMED-Klinikpersonal elektronisch erfasst werden. Die erfassten Daten werden strukturiert in einer Datenbank des HealthPortals abgelegt. Weder die Evaluatoren noch die Krankenkassen haben Zugriff auf das HealthPortal. Die entsprechenden Daten werden pseudonymisiert und verschlüsselt über die Vertrauensstelle den Evaluatoren zur Verfügung gestellt. Zusätzlich stellt das HealthPortal den STATAMED-Patientenlotsen die Funktion die digitalen abschließenden Fragebögen für die behandelten Patientinnen und Patienten zum Ausdruck bereit. Auf diese Weise wird die Studienkoordination an den STATAMED-Klinikstandorte unterstützt.

Das HealthPortal wird auf einem Server im DSGVO-konformen Rechenzentrum der colt GmbH gehostet. Aus Sicherheitsgründen werden verschiedene Studien-IDs pro eingeschriebenem STATAMED-Patienten vergeben. Die Verarbeitung der pseudonymisierten

Daten erfolgt gemäß den Vorschriften der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) und deren Umsetzung im Bundesdatenschutzgesetz (BDSG). Das Health-Portal dient ausschließlich als Kommunikations- und Dokumentationsplattform und gibt keine Empfehlungen zur Behandlungsoptimierung ab. Es erfolgt keine medizinische Versorgung über das HealthPortal.

Infrastruktur des HealthPortals

Das HealthPortal implementiert das im Projekt definierte Datenschutz- und Datenübertragungskonzept mit seinen rollenbasierten Zugriffsregeln und seinen Pseudonymisierungs- und Verschlüsselungskonzepten. Zur Nutzerauthentifizierung wird die Public Domain Software „Keycloak“ in Verbindung mit einer 2-Faktorauthentifizierung als Service instanziiert. Für die Übermittlung von elektronischen Datensätzen für die Teilnahmeerklärungen der STATAMED-Klinikstandorte und auch der Versicherten sowie den elektronischen Teilnehmerverzeichnissen werden abhängig von den teilnehmenden Krankenkassen zwei unterschiedliche Übertragungswege gewählt:

1) Nutzung des Nachrichtendienstes „Kommunikation im Medizinwesen“ (KIM) der Telematikinfrastruktur (TI)
2) Übermittlung in verschlüsselter Form (via KKS-Verfahren, spezifiziert durch den GKV-Spitzenverband)

Das Datenformat der Teilnahmeerklärungen und Teilnehmerverzeichnisse entspricht der Spezifikation eTE/TEVE der AOK Systems und ermöglicht die automatisierte Kommunikation mit dem Krankenkassenbackend oscare® MC 3.0/3.2.

Projektplattform

Das HealthPortal als Projektplattform wird nicht im Rahmen der besonderen Versorgung vergütet, ist jedoch zwingender Bestandteil des Versorgungsmodells im Rahmen des Projektes. Die projektspezifische Weiterentwicklung und der Betrieb des HealthPortals wird über Fördermittel aus dem Innovationsfonds nach § 92a SGB V gefördert. Die Nutzung des HealthPortals im Projekt begründet für die Krankenkassen sowie die übrigen Vertragsparteien keinerlei Verpflichtung, die Projektplattform nach Ende des Versorgungsvertrages bzw. nach Ablauf des Förderzeitraums unter Aufbringung von Eigenmitteln, z.B. im Rahmen einer Zwischenfinanzierung, zu nutzen. Ebenso wenig wird ein Anspruch auf die Überführung der Projektplattform in die Regelversorgung unter Aufbringung von Eigenmitteln begründet.

2.4. MOCO

2.5. Datenarten

Tabelle 4 zeigt die Primär- und Sekundärdaten, die für die Teilstudien erforderlich sind. Dabei wird der Grundsatz der Datensparsamkeit verfolgt.

Weiter auszuführen

Tabelle 4: Übersicht der Datenarten

Datenarten	Datenquelle	Datenerhebung	Benötigt von				Ethikvotum erforderlich? (Geprüft durch die jeweiligen Konsortialpartner)	
			HCHE	MHH	UKE	hcb	ja/nein/n.z.	
Versorgungs-/ Leistungsdaten während der Interventionsphase für Studienzwecke	HealthPlattform	Primärdaten	x		x	x	ja	HCHE
							n.z.	MHH
							ja	UKE
							nein	hcb
GKV-Routinedaten	AOK Rheinland/Hamburg AOK Niedersachsen	Sekundärdaten	x				ja	HCHE
							n.z.	MHH
							n.z.	UKE
							n.z.	hcb
KHEntgG § 21	STATAMED-Standorte	Sekundärdaten	x		x	x	ja	HCHE
							n.z.	MHH
							ja	UKE
							nein	hcb
Standortbezogene Finanz-,Personal-, Leistungsdaten	STATAMED-Standorte	Sekundärdaten	x			x	nein	HCHE
							n.z.	MHH
							n.z.	UKE
							nein	hcb
Datenerhebungen für die Teilstudien (Fragebogenbefragung, Einzelinterviews, Fokusgruppen, Qualitätszirkel)	Datenerhebung	Primärdaten	x	x	x		ja	HCHE
							ja	MHH
							nein	UKE
							n.z.	hcb
Ambulante Abrechnungsdaten (im Rahmen des § 140a SGB V,§ 630a BGB)	KV-Statistik/ Abrechnungsstatistik	Sekundärdaten	x			x	ja	HCHE
							n.z.	MHH
							n.z.	UKE
							nein	hcb

Abk: nicht zutreffend (n.z.)

Im Folgenden sind die verwendeten Datenarten im Projekt nach Primär- und Sekundärdaten genauer beschrieben:

Primärdaten

Versorgungs- und Leistungsdaten: Die Versorgungs- und Leistungsdaten (z.B. Zuweiserweg, durchgeführte Leistungen des STATAMED-Personals) werden ausschließlich während der Interventionsphase zu Studienzwecke durch das STATAMED-Personal im

HelathPortal erfasst. Nach Aufklärung, Einwilligung und Unterzeichnung der Teilnahmeerklärung (Versorgungsvertrag nach § 140 a SGB V oder nach 630a BGB) der Patientin oder des Patienten wird entlang des stationären und prästationären Behandlungspfades die Versorgungs- und Leistungsdaten dokumentiert. Leistungen der vorstationäre STATAMED-Versorgung durch eine Flying Nurse erfolgt ohne Patientenbezug (anonymisiert).

Fragebogenbefragung:

Einzelinterviews:

Fokusgruppen:

Qualitätszirkel:

Sekundärdaten

GKV-Routinedaten: Bei dem betroffenen Personenkreis handelt es sich um STATAMED-Patientinnen und Patienten der Interventionsgruppe und Personen der Kontrollgruppe, die ihr informiertes Einverständnis zur Einholung, Weiterleitung und Auswertung der GKV-Routinedaten gegeben haben. Die pseudonymisierten Routinedaten (z.B. Stammdaten, stationäre Krankenhausleistungen, ambulante ärztliche Leistungen, Arzneimitteldaten) werden mit den Forschungsdaten durch die Datenmanagementstelle in der Vertrauensstelle verknüpft und liefern keine Rückschlüsse auf einzelne Versicherte.

Krankenhausdaten nach § 21 KHEntgG:

Standortbezogene Finanz-, Personal- und Leistungsdaten:

Ambulante Abrechnungsdaten (Versorgungsvertrag):

2.6. Datenflüsse

Zur Realisierung des Projektvorhabens ist die intensive Zusammenarbeit aller Projektbeteiligten essentiell und ein Austausch bzw. die Weiterleitung von Daten für die komplexe Intervention von STATAMED und der STATAMED-Studie unerlässlich. Abbildung 1 zeigt die Datenflusswege für die Kontrollgruppe und Abbildung 2 die Datenflusswege für die Interventionsgruppe mit allen an der Datenverarbeitung beteiligten Projekt- und Konsortialpartnern.

Datenfluss STATAMED: Kontrollgruppe

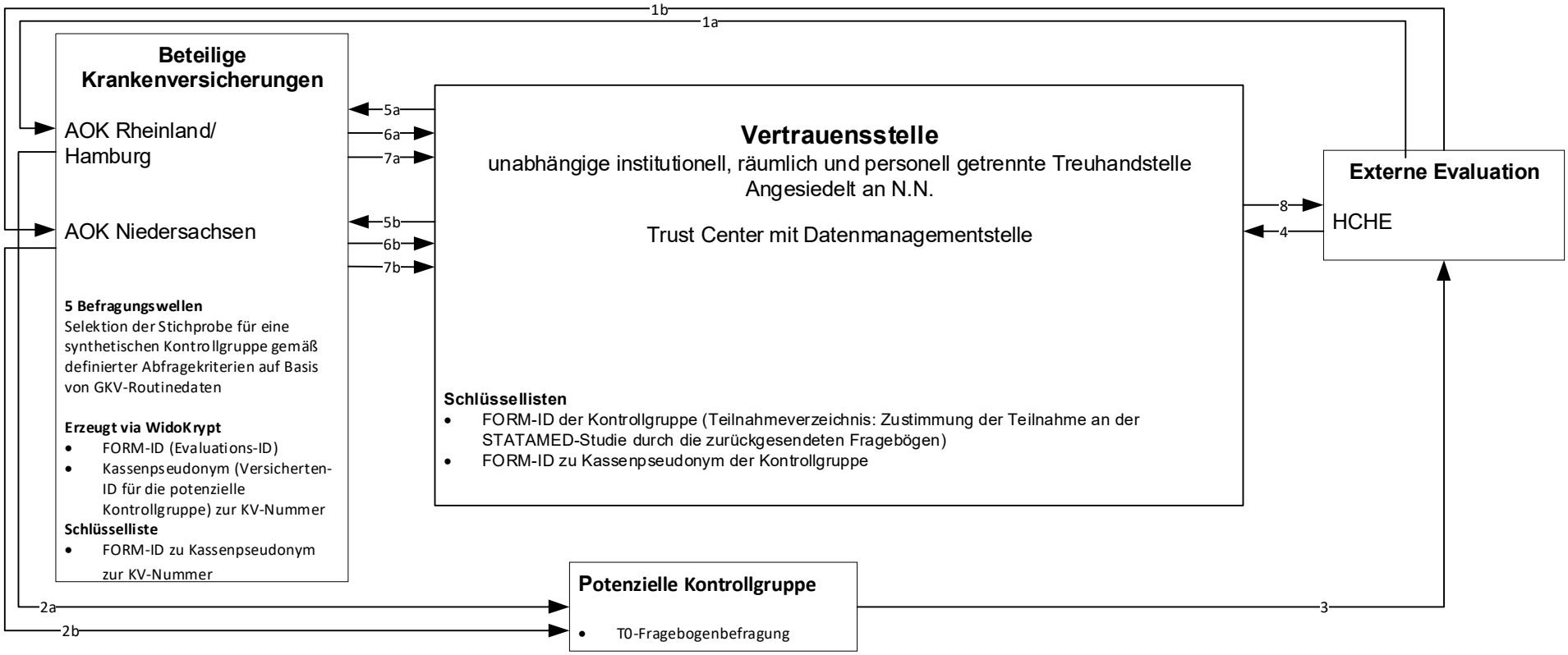

Abbildung 1: Datenfluss STATAMED – Kontrollgruppe

Die in der Abbildung 1dargestellten Ziffern werden im Folgenden beschrieben:

1a, b: Die HCHE stellt die Fragebögen der AOK Rheinland/Hamburg und AOK Niedersachsen zur Verfügung. Versicherte der Krankenkassen werden anhand festgelegter Selektionskriterien ausgewählt, um über das neue Versorgungsmodell STATAMED informiert zu werden und zur Teilnahme an der Fragebogenbefragung im Rahmen der STATAMED-Studie (als Teilnehmende der Kontrollgruppe) einzuladen.

2a, b: Die AOK Rheinland/Hamburg und AOK Niedersachsen versenden die Unterlagen für die Fragebogenbefragung per Post an potenzielle Teilnehmende der Kontrollgruppe. Die FORM-ID ohne Klarnamen dient als Kennzeichnung auf dem Fragebogen.

3: Die teilnehmende Versicherten der Fragebogenbefragung senden den Fragebogen anonymisiert per beigefügtem Freiumschlag an die HCHE zurück. Das auswertende wissenschaftliche Institut der HCHE hat keine Möglichkeit, Rückschlüsse auf die teilnehmende Person der Fragebogenbefragung zu ziehen. Die AOK Rheinland/Hamburg und AOK Niedersachsen haben keinen Zugriff auf die Befragungsdaten.

4: Die HCHE übermittelt die FORM-ID-Liste verschlüsselt als Teilnahmeverzeichnis der Kontrollgruppe (FORM-ID-Kennzeichen der zurückgesendeten Fragebögen) an die Vertrauensstelle.

5a, b: Die Vertrauensstelle übermittelt nach Abschluss jeder Befragungswelle die verschlüsselte Form-ID-Liste der Kontrollgruppe an die AOK Rheinland/Hamburg und AOK Niedersachsen.

6a, b: Die AOK Rheinland/Hamburg und AOK Niedersachsen übermitteln vor der GKV-Routinedatenlieferung zweimalig die Schlüsselliste der FORM-IDs zum generierten Kassenpseudonym der Kontrollgruppe (FORM-ID zu Kassenpseudonym“) zu den festgelegten Datenlieferzeitpunkten an die Vertrauensstelle.

7a, b: Die AOK Rheinland/Hamburg und AOK Niedersachsen übermitteln zweimalig zu den festgelegten Datenlieferzeitpunkten, vorbehaltlich einer Genehmigung der zuständigen Landesaufsichtsbehörde, pseudonymisierte GKV-Routinedaten mit Kassenpseudonym verschlüsselt an die Vertrauensstelle.

8: Die Vertrauensstelle führt die Datensätze der AOK Rheinland/Hamburg und AOK Niedersachsen zusammen und ergänzt die FORM-ID und übermittelt den Datensatz der GKV-Routinedaten verschlüsselt an die HCHE.

Datenfluss STATAMED: Interventionsgruppe

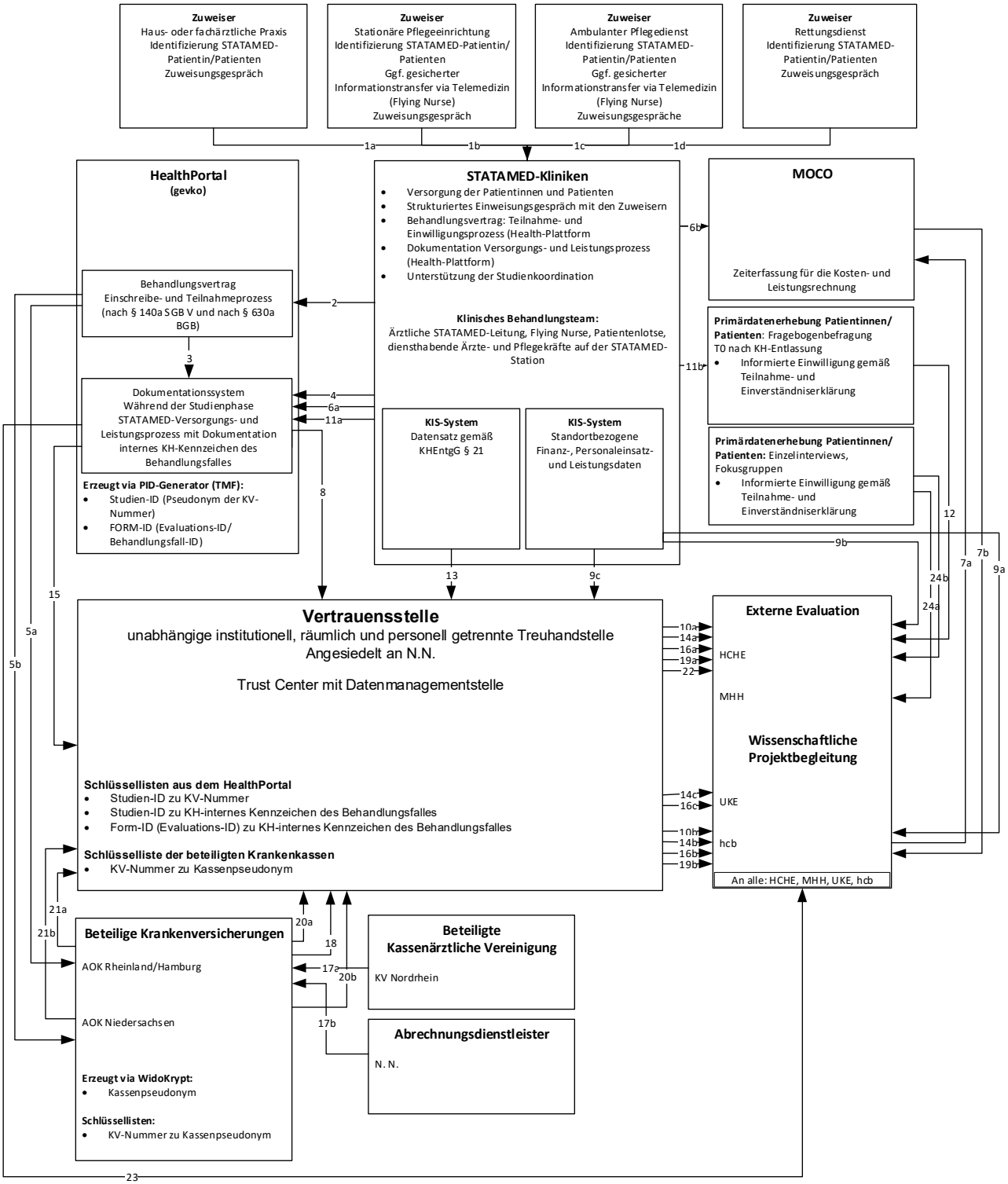

Abbildung 2: Datenfluss STATAMED – Interventionsgruppe

Die in der Abbildung 2 dargestellten Ziffern werden im Folgenden beschrieben:

1a-d: Der Zugangsweg für Patientinnen und Patienten zur vorstationären Versorgung erfolgt über die teilnehmenden Zuweiser von STATAMED. Bevor die Patientin oder der Patient in die STATAMED-Versorgung aufgenommen wird, findet ein strukturiertes Einweisungsgespräch zwischen den teilnehmenden Zuweisern und der ärztlichen STATAMED-Leitung statt. Dies gewährleistet einen reibungslosen Übergang in die Behandlung. Eine Erstinformation über die STATAMED-Versorgung wird den Patientinnen und Patienten ebenfalls durch die teilnehmenden Zuweiser bereitgestellt.

2: Der ärztliche STATAMED-Leitung der STATAMED-Klinik informiert und klärt die eingewiesene Patientin oder den eigewiesenen Patienten über die STATAMED-Versorgung und Studie auf. Die ärztliche STATAMED-Leitung holt die Einwilligung ein und legt dann auf dem Healthportal den digitalen Behandlungsvertrag (nach § 140a SGB V oder nach § 630a BGB) an. Die Teilnahme- und Einverständniserklärung der Patientin und des Patienten erfolgt.

3: Die im HealthPortal erfassten Stammdaten des Teilnahme- und Einschreibungsprozesses des Behandlungsvertrags werden automatisch ins Dokumentationssystem übertragen, welches zur Erfassung von Leistungs- und Versorgungsdaten während der Studienphase dient. Dabei wird automatisch eine Studien-ID (Studien-Pseudonym der Patientin/des Patienten für die Interventionsgruppe) und eine FORM-ID (Evaluations-ID für die Fragebogenbefragung und Kennzeichen des Behandlungsfalles) vergeben.

4: Im HealthPortal trägt die ärztliche STATAMED-Leitung das interne Krankenhaus-Kennzeichen des Behandlungsfalles (§ 21 KHEntgG.) der eingeschriebenen Patienten oder der eingeschriebenen Patientin ein.

5a, b: Die Teilnahme- und Einschreibungsdaten der Patientinnen und Patienten der Interventionsgruppe werden im HealthPortal erfasst und anschließend an die AOK Rheinland/Hamburg (Versicherte gemäß BGB § 630a und Versicherte der AOK Rheinland/Hamburg gemäß SGB V § 140a) sowie an die AOK Niedersachsen (Versicherte der AOK Niedersachsen gemäß SGB V § 140a) übermittelt.

6a: Das Behandlungsteam der STATAMED-Kliniken (ärztliche STATAMED-Leitung, Flying Nurse, Patientenlotse, diensthabende Ärztinnen/Ärzte und Pflegekräfte) dokumentiert über das Dokumentationssystem im HealthPortal kontinuierlich Versorgungs- und Leistungsdaten während der Studienphase (z.B. Leistungsart, Gesprächsanzahl, Drop Out)

entlang des Behandlungspfades der STATAMED-Patientinnen und Patienten aus der Interventionsgruppe.

6b: Das Behandlungsteam der STATAMED-Kliniken misst die Dauer für definierte Leistungsarten (wie beispielsweise die Dauer des Zuweisergesprächs) über die SSL-verschlüsselte webbasierte Plattform MOCO zur Berechnung des Zeit- und Arbeitsvolumens im Behandlungsprozess. Dabei werden keine patientenbezogenen Daten erfasst. Die Zeiterfassung erfolgt ab dem zweiten Jahr der Interventionsphase innerhalb vorab festgelegter Zeitfenster.

7a, b: Die hcb kann auf die dokumentierten Zeiten der SSL-verschlüsselten, webbasierten Plattform MOCO zugreifen. Die erfassten Zeiten werden von der hcb als Datei exportiert.

8: Vom HealthPortal des Dokumentationssystems erhält die Vertrauensstelle zu den festgelegten Zeitpunkten per Datenexport verschlüsselt drei getrennte Schlüssellisten "Studien-ID zu KV-Nummer“, Studien-ID zu Krankenhaus-internes Kennzeichen des Behandlungsfalls" und „Form-ID zu KH-internes Kennzeichen des Behandlungsfalls “.

9a: Die STATAMED-Kliniken übermitteln verschlüsselt standortbezogene Finanz-, Personaleinsatz- und Leistungsdaten (Daten ohne Personenbezug wie Summen-, Saldenlisten, Jahresabschluss, Mitternachtsstatistik) zu den festgelegten Lieferzeitpunkten an die hcb und HCHE.

9b: Die STATAMED-Kliniken übermitteln verschlüsselt standortbezogene Finanz-, Personaleinsatz- und Leistungsdaten (Daten ohne Personenbezug wie Summen-, Saldenlisten, Jahresabschluss, Mitternachtsstatistik) zu den festgelegten Lieferzeitpunkten an die HCHE.

9c: Die Vertrauensstelle erhält von den STATAMED-Kliniken zu den festgelegten Datenlieferzeitpunkten standortbezogene Finanz-, Personaleinsatz- und Leistungsdaten (z.B. aus der Radiologie, Labor, Konsile) mit personenbeziehbare Informationen (faktisch anonymisiert) verschlüsselt für die hcb und HCHE. Die Vertrauensstelle führt ein Datenlinkage zwischen den Daten und der Schlüssellisten "Studien-ID zu KV-Nummer“ und „Form-ID zu Krankenhaus-internes Kennzeichen des Behandlungsfalls" durch. Die „KV-Nummer“ und das „Krankenhaus-interne Kennzeichen des Behandlungsfalles“ wird für die Datenbereitstellung an die hcb und HCHE gelöscht.

10a: Die Vertrauensstelle übermittelt die pseudonymisierten Datensätze der standortbezogene Finanz-, Personaleinsatz- und Leistungsdaten verschlüsselt an die HCHE.

10b: Die Vertrauensstelle übermittelt die pseudonymisierten Datensätze der standortbezogene Finanz-, Personaleinsatz- und Leistungsdaten verschlüsselt an die hcb.

11a: Die Patientenlotsen der jeweiligen STATAMED-Kliniken unterstützen den externen Evaluator HCHE bei der Koordination der Primärdatenerhebung zur T0-Fragebogenbefragung (T0 = im Zeitraum 21 Tage nach Krankenhausentlassung) der STATAMED-Patientinnen und -Patienten der Interventionsgruppe. Über das Dokumentationssystem im HealthPortal wählt der Patientenlotse die jeweiligen Patientinnen und Patienten aus, die für die T0-Fragebogenbefragung angeschrieben werden sollen.

11b: Die Patientenlotsen stellen den teilnehmenden Patientinnen und Patienten die Fragebögen nach ihrer Entlassung aus dem Krankenhaus bereit (im Zeitraum von 21 Tagen nach Entlassung). Die Fragebögen werden mit der FORM-ID gekennzeichnet und das Anschreiben mit dem Fragebogen über das Dokumentationssystem im HealthPortal gedruckt und per Post den Teilnehmenden der Interventionsgruppe zugesendet.

12: Die teilnehmenden Patientinnen und Patienten der Fragebogenbefragung senden den Fragebogen anonymisiert per beigefügtem Freiumschlag an die HCHE zurück.

13: Die STATAMED-Kliniken übermitteln verschlüsselt die Krankenhausdaten des 21er Datensatzes (§ 21 KHEntgG) zu den festgelegten Datenlieferzeitpunkten an die Vertrauensstelle. Die Vertrauensstelle führt ein Datenlinkage zwischen dem 21er Datensatz und der Schlüsselliste "FORM-ID zu Krankenhaus-internes Kennzeichen des Behandlungsfalls" und „Studien-ID zu KV-Nummer“ durch. Die KV-Nummer und das interne Krankenhaus-Kennzeichen des Behandlungsfalles wird für die Datenbereitstellung gelöscht.

14a: Die Vertrauensstelle übermittelt den pseudonymisierten 21er Datensatz (§ 21 KHEntgG) verschlüsselt an die HCHE.

14b: Die Vertrauensstelle übermittelt den pseudonymisierten 21er Datensatz (§ 21 KHEntgG) verschlüsselt an die hcb.

14c: Die Vertrauensstelle übermittelt den pseudonymisierten 21er Datensatz (§ 21 KHEntgG) verschlüsselt an die UKE.

15: Vom HealthPortal des Dokumentationssystems werden die Datenexporte der Versorgungs- und Leistungsdaten während der Studienphase zu den festgelegten Datenlieferzeitpunkten verschlüsselt an die Vertrauensstelle übermittelt. Die Vertrauensstelle führt ein Datenlinkage zu den Versorgungs- und Leistungsdaten anhand der Schlüsselliste "Studien-ID zu KV-Nummer", „Form-ID zu KH-internes Kennzeichen des Behandlungsfalles“ durch und entfernt anschließend die „KV-Nummern“ und das „KH-interne Kennzeichen des Behandlungsfalles“ aus den Datensätzen, die an die HCHE, die hcb und der UKE übermittelt werden sollen.

16a: Die Vertrauensstelle übermittelt die pseudonymisierten Versorgungs- und Leistungsdaten (HealthPortal) verschlüsselt an die HCHE.

16b: Die Vertrauensstelle übermittelt die pseudonymisierten Versorgungs- und Leistungsdaten (HealthPortal) verschlüsselt an die hcb.

16c: Die Vertrauensstelle übermittelt die pseudonymisierten Versorgungs- und Leistungsdaten (HealthPortal) verschlüsselt an die UKE.

17a: Die Kassenärztliche Vereinigung übermittelt quartalsweise verschlüsselt an die AOK Rheinland/Hamburg die KV-Statistik über die abgerechneten ärztlichen Leistungen in niedergelassenen Praxen des vorangegangenen Quartals, die gemäß dem Versorgungsvertrag (nach § 140a SGB V und nach § 630a BGB) mit Mitteln des Innovationsfonds finanziert werden.

17b: Der Abrechnungsdienstleister übermittelt quartalsweise verschlüsselt an die AOK Rheinland/Hamburg die Abrechnungsstatistik über die abgerechneten ärztlichen Leistungen in niedergelassenen Praxen des vorangegangenen Quartals, die gemäß dem Versorgungsvertrag (nach § 140a SGB V und nach § 630a BGB) mit Mitteln des Innovationsfonds finanziert werden.

18: Die AOK Rheinland/Hamburg entfernt die Klarnamen und übermittelt die KV-Statistik und die Abrechnungsstatistik zweimal verschlüsselt über CryptShare an die Vertrauensstelle zu den festgelegten Datenlieferzeitpunkten. Die Vertrauensstelle führt ein Datenlinkage zwischen der KV-Statistik bzw. der Abrechnungsstatistik und der Schlüsselliste "Studien-ID zu KV-Nummer" durch und entfernt anschließend die KV-Nummern aus den Datensätzen.

19a: Die Vertrauensstelle übermittelt die pseudonymisierte KV-Statistik bzw. Abrechnungsstatistik verschlüsselt an die HCHE.

19b: Die Vertrauensstelle übermittelt die pseudonymisierte KV-Statistik bzw. Abrechnungsstatistik verschlüsselt an die hcb.

20a, b: Die AOK Rheinland/Hamburg und die AOK Niedersachsen übermitteln zweimal getrennt zu den festgelegten Datenlieferzeitpunkten der GKV-Routinedaten verschlüsselt via CryptShare eine Schlüsselliste "KV-Nummer zu Kassenpseudonym" an die Vertrauensstelle für die Versicherten der Interventionsgruppe der jeweiligen AOK Rheinland/Hamburg bzw. AOK Niedersachsen.

21a, b: Die AOK Rheinland/Hamburg und die AOK Niedersachsen übermitteln verschlüsselt via CryptShare zweimal zu den festgelegten Datenlieferzeitpunkten, unter Vorbehalt der Genehmigung durch die zuständige Landesaufsichtsbehörde, pseudonymisierte GKV-Routinedaten (KV-Nummer wird mit einem Kassenpseudonym ersetzt) an die Vertrauensstelle. Die Vertrauensstelle führt ein Datenlinkage zwischen der Schlüsselliste "KV-Nummer zu Kassenpseudonym" und anschließend der Schlüsselliste "Studien-ID zu KV-Nummer", Studien-ID zu KH-internes Kennzeichen des Behandlungsfalles“ und „FORM-ID zu KH-internes Kennzeichen des Behandlungsfalles“ durch. Daraufhin wird das Kassenpseudonym des Versicherten, die KV-Nummer und das KH-interne Kennzeichen des Behandlungsfalles wieder aus den Datensätzen entfernt.

22: Die Vertrauensstelle übermittelt die pseudonymisierte GKV-Routinedaten verschlüsselt an die HCHE.

23: Anonymisierte Studiendaten ohne Bezug zu Versicherten (erfasste Leistungsarten der prästationäre STATAMED-Versorgung), werden direkt aus dem Dokumentationssystem des HealthPortals verschlüsselt per Datenexport zu den festgelegten Datenlieferzeitpunkten an die HCHE, hcb, UKE und MHH übermittelt.

24a, b: Die Kontaktdaten potenzieller STATAMED-teilnehmende Patienten und Patientinnen der Interventionsgruppe für die Primärdatenerhebung zur formativen Evaluation/Prozessevaluation werden im Rahmen der Studie an die HCHE und MHH übermittelt, unter der Voraussetzung einer informierten Einwilligung der Teilnehmenden zur Kontaktaufnahme zu STATAMED-Studienzwecke liegt vor.

2.7. Datentransfer

2.7.1. Rollen und Zugriffberechtigung

2.8. Qualitätssicherung bei der Datenerhebung und -verarbeitung

2.9. Rechtsgrundlage der Datenverarbeitung

Im Rahmen von STATAMED wird die Rechtmäßigkeit der Verarbeitung nach Artikel 6 Absatz 1a und Artikel 9 Absatz 2a der DSGVO geregelt.

2.10. Einwilligungsverfahren

Die Einwilligung zur Teilnahme an der neuen Versorgungsform STATAMED durch die Patientinnen und Patienten der Interventionsgruppe erfolgt im Rahmen des Behandlungsvertrags gemäß § 140a SGB V für AOK Rheinland/Hamburg oder AOK Niedersachsen Versicherte bzw. gemäß § 630a BGB für GKV-Versicherte, die nicht dem Selektivvertrag beigetreten sind. Sie werden über das STATAMED-Projekt und die Studie von der ärztlichen STATAMED-Leitung aufgeklärt und informiert. Durch den Behandlungsvertrag (gemäß § 140a SGB V oder § 630a BGB) werden sie für die Teilnahme an der neuen Versorgungsform und der Studie eingeschrieben. Die schriftliche Zustimmung zur Durchführung der geplanten STATAMED-Versorgung, zur Datenerhebung, Datenweiterleitung und Datenverarbeitung zu Forschungszwecken geben sie informiert ab. Zusätzlich gilt für die GKV-Routinedaten der § 75 SGB X. Die Übermittlung der Daten erfolgt nur nach Genehmigung durch die Landesaufsichtsbehörde der Krankenkassen.

Die Versicherten der potenziellen Kontrollgruppe werden über die neue Versorgungsform STATAMED und die dazugehörige Studie durch die AOK Rheinland/Hamburg und AOK Niedersachsen informiert. Die Teilnahme an der STATAMED-Studie ist für die Versicherten freiwillig und steht in keinem Zusammenhang mit ihrer Versicherung bei der AOK Rheinland/Hamburg oder AOK Niedersachsen. Die Ethikkommission der Universität

Hamburg hat das Vorgehen zur Rekrutierung und Teilnahme an der STATAMED-Studie positiv bewertet und zugestimmt.

Die STATAMED-Zuweiser (niedergelassene Ärztinnen und Ärzte, stationäre Pflegeeinrichtungen, ambulante Pflegedienste, Rettungsdienste) werden über die Datenverarbeitung und Weiterleitung ihrer Kontaktdaten informiert und aufgeklärt. Die AOK Rheinland/Hamburg, als Konsortialführer des Innovationsfondsprojekts STATAMED, erhält die Registrierungsdaten zur notwendigen Projektdokumentation, das Universitätsklinikum Hamburg-Eppendorf (UKE) für die Planung und Durchführung der STATAMED-Zuweiser-Schulung. Für die verschiedenen Schulungsmodule (differenziert nach am Projekt teilnehmenden Zuweisergruppen) hat das Institut und Poliklinik für Allgemeinmedizin am Universitätsklinikum Hamburg-Eppendorf die jeweiligen SOPs entwickelt und führt die Schulungen online durch. Für die Teilnahme der Zuweiser ist eine Registrierung zwingend erforderlich, die durch die gevko GmbH || Gesundheit - Versorgung - Kommunikation erfolgt. Der Datenaustausch zwischen der gevko GmbH, der AOK Rheinland/Hamburg, der UKE und den weiteren an der Evaluation beteiligten Organisationen erfolgt digital und verschlüsselt. Die verantwortlichen Evaluatoren erhalten die Kontaktdaten über die Vertrauensstelle. Sie nutzen die personenbezogenen Daten ausschließlich im Rahmen der wissenschaftlichen Evaluation des Projektes STATAMED.

2.11. Widerruf und Datenlöschung

Die Teilnehmenden der Interventions- und Kontrollgruppe sowie die Zuweiser haben jederzeit das Recht, ihr Einverständnis zur Teilnahme an STATAMED ohne Angabe von Gründen zurückzuziehen und die Löschung ihrer Daten zu fordern. Dieser Rückzug kann schriftlich, telefonisch oder persönlich erfolgen. Die Teilnahmeerklärung zum Versorgungsvertrag gemäß § 140a SGB V und Teilnahme an der STATAMED-Studie kann von AOK Rheinland/Hamburg-Versicherte schriftlich, elektronisch oder zur Niederschrift bei der AOK Rheinland/Hamburg ohne Angabe von Gründen widerrufen. Die Teilnahmeerklärung zum Versorgungsvertrag gemäß § 140a SGB V und Teilnahme an der STATAMED-Studie kann von AOK Niedersachsen-Versicherte schriftlich, elektronisch oder zur Niederschrift bei der AOK Niedersachsen ohne Angabe von Gründen widerrufen werden. Die Teilnahmeerklärung zum Versorgungsvertrag gemäß § 630a BGB und Teilnahme an der STATAMED-Studie kann schriftlich, elektronisch oder zur Niederschrift bei den an STATAMED teilnehmenden Kliniken ohne Angabe von Gründen widerrufen werden.

Falls das Einverständnis zur Übermittlung der Daten (siehe Abschnitt Datenarten) widerrufen wird, werden die entsprechenden Daten umgehend gelöscht. Im Falle eines Widerrufs wird keine Datenlieferung durch die Krankenkassen (GKV Routinedaten), das HealthPortal oder die Klinikstandorte durchgeführt. Bei einem Widerruf der Teilnahme an der Fragebogenbefragung, den Interviews oder Fokusgruppen werden die Aufzeichnungen sofort gelöscht. Für Fokusgruppen kann das Transkript jedoch weiterhin zur Auswertung verwendet werden, da es keine persönlichen Angaben enthält. Ein Widerruf der Einwilligung führt außerdem zum Ausscheiden aus der neuen Versorgungsform STATAMED und der STATAMED-Studie.

2.12. Datenspeicherung und Aufbewahrungsfristen

Alle im Rahmen erhobenen Primär- und Sekundärdaten (siehe Abschnitt Datenarten) dürfen ausschließlich zur Weiterentwicklung und Qualitätsprüfung der neuen Versorgungsform STATAMED sowie für wissenschaftliche Fragestellungen, die die STATAMED-Teilstudien und ihre Einflussgrößen betreffen, ausgewertet und anonym veröffentlicht werden. Projektbezogene pseudonymisierte Daten werden von den verantwortlichen Institutionen der externen Evaluation (HCHE, MHH) sowie der wissenschaftlichen Projektbegleitung (UKE, hcb) gemäß den Vorschriften der „Guten Wissenschaftlichen Praxis“ für mindestens 10 Jahre zugriffsgeschützt auf einem Server oder passwortgeschützt auf einem Datenträger in einem Tresor gespeichert und anschließend gelöscht.

Personenbezogene oder personenbeziehbare Merkmale sowie identifizierbare Institutionsdaten werden am Ende des STATAMED-Projekts unwiderruflich der Vertrauensstelle externer Dienstleister gelöscht, um eine Identifizierung natürlicher Personen oder Institutionen nach Projektende zu verhindern.

3. Technische und organisatorische Maßnahmen

Folgend werden für die evaluierenden Institute das Sicherheitskonzept mit den jeweils technischen und organisatorischen Maßnahmen erläutert.

3.1. Sicherheitskonzept der Vertrauensstelle

3.2. Sicherheitskonzept des Hamburg Center for Health Economics

1. Technische und organisatorische Maßnahmen

☒ Erläuterungen zu den einzelnen Maßnahmen zur Gewährleistung der

Vertraulichkeit:

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Z.B.:

Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern

Benutzerkontrolle durch Passwortregelung zur Legitimation und durch automatische Bildschirmsperrung

Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

Die Studiendaten, die das HCHE erhält, (GKV-Routinedaten, Daten nach §21 KHEntG, Versorgungs- und Leistungsdaten aus dem healthportal, KV-Statistik aus dem Versorgungsvertrag, Befragungsdaten von Versicherten und Zuweisern) liegen ausschließlich in pseudonymisierter Form vor.

Ausschließlich am Projekt beteiligte Mitarbeitenden erhalten Zugriff auf die Studiendaten.

Die Datenspeicherung erfolgt auf den Servern der Universität Hamburg. Zugriff ist nur mit personalisiertem Benutzername und Passwort möglich. Die Ordner mit den STATAMED-Daten sind zudem mit einem weiteren Passwort geschützt, so ist sichergestellt, dass nur Projektmitarbeiter Zugriff erhalten.

Die jeweiligen Arbeitsrechner werden mit automatischen Bildschirmsperren geschützt.

Die Räume des HCHE sind durch eine Sicherheitsschließanlage und ein Alarmsystem gesichert. Die Mitarbeiter müssen den Schlüsselerhalt mit Unterschrift bestätigen.

Integrität:

Integrität ist gegeben, wenn personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Z.B.:

Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten

Regelmäßige Kontrolle der Aktualität

Ausschließlich die am Projekt beteiligten Mitarbeitenden erhalten Zugriff auf die Studiendaten.

Die Daten werden regelmäßig hinsichtlich Ihrer Aktualität geprüft.

Die Rohdaten werden in einem anderen Ordner, separat von den Auswertungsdaten, auf den Servern gespeichert. Eine Kontrolle der Aktualität der Daten ist zu jeder Zeit möglich.

Für die Server des HCHE wird regelmäßig ein automatisiertes Backup erstellt.

Verfügbarkeit:

Verfügbarkeit ist gegeben, wenn personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Z.B.:

klare und übersichtliche Ordnung des Datenbestandes

Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

Eine klare übersichtliche Ordnung und Beschreibung des Datensatzes wird sichergestellt. Um dies zu gewährleisten wird zusätzlich ein Datenhandbuch angelegt.

Der Zugriff kann über einen gesicherten Zugang am Arbeitsplatz oder über einen gesicherten VPN-Zugriff erfolgen. Wartungen finden außerhalb der Kernarbeitszeiten statt. Regelmäßige Verfügbarkeit ist gewährleistet.

Authentizität:

Authentizität ist gegeben, wenn jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können. Z.B.:

Dokumentation der Ursprungsdaten und ihrer Herkunft

Nachvollziehbarkeit der Verarbeitungsschritte

Die Dokumentation der Ursprungsdaten und ihre Herkunft wird in einem Datenhandbuch festgehalten.

Die Rohdaten werden separat gespeichert und bleiben unverändert.

Die Nachvollziehbarkeit der Verarbeitungsschritte und Auswertungen wird mit Hilfe von Syntaxen sichergestellt.

Revisionsfähigkeit:

Revisionsfähigkeit ist gegeben, wenn festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Z.B.:

Festlegung klarer Zuständigkeiten und Verantwortlichkeiten

Protokollierung der Eingabe und weiteren Verarbeitung der Daten

Aufbewahrung der Protokolldaten

Alle Arbeitsschritte zur Eingabe und Verarbeitung der Daten werden durch die Mitarbeitenden mit Hilfe von Syntaxen protokolliert und in einem Datenhandbuch vermerkt. Diese Protokolldaten werden ebenfalls auf den Servern gesichert. Nur die am Projekt beteiligten Mitarbeitenden erhalten Zugriff.

Zuständigkeiten und Verantwortlichkeiten werden protokolliert.

Transparenz:

Transparenz ist gegeben, wenn die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können. Z.B.:

vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge

Die Transparenz wird durch das Datenhandbuch und Dokumentation der Syntaxen sichergestellt. Zusätzlich wird die für die Verarbeitung und Auswertung verwendete Software nachvollziehbar protokolliert.

2. Technik des Verfahrens

2.1 ☐ Verfahren für Einzelplatzsystem

Betriebssystem:

	☐ Unix ☐ Windows NT ☐ Windows [...] ☐ anderes [...]

2.2 ☒ Client – Server - Verfahren

Client (Datenendgerät):	☐ Terminal / Netz -PC (ohne Laufwerk/Festplatten) ☒ PC (Arbeitsplatzrechner / Workstation)
Betriebssystem des Servers (z. B. Windows NT): Windows und Linux	
Client – Server Kommunikation erfolgt über	
☒ geschlossenes Netz innerhalb der Behörde (LAN) ☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises: ☐ Landesverwaltungsnetz ☐ Sonstiges ☐ offenes Netz (z. B. Internet): [...] ☐ sonstige eingesetzte Hardware (z. B. Chipkarte, Kartenlesegeräte, Videogeräte): [...]	
Datenspeicherung erfolgt auf	
☒ Server innerhalb der Behörde ☐ Server bei anderen Institutionen ☐ PC/ Arbeitsplatzrechner ☐ Sonstiges [...] Art der Daten (lfd. Nr. aus Ziffer 3): [...]	

3. Eingesetzte Software

(einschl. Standardverfahren)	Version / Stand / Datum:
STATA	18 (oder neuer)
SPPS	29 (oder neuer)
RStudio	9.3.191.259 (oder neuer)
MAXQDA	2022 (oder neuer)
MS Office	2019 (oder neuer)
Adobe Reader	23.006.20380 (oder neuer)
AMOS	28 (oder neuer)

3.3. Sicherheitskonzept der Medizinischen Hochschule Hannover

1. Technische und organisatorische Maßnahmen

☒ Erläuterungen zu den einzelnen Maßnahmen zur Gewährleistung der

Vertraulichkeit:

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Z.B.:

Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern

Benutzerkontrolle durch Passwortregelung zur Legitimation und durch automatische Bildschirmsperrung

Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

Die Räumlichkeiten des Instituts für Allgemeinmedizin und Palliativmedizin der Medizinischen Hochschule Hannover sind mit Sicherheitsschlössern ausgestattet, die einen unbefugten Zutritt zu den einzelnen Büros verhindern. Zudem ist das Gebäude außerhalb der Bürozeiten mit einer Alarmanlage versehen. Die Studiendaten werden auf einem gesicherten Server der Medizinischen Hochschule Hannover gespeichert, der Zugriff zu den Arbeitsrechnern ist nur durch personalisierten Benutzernamen und Passwort möglich.

Die Vertraulichkeit im Rahmen der wissenschaftlichen Durchführung und Auswertung der qualitativen Prozessevaluation wird durch die Vergabe einer Identifikationsnummer für alle Audioaufnahmen gewahrt. In einer passwortgeschützten Liste werden Identifikationsnummer und Name der Teilnehmenden zusammengeführt. Die Liste wird getrennt von den erhobenen Daten gespeichert, so dass es keine Verbindung zwischen den persönlichen Informationen der Teilnehmenden und den Identifikationsnummern gibt. Einverständniserklärungen werden ebenfalls getrennt von erhobenen Daten in einem abgeschlossenen Aktenschrank verwahrt. Die Daten werden auf dem internen Server der MHH im STATAMED-Projektordner gesichert und mit begrenzten Zugangsrechten versehen. Dateien, die personenbezogene Daten enthalten, werden in einem separaten Unterordner gespeichert und mit einem Passwortschutz versehen. Der Zugang zu den digitalen Ordnern ist auf die an der Studie beteiligten Mitarbeitenden beschränkt.

Integrität:

Integrität ist gegeben, wenn personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Z.B.:

Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten

Regelmäßige Kontrolle der Aktualität

Der Zugriff auf die Studiendaten ist ausschließlich auf die Projektleitung sowie Mitarbeitende im STATAMED-Projekt beschränkt (s. Abschnitt Vertraulichkeit). Die Daten werden gemäß den Sicherheitsrichtlinien des MHH-Servers im Rahmen täglicher Back-Ups zum Schutz vor Datenverlust oder Beschädigung gesichert. Mitarbeitende prüfen zudem regelmäßig die Aktualität der Daten, die Rohdaten der qualitativen Teilstudien (z.B. Audiodateien) werden nicht verändert. Die Datenaufbereitung und –auswertung erfolgen regelgeleitet und qualitätsgesichert, die Dateien werden als separate Dateien abgespeichert. Die Arbeitsschritte im Datenmanagement werden nachvollziehbar dokumentiert.

Verfügbarkeit:

Verfügbarkeit ist gegeben, wenn personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Z.B.:

klare und übersichtliche Ordnung des Datenbestandes

Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

Die pseudonymisierten Daten werden entsprechend der Teilstudien sortiert und übersichtlich dargestellt. Der Zugriff auf die Daten wird a) über den benutzerspezifischen, passwortgeschützten Arbeitsplatz b) über den benutzerspezifischen, passwortgeschützten Citrix-Client der Medizinischen Hochschule Hannover ermöglicht. Wartungen des Systems finden außerhalb der Kernarbeitszeiten statt. Eine regelmäßige Verfügbarkeit der Daten ist somit gewährleistet.

Authentizität:

Authentizität ist gegeben, wenn jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können. Z.B.:

Dokumentation der Ursprungsdaten und ihrer Herkunft

Nachvollziehbarkeit der Verarbeitungsschritte

Die Datenstrukturen werden festgelegt und dokumentiert. Die Rohdaten (v.a. Audioaufnahmen der qualitativen Teilstudien) bleiben unverändert und erhalten eine Identifikationsnummer, diese in einer passwortgeschützten Liste mit dem Namen der Teilnehmenden zusammengeführt werden. Die Liste wird getrennt von den erhobenen Daten gespeichert, so dass es keine Verbindung zwischen den persönlichen Informationen der Teilnehmenden und den Identifikationsnummern gibt. Dateien, die personenbezogene Daten enthalten, werden in einem separaten Unterordner gespeichert und mit einem Passwortschutz versehen. Die aufbereiteten Daten werden für die Datenauswertung in jedem Prozessschritt als Arbeitsdateien gespeichert.

Revisionsfähigkeit:

Revisionsfähigkeit ist gegeben, wenn festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Z.B.:

Festlegung klarer Zuständigkeiten und Verantwortlichkeiten

Protokollierung der Eingabe und weiteren Verarbeitung der Daten

Aufbewahrung der Protokolldaten

Die Arbeitsschritte zur Aufbereitung und Auswertung der pseudonymisierten, qualitativen Daten werden protokolliert, im Arbeits- und Zeitplan werden Zuständigkeiten festgeschrieben. Die entsprechenden Dateien werden auf den institutseigenen Servern der MHH im Projektordner abgelegt, die nur für Projektmitarbeitende zugänglich sind.

Transparenz:

Transparenz ist gegeben, wenn die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können. Z.B.:

vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge

Die eingesetzte Software ist umfangreich dokumentiert, bei der verwendeten Standardsoftwarte sind die entsprechende Anleitungen vorhanden. Die Datenverarbeitungsvorgänge werden nachvollziehbar und systematisch dokumentiert.

2. Technik des Verfahrens

2.1 ☐ Verfahren für Einzelplatzsystem

	Betriebssystem: Institutsrechner und Arbeitslaptop
	☐ Unix ☐ Windows NT ☒ Windows [...] ☐ anderes [...]

2.2 ☐ Client – Server - Verfahren

Client (Datenendgerät):	☐ Terminal / Netz -PC (ohne Laufwerk/Festplatten) ☒ PC (Arbeitsplatzrechner / Workstation)
Betriebssystem des Servers (z. B. Windows NT): Windows 2016	
Client – Server Kommunikation erfolgt über	
☒ geschlossenes Netz innerhalb der Behörde (LAN)	
☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises:	

	☐ Landesverwaltungsnetz	☐ Sonstiges
	☐ offenes Netz (z. B. Internet): [...]	
	☐ sonstige eingesetzte Hardware (z. B. Chipkarte, Kartenlesegeräte, Videogeräte): [...]	
	Datenspeicherung erfolgt auf	
	☒ Server innerhalb der Behörde	☐ Server bei anderen Institutionen
	☒ PC/ Arbeitsplatzrechner	☐ Sonstiges [...]
	Art der Daten (lfd. Nr. aus Ziffer 3): [...]	

3. <u>Eingesetzte Software</u>

	(einschl. Standardverfahren)	Version / Stand / Datum:
	Microsoft Office (Excel, Word) MAXQDA	2016 oder aktueller 2020 oder aktueller

3.4. Sicherheitskonzept des Universitätsklinikums Hamburg-Eppendorf

1. <u>Technische und organisatorische Maßnahmen</u>

☒	Erläuterungen zu den einzelnen Maßnahmen zur Gewährleistung der
Vertraulichkeit:	

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Z.B.:

Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern

Benutzerkontrolle durch Passwortregelung zur Legitimation und durch automatische Bildschirmsperrung

Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

Ausschließlich die Mitarberinnen und Mitarbeiter, die im Rahmen des STATAMED Projektes angestellt sind, sowie Prof. Dr. med. Martin Scherer (als Projektgruppenleiter) erhalten Zugriff auf die Studiendaten (i. "Versorgungs-/Leistungsdaten" der Healthplattform, ii. KHEntgG § 21 Daten der STATAMED-Standorte, iii. durch die Projektgruppe UKE erhobene Daten aus den Qualitätszirkeln (Audio-/Videoaufnahmen, Transkripte, Protokolle)).
Die Studiendaten werden auf einem abgesicherten Datenserver des UKE gespeichert, auf den ein Zugriff nur mithilfe von personalisierten Benutzernamen und Passwörtern möglich ist. Die jeweiligen Arbeitsrechner werden mit automatischen Bildschirmsperrungen zusätzlich gesichert.

Die Räumlichkeiten des Insituts und der Poliklinik für Allgemeinmedizin des Universitätsklinikums Hamburg-Eppendorf sind mit Sicherheitsschlössern ausgestattet, sodass ein unbefugter Zutritt zu den einzelnen Büros nicht möglich ist.

Absatz zu/vom Trust Center?

Absatz zur Datenübermittlung?

Integrität:

Integrität ist gegeben, wenn personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Z.B.:

Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten

Regelmäßige Kontrolle der Aktualität

Ausschließlich die Mitarberinnen und Mitarbeiter, die im Rahmen des STATAMED Projektes angestellt sind, sowie Prof. Dr. med. Martin Scherer (als Projektgruppenleiter) erhalten Zugriff auf die Studiendaten, auf welche nur mithilfe von personalisierten Benutzernamen und Passwörtern ein Zugriff möglich ist. Der Zugriff ist somit auf Mitwirkende des STATEMED Projektes begrenzt. Die Daten werden neben dem abgesicherten Datenserver des UKE auf einem externen, passwortgeschützen Datenspeicher gesichert, welcher in einem abschließbaren Schrank aufbewahrt wird. Darüberhinaus werden die Daten regelmäßig auf ihre Aktualität überprüft. Die Rohdaten werden auf dem abgesicherten Datenserver des UKE und dem externen Speichermedium in einem anderen Ordner gespeichert, als die Auswertungsdaten, so dass eine Kontrolle der Aktualität der Daten zu jeder Zeit möglich ist. Die Rohdaten werden nicht verändert. Zur Transparenz und Nachvollziehbarkeit werden alle Arbeitsschritte des Datenmanagements nachvollziehbar dokumentiert.

Verfügbarkeit:

Verfügbarkeit ist gegeben, wenn personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Z.B.:

klare und übersichtliche Ordnung des Datenbestandes

Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

Eine klare und übersichtliche Ordnung der Datensätze wird sichergestellt. Dies soll zusätzlich mithilfe eines Datenhandbuchs gewährleistet werden. Der Zugriff auf die Daten kann nur über einen passwortgeschützen Zugang am Arbeitsplatz erfolgen. Wartungen finden außerhalb der Kernarbeitszeit statt. Somit ist die regelmäßige Verfügbarkeit gewährleistet.

Authentizität:

Authentizität ist gegeben, wenn jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können. Z.B.:

Dokumentation der Ursprungsdaten und ihrer Herkunft

Nachvollziehbarkeit der Verarbeitungsschritte

Die gesamten Datenstrukturen und Ursprünge werden in dem Datenhandbuch vermerkt. Auch werden die Rohdaten zusätzlich gespeichert s.o. Die Nachvollziehbarkeit der Verarbeitungsschritte aller Auswertungen wird mithilfe von Syntaxen oder Beschreibung der qualitativen Auswertungsmethoden inkl. Kategoriensystem sichergestellt.

Revisionsfähigkeit:

Revisionsfähigkeit ist gegeben, wenn festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Z.B.:

Festlegung klarer Zuständigkeiten und Verantwortlichkeiten

Protokollierung der Eingabe und weiteren Verarbeitung der Daten

Aufbewahrung der Protokolldaten

Alle Arbeitsschritte zur Eingabe und Verarbeitung der Daten werden durch alle Mitarbeitenden mithilfe von Syntaxen oder Methodenbeschreibungen protokoliert und in dem Datenhandbuch vermerkt. Diese Protokolldaten werden ebenfalls auf den jeweiligen Speichermedien und Servern abgesichert.

Transparenz:

Transparenz ist gegeben, wenn die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können. Z.B.:

vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge

Die Tranparenz wird sowohl durch das Datenhandbuch als auch die Dokumentation und Protokollierung der Syntaxen und Methodenbeschreibungen sichergestellt.

2. Technik des Verfahrens

2.1 ☐ Verfahren für Einzelplatzsystem

Betriebssystem: Laptop (Data Warehouse) für Trust Center (Offline)

	☐ Unix ☐ Windows NT ☐ Windows [...] ☐ anderes [...]

2.2 ☐ Client – Server - Verfahren

Client (Datenendgerät):	☐ Terminal / Netz -PC (ohne Laufwerk/Festplatten) ☒ PC (Arbeitsplatzrechner / Workstation)
Betriebssystem des Servers (z. B. Windows NT): [...]	
Client – Server Kommunikation erfolgt über	
☒ geschlossenes Netz innerhalb der Behörde (LAN) ☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises: ☐ Landesverwaltungsnetz ☐ Sonstiges ☐ offenes Netz (z. B. Internet): [...] ☐ sonstige eingesetzte Hardware (z. B. Chipkarte, Kartenlesegeräte, Videogeräte): [...]	
Datenspeicherung erfolgt auf	
☒ Server innerhalb der Behörde ☒ PC/ Arbeitsplatzrechner Art der Daten (lfd. Nr. aus Ziffer 3): [...]	☐ Server bei anderen Institutionen ☒ Sonstiges [...] Externer Datenspeicher

3. Eingesetzte Software

(einschl. Standardverfahren)	Version / Stand / Datum:
IBM SPSS Statistics	22 oder aktueller
Microsoft Office	2013 oder aktueller
MaxQda	2022

3.5. Sicherheitskonzept des Institute for Health Care Business GmbH

1. Technische und organisatorische Maßnahmen

☒ Erläuterungen zu den einzelnen Maßnahmen zur Gewährleistung der

Vertraulichkeit:

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Z.B.:

-Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern

-Benutzerkontrolle durch Passwortregelung zur Legitimation und durch automatische Bildschirmsperrung

-Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

Die Büroräume der hcb GmbH sind mit Sicherheitsschlössern versehen. Sowohl der Haupteingang zum Gebäude als auch der Eingang zum Büro sind mit Schlössern versehen, die eine zeitliche Nachvollziehbarkeit der Zu- und Abgänge gewährleisten. Zudem ist der Serverraum separat abgeschlossen.

Es haben ausschließlich die an dem Projekt beteiligten Mitarbeiterinnen und Mitarbeiter der hcb GmbH Zugriff auf die im Rahmen des Projekts erhobenen Daten. Die Daten werden in einem separaten Projektlaufwerk auf einem abgesicherten Server gespeichert, auf welchen ausschließlich über die jeweiligen Arbeitsrechner zugegriffen werden kann. Diese Arbeitsrechner sind passwortgeschützt und verfügen zusätzlich über eine automatische Bildschirmsperrung. Der Zugriff auf den Sever kann jederzeit verweigert werden.

Die Mitarbeiterinnen und Mitarbeiter wurden über die Verpflichtung zur Verschwiegenheit, zur Wahrung der Datengeheimnisse, des Sozialgeheimnisses sowie von Geschäftsgeheimnissen gemäß der gesetzlichen Vorschrift der geltenden Datenschutzbestimmungen (Datenschutz-Grundverordnung - DS-GVO sowie Bundesdatenschutzgesetz - BDSG neu) unterrichtet und haben den Erhalt der Verpflichtungserklärung unterzeichnet.

Integrität:

Integrität ist gegeben, wenn personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Z.B.:

Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten

Regelmäßige Kontrolle der Aktualität

Die Rohdaten der Studie werden nicht verändert und in einem separaten Ordner auf dem Projektlaufwerk abgespeichert. Auf dieses Projektlaufwerk haben ausschließlich die an dem Projekt beteiligten Mitarbeiterinnen und Mitarbeiter Zugriff.

Die Daten werden regelmäßig hinsichtlich ihrer Aktualität überprüft.

Verfügbarkeit:

> Verfügbarkeit ist gegeben, wenn personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Z.B.:
>
> klare und übersichtliche Ordnung des Datenbestandes
>
> Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

Eine klare und übersichtliche Ordnung des Datensatzes wird sichergestellt.

Es haben ausschließlich die an dem Projekt beteiligten Mitarbeiterinnen und Mitarbeiter Zugriff auf die im Projekt erhobenen Daten.

Authentizität:

> Authentizität ist gegeben, wenn jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können. Z.B.:
>
> Dokumentation der Ursprungsdaten und ihrer Herkunft
>
> Nachvollziehbarkeit der Verarbeitungsschritte

Die Rohdaten werden separat abgespeichert und bleiben als Datenbasis unverändert. Die aufbereiteten Daten werden regelmäßig in Versionen als Arbeitsdateien gespeichert. Erhaltene Daten werden unter Angabe des Datums in einem Verzeichnis gelistet und eine Verwendung durch Bearbeitende gekennzeichnet. Die Verarbeitungsschritte werden zusätzlich in den Arbeitsdateien dokumentiert, so dass die Nachvollziehbarkeit gewährleistet ist.

Revisionsfähigkeit:

> Revisionsfähigkeit ist gegeben, wenn festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Z.B.:
>
> Festlegung klarer Zuständigkeiten und Verantwortlichkeiten
>
> Protokollierung der Eingabe und weiteren Verarbeitung der Daten
>
> Aufbewahrung der Protokolldaten

Alle Arbeitsschritte bzgl. der Verarbeitung der Daten werden durch die Projektmitarbeiter dokumentiert. Die erhaltenen Daten werden unter Angabe des Datums in einem Verzeichnis gelistet und eine Verwendung durch Bearbeitende gekennzeichnet.

Es haben ausschließlich die an dem Projekt beteiligten Mitarbeiterinnen und Mitarbeiter Zugriff auf die im Projekt erhobenen Daten.

Transparenz:

Transparenz ist gegeben, wenn die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können. Z.B.:

vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge

Die verwendete Software ist dokumentiert. Die Datenverarbeitungsvorgänge werden vollständig und nachvollziehbar dokumentiert. Zudem existiert ein Backup-Ordner mit den ursprünglichen Daten.

2. Technik des Verfahrens

2.1 ☐ Verfahren für Einzelplatzsystem

	Betriebssystem: Laptop (Data Warehouse) für Trust Center (Offline)			
	☐ Unix	☐ Windows NT	☒ Windows 11	☒ anderes [Linus]

2.2 ☒ Client – Server - Verfahren

	Client (Datenendgerät):	☐ Terminal / Netz -PC (ohne Laufwerk/Festplatten) ☒ PC (Arbeitsplatzrechner / Workstation)
	Betriebssystem des Servers (z. B. Windows NT): Windows 2022	
	Client – Server Kommunikation erfolgt über	
	☒ geschlossenes Netz innerhalb der Behörde (LAN)	
	☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises:	
	☐ Landesverwaltungsnetz	☒ Sonstiges

	☐ offenes Netz (z. B. Internet): [...]	
	☐ sonstige eingesetzte Hardware (z. B. Chipkarte, Kartenlesegeräte, Videogeräte): [...]	
	Datenspeicherung erfolgt auf	
	☒ Server innerhalb der Behörde	☐ Server bei anderen Institutionen
	☐ PC/ Arbeitsplatzrechner	☐ Sonstiges [...]
	Art der Daten (lfd. Nr. aus Ziffer 3): [...]	

3. Eingesetzte Software

	(einschl. Standardverfahren)	Version / Stand / Datum:
	MS Excel Stata	Version 2310 oder aktueller Version 18 oder aktueller

4. Risikobewertung / Datenschutz-Folgeabschätzung (DSFA)

Bei der Durchführung des vorliegenden Forschungsvorhabens werden neben den allgemeinen Schutzzielen und Rahmenbedingungen gemäß DSGVO (Art. 35 Abs. 7 lit. c) stets die Risiken für die „Rechte und Freiheiten“ der Betroffenen (Studienteilnehmende) berücksichtigt. Im Rahmen der Vorbereitung des Forschungsprojektes wurden von den Institutionen der unabhängigen Evaluation und der wissenschaftlichen Projektbegleitung entsprechende technische und organisatorische Maßnahmen zur Risikominimierung vorgenommen.

Für den wissenschaftlichen Erfolg des STATAMED-Forschungsprojektes sind die Gewährleistung der Integrität, der Authentizität, der Vertraulichkeit und der Verfügbarkeit der erhobenen und verarbeiteten Daten sowie der datenverarbeitenden Verfahren notwendige Voraussetzung. Zu den dafür wesentlichen Aufgaben der Infrastruktur zählen:

- Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO
- Gewährleistung der Sicherheit personenbezogener Daten gemäß Abschnitt 2 DS-GVO (Art. 32-34)

Nach Risikobewertung des Studienvorhabens durch die jeweils verantwortlichen Institutionen der unabhängigen Evaluation und der wissenschaftlichen Projektbegleitung ist von einem xx Risiko sowie einer xx Eintrittswahrscheinlichkeit auszugehen. Über den bereits umgesetzten technischen und organisatorischen Maßnahmen hinaus sind daher keine weiteren Maßnahmen erforderlich.

References

1. Innovationsausschuss beim Gemeinsamen Bundesausschuss GBA. StatAMed – Transformation des Patientenpfades durch ein sektorenübergreifendes kurzstationäres allgemeinmedizinisch-orientiertes Versorgungmodell; 2023.
2. BfDI. Bürgerinnen und Bürger. Basiswissen.

Anlagen