Telemedizinisches Kompetenznetzwerk "Antibiotic Stewardship in Pediatrics"

Informationssicherheitskonzept

Version: 1.1

Datum: 07.02.2022

Autoren

Daniela Eisenschmidt-Bönn (IT-Koordinatorin)

Lukas Dubiel (IT-Beauftragter und IT-Techniker)

Freigabe und Metadaten des Konzeptes

Dokumen-tenname	IT-Sicherheits-konzept			
Seiten	41			
Schutzklasse	TeleKasper Kooperations-netzwerk			
Anhänge	7			
Status		**Version**	1.1	
Autoren	Daniela Eisenschmidt-Bönn Lukas Dubiel			
Prüfer	**Bernhard Gröhling** **ISB** Klinikum der Ludwig-Maximilian-Universität München Stabsstelle IT-Sicherheit	**Dr. Susanne Aust** **ISB** Universitätsklinikum Halle (Saale) Zentraler Dienst 16 SG Informations-sicherheit	**Frank Lorenz** **ISB** Universitäts-klinikum Essen	**Dr. Holger Carstensens** **ISB** Universitäts-klinikums des Saarlandes
Freigabe				

Inhaltsverzeichnis

Einleitung und Ziele

Das Projekt TeleKasper (Telemedizinisches Kompetenznetzwerk "Antibiotic Stewardship in Pediatrics" steht für ein auf stationäre **pädiatrische Einrichtungen** spezialisiertes „Antibiotic Stewardship“ Programm. Dafür wird ein deutschlandweites, telemedizinisches Kooperationsnetzwerk aus circa 40 pädiatrischen Kliniken aufgebaut. Vier Universitätskliniken (München, Homburg, Essen, Halle (Saale)) bilden dabei die Zentren des Netzwerkes (HUBs), welche für die infektiologische Betreuung von circa 35 weiteren Kinderkliniken in der Peripherie verantwortlich sind.

Eine speziell für das Projekt entwickelte Web- und mobile Applikation fungiert als zentrales Element des Kooperationsnetzes und wird allen Mitgliedern als **Lexikon**, **Fortbildungsmedium** und **Kommunikationswerkzeug** dienen. Hierbei werden u.a. im Rahmen von Konsiliardiensten patientenbezogene Gesundheitsdaten ausgewertet und zur Behandlungsoptimierung herangezogen.

Ziel dieses Dokumentes ist die Etablierung eines Informationssicherheitskonzeptes, welches überregional für alle Universitätskliniken, die am TeleKasper beteiligt sind, gilt. Dabei werden alle relevanten Mindestanforderungen für einen sicheren Umgang mit mobilen Anwendungen und Endgeräten definiert, um den Schutz der **Authentizität**, **Integrität, Verfügbarkeit** und **Vertraulichkeit** von Informationen zu erhöhen. Basis der hier vorgestellten Maßnahmen sind das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [1], die Informationssicherheitsrichtlinien des Universitätsklinikums Halle (Saale) (UKH) [2] und das UKH Informationssicherheitskonzept [3].

Weiterhin dient dieses Dokument als Richtlinie für alle teilnehmenden nicht-universitären Kliniken, welche durch das Patientendaten-Schutz-Gesetz (PDSG) dazu verpflichtet sind, die Anforderungen an Informationssicherheit kritischer Infrastrukturen zu erfüllen.

Geltungsbereich

Dieses Dokument ist mindestens gültig bis zum Ende des TeleKasper Projektes oder bis zum Ende der Laufzeit der hier beschriebenen und im Rahmen des Projektes etablierten Systeme. Eine Revision dieses Dokumentes ist spätestens bei einer Änderung der Rahmenbedingungen, der Gefährdungslage oder Systemarchitektur fällig.

Das IT-Sicherheitskonzept richtet sich an alle Beteiligten des TeleKasper Projektes. Dies umfasst im engeren Sinne den IT-Betrieb, die IT-Beauftragten oder IT-Sicherheitsbeauftragten der teilnehmenden Kliniken und im weiteren Sinne die Nutzer*innen der Applikation. Alle Nutzer*innen sollen sich der Notwendigkeit der Informationssicherheit und deren Ziele bewusst sein und entsprechend verantwortungsvoll handeln.

Begriffsbestimmung

Grundlegende Schutzziele der Informationssicherheit im TeleKasper sind:

Begriff	**Erklärung**
Authentizität	„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.“ [1]
Integrität	„[...] bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. [...]“ [1]
Verfügbarkeit	„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.“ [1]
Vertraulichkeit	„[...] ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ [1]

Überblick TeleKasper-Kooperationsnetzwerk

TeleKasper-Kooperationsnetzwerk

Das TeleKasper (Telemedizinisches Kompetenznetzwerk "Antibiotic Stewardship in Pediatrics") Kooperationsnetzwerk ist ein Verbund von circa 40 Universitäts- und nicht-universitären Kinderkliniken mit dem Ziel ein "Antibiotic Stewardship" Programm für die Pädiatrie zu etablieren, um den unkritischen Einsatz von Antibiotika zu reduzieren und die Entstehung multiresistenter Keime zu minimieren.

Das Netzwerk selbst besteht aus verschiedenen Ebenen (Abbildung 3). Dabei sind nicht-universitäre Krankenhäuser in regionalen Netzwerken zusammengeschlossen. Jedes dieser Netzwerke wird von einer Klinik mit Expertise im Bereich pädiatrisches Antibiotic Stewardship und Infektiologie (HUB) koordiniert. Die einzelnen HUBs wiederum sind übergeordnet in einem Verbund (Konsortium) zusammengeschlossen, in dem alle Konsortialpartner gleichberechtigt auftreten. Das Universitätsklinikum Halle (Saale) (UKH) (rot) nimmt dabei als IT-Knotenpunkt des TeleKasper Netzwerkes zusätzlich eine gesonderte Rolle ein. Neben den vier Universitätskliniken ist das Institut für Medizinische Epidemiologie, Biometrie und Informatik der Martin-Luther-Universität Halle-Wittenberg (IMEBI, gelb) ebenfalls Teil des Konsortiums. Die übergeordnete Koordination und Repräsentation aller Konsortialpartner übernimmt der Leiter des Netzwerkes, das LMU Klinikum in München (grün). Weiterer Netzwerkpartner ist die AOK Bayern, welche ausschließlich beratende Tätigkeiten übernimmt. Über die gesamte Projektlaufzeit bilden die Softwarefirma MEKmedia GmbH und Zoom Video Communications externe Vertragspartner.

Datenmanagement und Datenschutz

Da die Thematik des Datenmanagements und Datenschutzes ausführlich im Rahmen der Studienbeschreibung dargestellt ist, soll dieser Abschnitt vielmehr als Zusammenfassung dienen. Detaillierte Informationen können in weiteren Dokumenten nachgelesen werden:

- Studienprotokoll
- Verzeichnis für Verarbeitungstätigkeiten
- Stellungnahme zur datenschutzrechtlichen Zulässigkeit der Verarbeitung personenbezogener Daten

- Datenschutzrechtliche Einschätzung zur Nutzung des Videokonferenzsystems „Zoom“

Art der Daten und Datenverarbeitungstätigkeiten

Im TeleKasper Projekt müssen die Daten nach ihrer Form und der Art der Erhebung unterschieden werden. Die dazugehörigen Datenflüsse sind in den beiden untenstehenden Abbildungen graphisch skizziert.

Im Rahmen des TeleKasper Projektes werden **vier** grundlegende Arten von Daten von verschiedenen Beteiligten des Netzwerkes generiert, prozessiert und abgerufen (Abbildung 3, Abbildung 4). Die Erhebung der Daten erfolgt stets zweckgebunden und nach dem Gebot der Datensparsamkeit. Jegliche Datentransformationsprozesse sowie Datenausleitungen und -Speicherungen sind an definierte Rechte und Rollen gekoppelt (siehe Berechtigungskonzept).

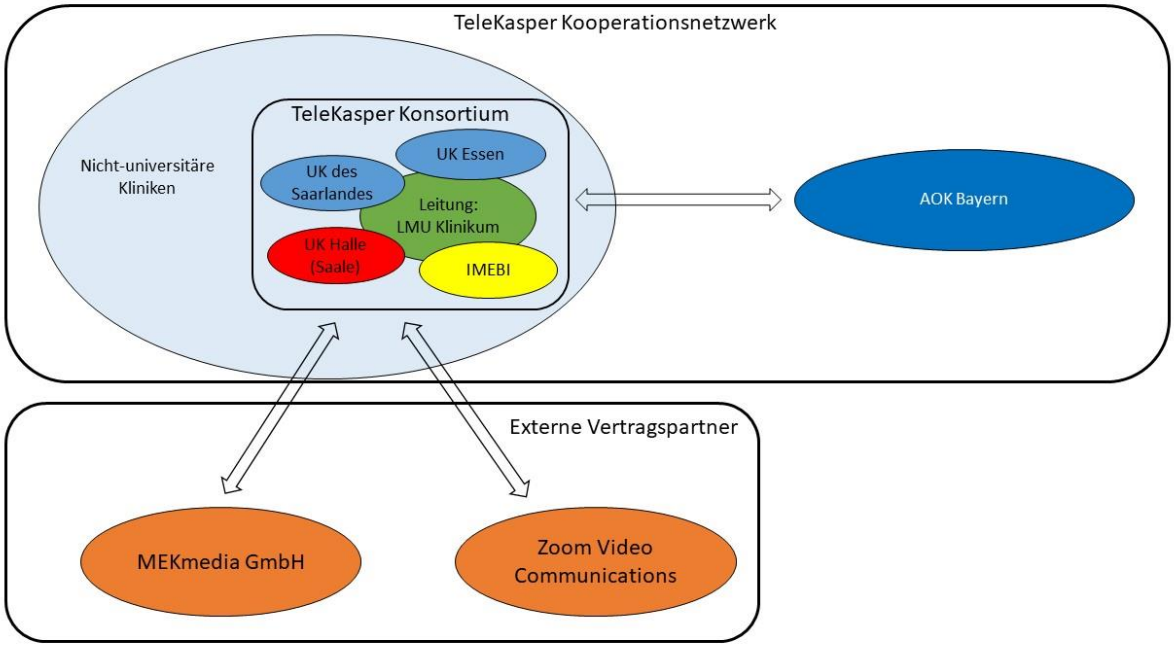

Abbildung 1: Schematische Darstellung des TeleKasper Kooperationsnetzwerkes inklusive teilnehmender externer Vertragspartner.

Art der Daten

- Pseudonymisierte patientenbezogene Gesundheitsdaten
- Pseudonymisierte personenbezogene Nutzerdaten
- Nicht-personenbezogene Daten
- Systemdaten

Art der Datenverarbeitungstätigkeiten

Pseudonymisierte patientenbezogene Gesundheitsdaten werden im Kontext eines TELE-Konsils zwischen Nutzer*innen nicht-universitärer Kliniken und Mitarbeiter*innen der HUBs über Server des UKHs transferiert (Abbildung 3, pink markierter Datenfluss). Diese Daten werden ausschließlich nach Aufklärung und Vorliegen der Einverständniserklärung erhoben. Sie werden auf Servern des UKHs gespeichert und stehen den anfragenden nicht-universitären Kliniken in aufbereiteter Form als Dokumentationsbogen für die Patientenakte zur Verfügung. Der Zugriff auf die Dokumentationsbögen beschränkt sich hierbei auf die eigenen behandelten Patienten. Die vollständige Identifikation des betreffenden Patienten ist ausschließlich durch die anfragende nicht-universitäre Klinik möglich, da dort die Patientenidentifikationslisten sicher verwahrt werden.

Infektiologisch komplexe Fälle werden in Fallkonferenzen mittels cloudbasiertem Videokonferenzsystem besprochen. Die dargestellten Patientendaten werden von der anfragenden Klinik, nach Vorliegen der Einverständniserklärung, aufbereitet und mindestens pseudonymisiert präsentiert. Alle Echtzeitdaten der Konferenz verlaufen dabei entweder direkt zwischen den Video-Endpunkten oder über Server in Deutschland. Aufzeichnungen von Konferenzen werden nur nach erfolgtem Einverständnis durchgeführt und ausschließlich auf lokalen Laufwerken gespeichert (Abbildung 4A). Erhobene Nutzerdaten werden nach datenschutzrechtlicher Aufklärung und Einverständniserklärung gespeichert. Über den Transfer der Nutzerdaten in ein Drittland (USA), welcher durch aktuell geltende EU-Standardvertragsklauseln rechtlich abgesichert wird, wird ebenfalls aufgeklärt. Die datenschutzrechtliche Freigabe des angegebenen Videokonferenzsystems (Zoom) liegt im Anhang vor.

In unabhängig von der TeleKasper Applikation und des Videokonferenzsystems regelmäßig durchgeführten Punkt-Prävalenz-Erhebungen (PPE) werden weitere patientenbezogene Gesundheitsdaten in pseudonymisierter Form erhoben (Abbildung 4B, pink markierter Datenfluss). Dies erfolgt ebenfalls nur nach vorheriger Aufklärung und Vorliegen der Einverständniserklärung. Nach Eingabe in das Umfrageprogramm LimeSurvey werden die Daten durch die verantwortlichen Hubs einer Plausibilitätskontrolle unterzogen und anschließend durch Löschung der Patientenidentifikationslisten durch die nicht-universitären Kliniken irreversibel anonymisiert. Die Speicherung der Daten erfolgt auf Servern des UKHs, die Auswertung übernimmt das Institut für medizinische Epidemiologie, Biometrie und Informatik der Martin-Luther-Universität Halle-Wittenberg (Abbildung 4B).

Weitere personenbezogene Daten werden durch alle Nutzer*innen der TeleKasper App in Form eines Profils erhoben. Prinzipiell werden diese Daten nur unter einer angelegten Arzt ID gespeichert. Die Angabe des identifizierenden Nutzernamens ist dennoch optional möglich. Die datenschutzrechtliche Aufklärung aller Nutzer findet vor dem Anlegen des entsprechenden Logins statt. Das vollständige Nutzer-Profil wird auf Servern des UKHs gespeichert. Teile der Nutzerdaten (E-Mail, Nutzer ID, Passwort) werden zur Synchronisation der Systeme auf deutschen Servern in der Microsoft Azure Cloud gespeichert. In aufbereiteter Form steht das Profil dem LMU Klinikum für die Prozessevaluation zur Verfügung, kann aber auch teilweise von der HUB-Koordination eingesehen werden (Abbildung 3, grün markierter Datenfluss). Eine Stellungnahme zur datenschutzrechtlichen Unbedenklichkeit der Microsoft Azure Cloud liegt vor. **Nicht-personenbezogene Daten** werden von den Nutzer*innen nicht-universitärer Kliniken, aber auch von den Mitarbeitern aller HUBs in Form von TELE-Infos, Feedbackfragebögen, Text- und Multimediadaten generiert und transferiert. Diese Daten liegen sowohl in der Microsoft Azure Cloud (Mandant: MEKmedia GmbH), dessen Nutzung datenschutzrechtlich begutachtet und freigegeben wurde (siehe Anlage), als auch auf Servern des UKHs (Abbildung 3, blau markierte Datenflüsse). **Aggregierte Daten**, z.B. Strukturdaten, Apothekendaten, Daten aus dem Krankenhauscontrolling und von Erreger- und Resistenzstatistiken, gelten ebenfalls als nicht-personenbezogene Daten und werden von den nicht-universitären Kliniken bereitgestellt, über Software, wie. z.B. Confluence, zentral gesammelt und auf Servern des UKHs gespeichert (Abbildung 4B, grün markierte Datenflüsse).

Systemdaten werden in Form von Updates oder im Rahmen der Prozess-und Funktionskontrolle sowohl von MEKmedia GmbH, dem Rechenzentrum am UKH (Zentraler Dienst 1, Information und Kommunikation (IuK)), als auch der TeleKasper Administration generiert und können unter Umständen die vorhandenen Datenbanken beeinflussen (Abbildung 3, grau markierte Datenflüsse).

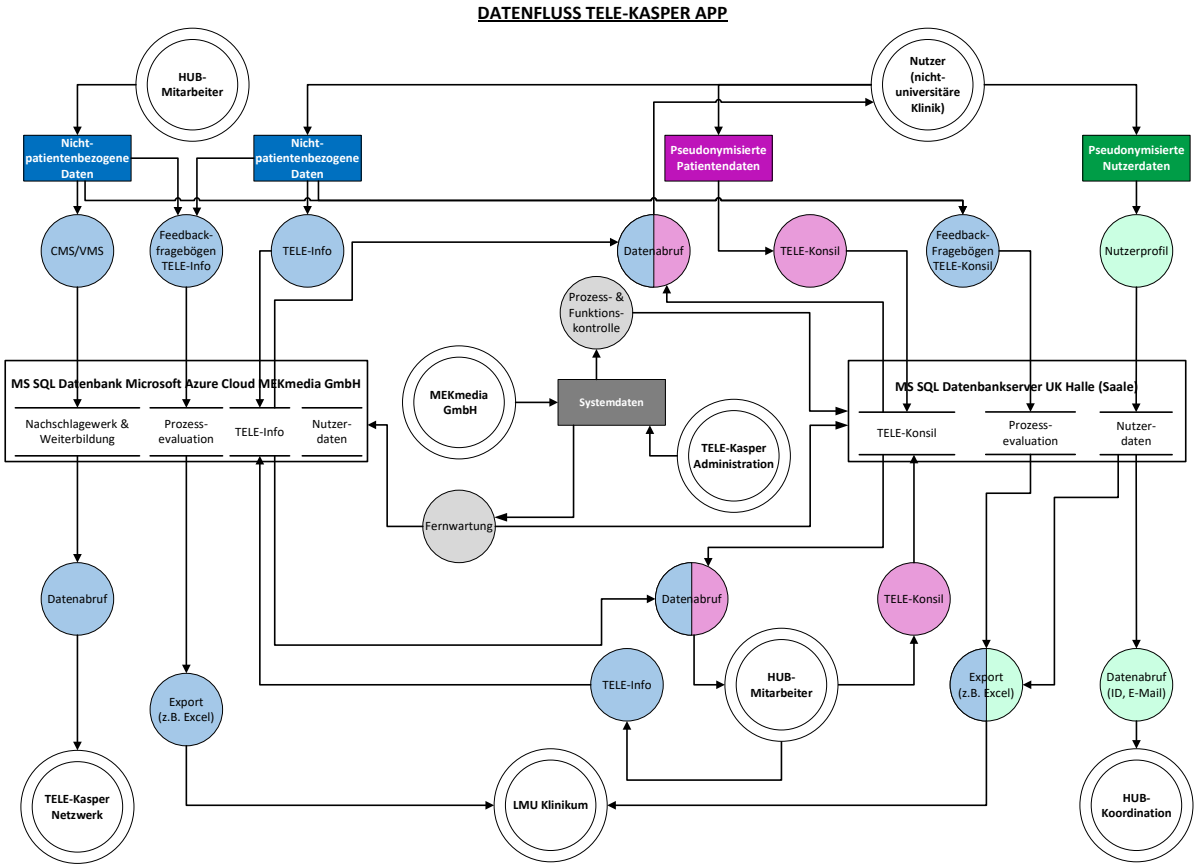

Abbildung 2: Datenflussmodell der TeleKasper App.

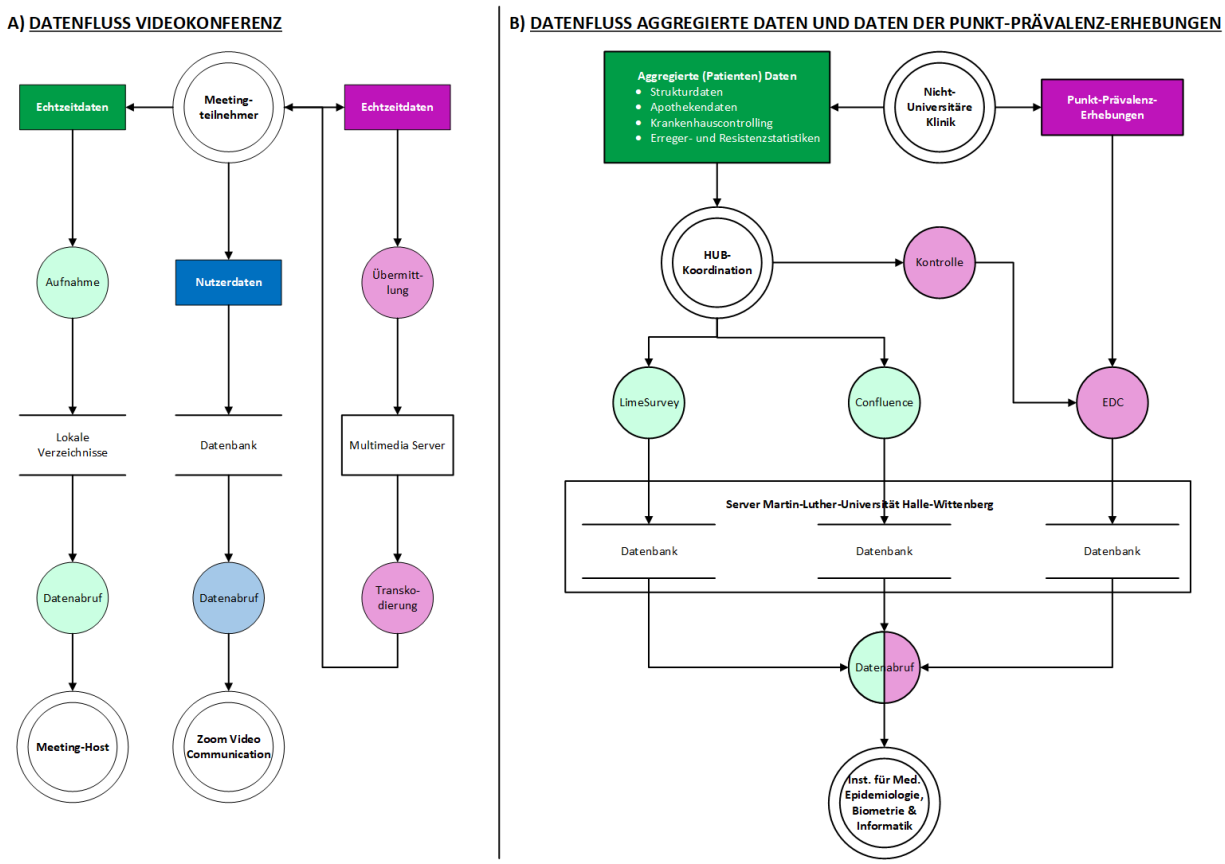

Abbildung 3: Datenflussmodell für Videokonferenzen, aggregierte Daten und Daten der Punkt-Prävalenz-Erhebungen.

Datenbereitstellung im TeleKasper Projekt

Alle bereitstehenden Daten werden manuell in die verwendeten Systeme übertragen. Es bestehen keine Schnittstellen zu existierenden Krankenhausinformationssystemen.

Zuständig- und Verantwortlichkeiten

Im Rahmen des Projektes handelt es sich um geteilte Zuständig- und Verantwortlichkeiten. Die Verantwortlichkeit für eine regelkonforme Bereitstellung der Daten liegt sowohl bei den teilnehmenden nicht-universitären Kliniken als auch bei den verantwortlichen Hubs. Eine gemäß den Richtlinien durchgeführte Aufbewahrung der Daten liegt im Verantwortungsbereich des UKHs, Zentraler Dienst 1 - Information und Kommunikation, der TeleKasper Administration und MEKmedia GmbH. Hauptverantwortlich für die Auswertung aller Daten sind das Institut für Medizinische Epidemiologie, Biometrie und Informatik (IMEBI) der Martin-Luther-Universität

Halle-Wittenberg und das LMU Klinikum. Die entsprechenden rechtlichen Grundlagen liegen durch die unterzeichneten Kooperationsverträge und Auftragsdatenverarbeitungsverträge sowie die existierenden Konsortialverträge vor.

Innerhalb der einzelnen Projektbereiche, wie der Bereich der Punkt-Prävalenz-Erhebungen und der Bereich der TeleKasper Anwendung gelten zusätzlich fest definierte Rollen, für die feste Rechte und Verantwortlichkeiten gelten. Diese werden im beigefügten Berechtigungskonzept (siehe Anhang) dargestellt. Dieses Konzept ist ausschließlich für das TeleKasper Kooperationsnetzwerk gültig und wird durch die standortspezifischen Berechtigungskonzepte der teilnehmenden Einrichtungen ergänzt.

Technische Rahmenbedingungen

Beschreibung der Systemarchitektur

TeleKasper Anwendung und Verwendung mobiler Endgeräte

Die TeleKasper App kann als native Applikation direkt aus den gängigen App-Stores bezogen und auf mobilen Endgeräten mit iOS oder Android-Betriebssystemen installiert werden. Zusätzlich steht sie als browser-basierte Anwendung für alle Standardbrowser zur Verfügung. Der Zugriff auf die App erfolgt über einen personalisierten Login (E-Mail, Passwort) nach den aktuell vom BSI empfohlenen Passwortrichtlinien [1]. Ein „Bring Your Own Device“ (Nutzen privater Endgeräte im klinik-internen Netz) ist nur dann zulässig, wenn deren Einsatz durch geeignete Sicherheitsvorkehrungen, wie z.B. ein Mobile Device Management, abgesichert ist. Der Einsatz privater Endgeräte in den teilnehmenden Kliniken muss durch die vorliegenden standortspezifischen Informationssicherheitskonzepte und -Richtlinien festgeschrieben sein, weshalb die Verantwortung, ggf. auch für den auftretenden Schaden, vollständig bei den Einrichtungen liegt.

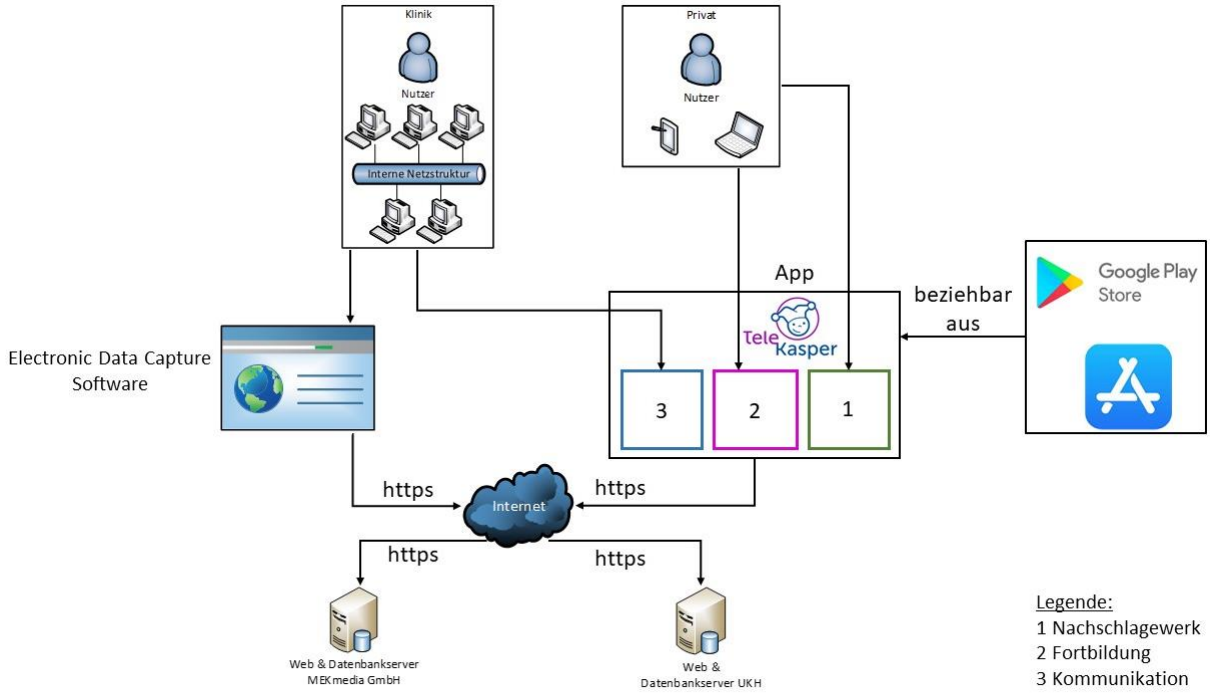

Abbildung 4: Allgemeine Systemarchitektur der TeleKasper Anwendung.

Im Rahmen der Punkt-Prävalenz-Erhebungen (PPE) werden Daten in der EDC Software LimeSurvey erhoben. Die PPE wird als Online-Umfrage mittels statischem Link und persönlichen Token zur Verfügung gestellt.

Erstellung eines Accounts für die App

Für die Generierung eines Nutzer-Accounts in der App ist sowohl die TeleKasper Administration, als auch ein definierter Verantwortlicher in jeder teilnehmenden Klinik verantwortlich. Nach Datenschutzrechtlicher Aufklärung wird die E-Mail Adresse im System hinterlegt und automatisch eine Einladung für die Applikation versendet. Diese beinhaltet einen Einmal-Token, welcher 24 Stunden gültig ist, und zur Aktivierung des Accounts benötigt wird. Nach Freischalten des Accounts kann der Nutzer ein persönliches Login generieren, welches sowohl für die Webanwendung als auch für die mobile Anwendung gültig ist.

Verwendete Serverkomponenten

Die für die TeleKasper App verwendeten Server sind an zwei Standorten lokalisiert. Nicht-personenbezogene Daten aus dem Nachschlagewerk, dem Fortbildungsmodul und der TELE-Info

werden unter der Verantwortung von MEKmedia GmbH in der Microsoft Azure Cloud gespeichert. Der dort eingesetzte Webserver besitzt neben Schnittstellen zum internen Datenbank-Server u.a. auch Schnittstellen zum eigenen Mail-Server, welcher für die Benachrichtigung der Nutzer aus diesen Teilen der App relevant ist. Der Zugriff auf diese App-Module ist aus **allen** verfügbaren Netzen möglich.
Personenbezogene Daten aus den App-Bereichen „TELE-Konsil“ und „Nutzer-Profil“ werden ausschließlich auf Servern des UKHs verschlüsselt abgelegt. Der eingesetzte Web-Server steht dabei in einer eigenen DMZ und weist Schnittstellen zum verwendeten Datenbank-Server, Mail-Server und Backup-Server auf. Der Zugriff aller Teilnehmer auf diesen Web-Server ist **ausschließlich** aus den klinik-internen Netzen möglich und wird über das Freischalten statischer, extern erreichbarer IP-Adressen der teilnehmenden Kliniken realisiert. Die für die PPE verwendeten Server stehen ebenfalls am UKH. Alle hier verwendeten Server werden durch den aktuellen Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen gesichert, welche regelmäßig von unabhängigen Prüfstellen auditiert (BSI, Juni 2021) werden. Die eingesetzten technischen und organisatorischen Maßnahmen können dem Anhang entnommen werden.

Datenverkehr und-speicherung

Der Datenverkehr zwischen allen Komponenten ist über http/https abgesichert, sodass ausschließlich die Ports 80 und 443 an der Firewall geöffnet sein müssen. Auf den eingesetzten Endgeräten verbleiben die Daten zur Bearbeitung ausschließlich im Zwischenspeicher. Bis auf den Export des TELE-Konsil Berichtes als PDF-Dokument findet keine langfristige lokale Speicherung der Daten auf den Endgeräten statt. Gemäß der dargestellten Architektur ist die Speicherung der Berichte nur auf klinikinternen Geräten möglich. Personenbezogene Daten werden auf den verwendeten Servern des UKHs in verschlüsselter Form gespeichert.

Übersicht über die Schnittstellen verwendeter IT-Systeme

Server-Lokalisation	**Schnittstellen zwischen folgenden Serverkomponenten**	
Universitätsklinikum Halle (Saale)	Web-Server	Datenbank-Server
	Web-Server	Backup-Server
	Datenbank-Server	Backup-Server
	Mail-Server	Backup-Server
	Web-Server	Öffentlichen Internet

MEKmedia GmbH	(Azure Cloud) Web-Server	Öffentliches Internet
	(Azure Cloud) Web-Server	(Azure Cloud) Mail-Server
	(Azure Cloud) Web-Server	(Azure Cloud) Datenbank-Server
	(Azure Cloud) Web-Server	(Azure Cloud) Backup-Server
	(Azure Cloud) Datenbank-Server	(Azure Cloud) Backup-Server

Backup Konzept

Für die Durchführung und Kontrolle eines ordnungsgemäßen Backups sind die Mitarbeiter des UKHs, Bereich Information und Kommunikation verantwortlich.
Die Datenbanken am UKH werden in Form eines Full-Backups täglich sowohl auf SAN Festplatten als auch extern auf Magnetbändern gespeichert. Nach dem Backup werden die auf SAN-Festplatten gespeicherten Daten sieben Tage aufbewahrt, Daten auf Magnetbändern verbleiben 10 Tage bis sie durch das nächste Full-Backup überschrieben werden. Transaktionsprotokolle werden alle 15 Minuten gespeichert.
Nicht personenbezogene Daten in der Azure Cloud von MEKmedia GmbH werden täglich auf einem Cloud Storage gesichert. Dieses Backup-Prinzip wurde bei Microsoft von autorisierten Mitarbeitern der Firma MEKmedia GmbH in Auftrag gegeben.
In den nicht-universitären Kliniken wird die Sicherung von Daten, wie z.B. den Dokumentationsbögen der TELE-Konsile oder den Patienteneinwilligungen durch deren standortspezifische Backup-Konzepte definiert und liegt vollständig in der Verantwortung der entsprechenden Einrichtung.

Schutzbedarfsfeststellung

Die Darlegung des Schutzbedarfes erfolgt für jede im TeleKasper Kooperationsnetzwerk auftretende Komponente, bezug nehmend zur zuvor erläuterten Abbildung 4. Hierfür wird eine Einschätzung des Schutzbedarfes für jede Schutzbedarfskategorie in eine der Stufen „Normal“, „Hoch“ oder „Sehr hoch“ vorgenommen. Dabei wird vornehmlich die Beeinträchtigung der Aufgabenerfüllung im Projekt betrachtet.

Anpassung der Schutzbedarfskategorien

Vertraulichkeit

„[...] ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“ [1]

Schutzbedarfsklassen für Vertraulichkeit

Klasse	**Beeinträchtigungen**
Normal	Allenfalls unerhebliche Beeinträchtigung der Abläufe. Die auf dem System verarbeiteten Daten bedürfen keines besonderen Schutzes.
Hoch	Erhebliche Beeinträchtigung der Abläufe. Es werden vertrauenswürdige Daten verschlüsselt übermittelt, wobei dies nicht immer gewährleistet werden kann.
Sehr hoch	Starke Beeinträchtigung der Abläufe. Es sind Daten involviert, die einen besonderen Schutz benötigen, wie personenbezogene Daten. Bei Preisgabe der Daten kann ein Missbrauch nicht ausgeschlossen werden.

Integrität

„[...] bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. [...]“ [1]

Schutzbedarfsklassen für Integrität

Klasse	**Beeinträchtigungen**
Normal	Allenfalls unerhebliche Beeinträchtigung der Abläufe. Die Integrität des Systems oder der Daten ist vernachlässigbar in Bezug auf die Aufgabenerfüllung. Fehler im Datensatz lassen sich leicht erkennen und beheben.
Hoch	Erhebliche Beeinträchtigung der Abläufe. Die Integrität des Systems oder Daten ist bedeutend für die Aufgabenerfüllung. Fehler im Datensatz lassen sich nur teilweise erkennen und unter Umständen nicht mehr beheben.

Sehr hoch	Starke Beeinträchtigung der Abläufe. Ein Bruch der Integrität des Systems oder der Daten kann nicht toleriert werden. Keine Möglichkeit der Fehlerfeststellung im Datensatz. Eine Behebung der Fehler ist nicht mehr möglich.

Verfügbarkeit

„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können." [1]

Schutzbedarfsklassen für Verfügbarkeit

Klasse	**Beeinträchtigungen**
Normal	Allenfalls unerhebliche Beeinträchtigung der Abläufe. Ausfallzeiten von höchstens 48 Stunden können hingenommen werden.
Hoch	Erhebliche Beeinträchtigung der Abläufe. Ausfallzeiten dürfen maximal 24 Stunden betragen.
Sehr hoch	Starke Beeinträchtigung der Abläufe. Ausfallzeiten, die über acht Stunden hinausgehen, können nicht toleriert werden.

Authentizität

„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein." [1]

Schutzbedarfsklassen für Authentizität

Klasse	**Beeinträchtigungen**
Normal	Allenfalls unerhebliche Beeinträchtigung der Abläufe. Ein Zugriff oder die Übermittlung von Daten durch unbefugte Personen oder falsche Identitäten verursacht keinen Schaden.

Hoch	Erhebliche Beeinträchtigung der Abläufe. Es muss sichergestellt werden, dass der Kommunikationspartner echt ist. Gefälschte Informationen durch falsche Identitäten lassen sich jedoch einfach herausfiltern.
Sehr hoch	Starke Beeinträchtigung der Abläufe. Bekommen unbefugte Personen Zugriff, ist die Prüfung der Echtheit der Daten so gut wie nicht möglich. Hier besteht eine große Gefahr, dass ein hoher Schaden eintritt.

Schutzbedarfsfeststellung für Anwendungen

Anwendung		**Schutzbedarfsfeststellung**		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A001	TeleKasper Anwendung (TELE-Konsil)	Vertraulichkeit	sehr hoch	Es werden vertrauliche Daten (Patientendaten) mit der Anwendung zwischen definierten Kliniken geteilt.
		Integrität	normal	Fehlerhafte Eingaben können leicht erkannt und korrigiert werden.
		Authentizität	sehr hoch	Die Eingabe und der Zugriff auf alle vertraulichen Daten muss klar definiert sein.
		Verfügbarkeit	hoch	Eine Beeinträchtigung beeinflusst ausschließlich die Zielstellung des Projektes. Die persönliche Unversehrtheit des Patienten ist nicht beeinträchtigt, da die Anwendung ausschließlich als Beratungsdienst dient. Ein Ausfall von bis zu 24 h wird toleriert.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A002	TeleKasper Anwendung (Nachschlagewerk, Fortbildung, TELE-Info)	Vertraulichkeit	normal	Es werden keine vertraulichen Daten in diesem App-Bereich geteilt.
		Authentizität & Integrität	normal	Fehlerhafte Daten können leicht erkannt und korrigiert werden.
		Verfügbarkeit	normal	Eine Beeinträchtigung beeinflusst ausschließlich die Zielstellung des Projektes. Ein Ausfall von mehr als 24 h wird toleriert.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A003	LimeSurvey	Vertraulichkeit	Sehr hoch	Es werden vertrauliche Daten (Patientendaten) mit der Anwendung zwischen definierten Kliniken geteilt.
		Authentizität & Integrität	hoch	Fehlerhafte Daten können nicht erkannt und korrigiert werden. Falsche Informationen können zu einem verfälschten Ergebnis des Projektes führen.
		Verfügbarkeit	normal	Daten lassen sich über andere Wege (Anwendungen, Papierformulare) zwischenspeichern. Ein Nachtrag der Daten ist jederzeit durchführbar. Der Abruf der gespeicherten Daten ist auch anderweitig möglich.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Nr.	Bezeichnung	
A004	Confluence	Vertraulichkeit	normal	Zwar werden unter Umständen auch vertrauliche Dokumente mit den Anwendungen angefertigt, die Anwendung selber hat dadurch jedoch noch keinen hohen Schutzbedarf bezüglich Vertraulichkeit.
		Authentizität & Integrität	normal	Fehlerhafte Daten können leicht erkannt und korrigiert werden.
		Verfügbarkeit	normal	Daten lassen sich über andere Wege (Anwendungen, Papierformulare) zwischenspeichern. Da hier keine zeitkritischen Daten vorliegen, ist ein Abruf nach max. 48 h vertretbar.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
A005	Datenbank-Software	Vertraulichkeit	Sehr hoch	Es werden vertrauliche Daten verarbeitet.
		Authentizität & Integrität	Sehr hoch	Vertrauliche Daten werden in der Datenbank gespeichert. Ein Fehler bei der Übertragung der Daten lässt sich nicht erkennen und dementsprechend nicht korrigieren.
		Verfügbarkeit	hoch	Daten werden in der Software gespeichert und wieder zum Abruf bereitgestellt. Ein Ausfall würde das Projekt funktionsunfähig machen.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Nr.	Bezeichnung	Nr.
A006	Microsoft Outlook	Vertraulichkeit	hoch	Es gibt zwar eine Betriebsvereinbarung, gemäß der es untersagt ist, vertrauliche Daten unverschlüsselt zu versenden. Dies kann jedoch bei extern eingehender E-Mail nicht kontrolliert werden. Daher ist der Schutzbedarf als hoch zu bewerten.
		Authentizität & Integrität	hoch	E-Mails müssen vor Fälschungen geschützt werden.
		Verfügbarkeit	hoch	Sowohl interne als auch ein Teil der projektrelevanten Kommunikation erfolgt über E-Mail. Ein Ausfall ist daher maximal 24 h akzeptabel.

Schutzbedarfsfeststellung für IT-Systeme

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
S001	Web-Server UKH (virtualisiert)	Vertraulichkeit	Sehr hoch	Maximumprinzip gemäß Anwendung A001.
		Authentizität & Integrität	hoch	Es gilt das Maximumprinzip, da zu Grunde liegende Hardware durch mehrere virtuelle Maschinen geteilt wird, aber ohne unmittelbaren Kontakt zur Primärversorgung. Verarbeitete Daten können im Nachhinein nur teilweise wieder korrigiert werden.
		Verfügbarkeit	hoch	Eine Beeinträchtigung beeinflusst ausschließlich die Zielstellung des Projektes. Die persönliche Unversehrtheit des Patienten ist nicht beeinträchtigt, da die Anwendung ausschließlich als Beratungsdienst dient. Ein Ausfall von bis zu 24 h wird toleriert.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
S002	Virtualisierungs-Server	Vertraulichkeit	Sehr hoch	Maximumprinzip gemäß Anwendung A001.
		Authentizität & Integrität	hoch	Es gilt das Maximumprinzip, da zu Grunde liegende Hardware durch mehrere virtuelle Maschinen geteilt wird, aber ohne unmittelbaren Kontakt zur Primärversorgung.
		Verfügbarkeit	hoch	Teilung der Server-Hardware mit anderen Projekten/ Bereichen. Da hier nicht die Primärversorgung betroffen ist, ist die Verfügbar nur auf hoch anzusetzen.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
S003	Datenbank-Server UKH	Vertraulichkeit	Sehr hoch	Es gilt das Maximumprinzip, da zu Grunde liegende Hardware durch mehrere DB-Instanzen geteilt wird, mit unmittelbaren Kontakt zur Primärversorgung.
		Authentizität & Integrität	Sehr hoch	Maximumprinzip gemäß A005.
		Verfügbarkeit	hoch	Maximumprinzip gemäß A005. Teilung der Speicherbereiche der Datenbank mit der Primärversorgung.
S004	Mail-Server UKH	Vertraulichkeit	hoch	Maximumprinzip gemäß A006.
		Authentizität & Integrität	hoch	Maximumprinzip gemäß A006.
		Verfügbarkeit	hoch	Maximumprinzip gemäß A006.
S005	Backup-Server UKH	Vertraulichkeit	Sehr hoch	Identisches System wird für Backup vertraulicher Daten eingesetzt.
		Authentizität & Integrität	Sehr hoch	Alle Daten müssen wahrheitsgemäß gesichert werden. Ein Fehler beim Generieren der Backups kann im Nachhinein nicht korrigiert bzw. nachvollzogen werden.
		Verfügbarkeit	Sehr hoch	Bei einem totalen Datenausfall müssen die Daten umgehend zur Verfügung stehen.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
S006	Web-Server MEKmedia GmbH	Vertraulichkeit	hoch	Cloudbasierte Lösung. Der Teil der TeleKasper Anwendung beinhaltet keine vertrauenswürdigen Daten. Es werden jedoch Benutzernamen und Passwörter gespeichert, wobei die Passwörter verschlüsselt abgelegt werden.
		Authentizität & Integrität	normal	Cloudbasierte Lösung. Ausschließlich nicht-personenbezogene Daten werden damit in die DB geschrieben. Ein Fehler in den Daten kann einfach behoben werden. Ein fremder Zugriff verursacht keinen Schaden, da die Passwörter verschlüsselt vorliegen.
		Verfügbarkeit	hoch	Eine Beeinträchtigung beeinflusst ausschließlich die Zielstellung des Projektes Da jedoch auf dem Web-Server Teile der TeleKasper App liegen, würde somit die App nicht voll funktionsfähig sein. Ein Ausfall von mehr als 24 h wird toleriert.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzwert	Begründung
S007	Datenbank-Server MEKmedia GmbH	Vertraulichkeit	hoch	Cloudbasierte Lösung. Es werden keine vertraulichen Daten auf diesem Server abgelegt. Passwörter liegen verschlüsselt vor. Da auf dem Datenbank-Server in der Datenbank unter anderem Anmeldedaten liegen, die teilweise verschlüsselt sind, wird hier die Vertraulichkeit auf hoch gesetzt.
		Authentizität & Integrität	normal	Cloudbasierte Lösung. Fremde Zugriffe auf das System würden einen geringen Schaden für das Projekt verursachen, da nur Zugriff auf nicht personenbezogene Daten möglich ist.
		Verfügbarkeit	hoch	Eine Beeinträchtigung beeinflusst ausschließlich die Zielstellung des Projektes. Da jedoch auf dem Web-Server Teile der TeleKasper App liegen, würde somit die App nicht voll funktionsfähig sein. Ein Ausfall von mehr als 24 h wird toleriert.
S008	Mail-Server MEKmedia GmbH	Vertraulichkeit	hoch	Maximumprinzip gemäß A006.
		Authentizität & Integrität	hoch	Maximumprinzip gemäß A006.
		Verfügbarkeit	hoch	Maximumprinzip gemäß A006.

Anwendung		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
S009	Backup-Server MEKmedia	Vertraulichkeit	hoch	Cloudbasierte Lösung. Es werden keine personenbezogenen Daten gesichert. Da auf dem Backup-Server unter anderem Anmeldedaten liegen, die teilweise verschlüsselt sind, wird hier die Vertraulichkeit auf hoch gesetzt.
		Authentizität & Integrität	hoch	Cloudbasierte Lösung. Daten müssen wahrheitsgemäß gesichert werden. Da hier die Prozesse automatisiert ablaufen, können später generierte Fehler nicht im Nachhinein korrigiert werden.
		Verfügbarkeit	hoch	Bei akutem Datenverlust müssen die Daten in einem Zeitraum von max. 24 h wiederhergestellt werden. Ein Verlust führt zur signifikanten Beeinträchtigung des Projektes, was sich in einer nur teilweise funktionierenden App darstellen würde.

Schutzbedarfsfeststellung für Kommunikationsverbindungen

Anwendung		**Schutzbedarfsfeststellung**		
Nr.	Bezeichnung	Grundwert	Schutzbedarf	Begründung
K008	Öffentliches Netz (Internet)	Vertraulichkeit	normal	Alle personenbezogenen Daten werden verschlüsselt transportiert.
		Authentizität & Integrität	normal	Die Kommunikation erfolgt über das Internet. Gefälschte Informationen beeinflussen das Ziel des Projektes. Geänderte oder gefälschte Daten lassen sich zum größten Teil erkennen und beheben.
		Verfügbarkeit	Sehr hoch	Ein Ausfall von >24 h würde das Ergebnis der Studie signifikant beeinflussen. Während der Ausfallzeit kann die App nicht genutzt werden.

K008	Klinikinterne Netz	Vertraulichkeit	Sehr hoch	Da Systeme der Primärversorgung angeschlossen sind und Patientendaten übertragen werden.
		Authentizität & Integrität	Sehr hoch	Informationen müssen zuverlässig und wahrheitsgetreu transportiert werden. Fehler in der Datenverarbeitung können aufgrund der hohen Datenmengen nicht einfach behoben werden.
		Verfügbarkeit	Sehr hoch	Bei einem Ausfall des klinikinternen Netzes ist eine medizinische Versorgung nur durch einen sehr hohen Aufwand zu kompensieren. Zusätzlich ist die Funktionalität der App stark eingeschränkt.

IT Grundschutz im TeleKasper

Allgemeine Anforderungen

Allgemeingültige Anforderungen können aus den jeweils geltenden Gesetzestexten abgeleitet werden.

Anforderungen	**Vorgaben**
"angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse [...] treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."	BSIG §8a Abs. 1
Grundsätze für die Verarbeitung personenbezogener Daten.	DSGVO Art. 5
Sicherheit der Verarbeitung.	DSGVO Art. 32

Anzuwendende Vorgaben

Auszugsweise werden im folgenden einige ggf. zu beachtende gesetzliche Regelungen genannt:

- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) [4]
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) [5]
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-Kritis V) [6]
- Datenschutz-Grundverordnung (DSGVO) [7]
- Branchenspezifischer Sicherheitsstandard (B3S) für Krankenhäuser Version 1.1 [8]

Neben den oben genannten Regelungen müssen ggf. auch noch weitere Gesetze auf Landesebene berücksichtigt werden:

- Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NW) [9]

- Krankenhausgesetz Sachsen-Anhalt (KHG LSA) [10]
- Saarländisches Krankenhausgesetz (SKHG) [11]
- Krankenhausgesetz des Landes Nordrhein-Westfalen (KHG NRW) [12]
- Bayerisches Krankenhausgesetz (BayKrG) [13
- Landeskrankenhausgesetz (LKG) [14]

Auch sollten am jeweiligen Standort die übergeordneten Regelungen wie z.B. Betriebsvereinbarungen, Richt- und Leitlinien berücksichtigt werden.

Risikoeinschätzung

Die Basis- und Standard-Anforderungen der relevanten Bausteine des IT-Grundschutzkompendiums sind für die einzelnen Komponenten erfüllt. Jede teilnehmende Klinik ist dazu verpflichtet die gesetzlichen Auflagen zu erfüllen und durch geeignete technische und organisatorische Maßnahmen die Sicherheit aller Informationen zu maximieren. Hausinterne Informationssicherheitsrichtlinien und -Konzepte spezifizieren diese Anforderungen. Da alle im TeleKasper verwendeten Komponenten bereits in diese Infrastrukturen integriert sind, ist das Risiko für einen potentiellen Informationssicherheitsvorfall bestmöglich minimiert. Die über Microsoft Azure angebotenen Dienste erfüllen ebenfalls die internationalen Zertifizierungsnormen für Informationssicherheitsmanagementsysteme und den Schutz von personenbezogenen Daten in Public Clouds (ISO 27001, ISO 27018). Zusammen mit den umgesetzten technischen und organisatorischen Maßnahmen von MEKmedia GmbH zum Schutze der Daten kann das Risiko für einen Vorfall auch als minimal eingestuft werden.

IT-Sicherheitsrichtlinien TeleKasper

Nachfolgende Gefährdungslagen und Vorkehrungen wurden für das TeleKasper Projekt abgeleitet. Die Vorkehrungen sollten soweit im eigenen standortspezifischen IT-Sicherheitskonzept (bzw. daraus resultierenden IT-Sicherheitsrichtlinien) beachtet werden, sofern diese im entsprechenden Klinikum Anwendung finden. Die ausführlichen Beschreibungen der einzelnen Punkte sind folgenden Kapiteln des IT-Grundschutz-Kompendiums (Edition 2021) zu entnehmen:

- 2.1 Allgemeiner Client
- 3.1 Laptops

- 3.2.1 Allgemeine Smartphones und Tablets
- 3.2.3 iOS (for Enterprise)
- 3.2.4 Android
- 1.2 Webbrowser
- 1.4 Mobile Anwendungen
- 9 Mobiler Arbeitsplatz

Stationäre und mobile Endgeräte

Allgemeingültige Gefährdungslagen:

- Schadprogramme
- Datenverlust durch lokale Datenhaltung
- Hardware-Defekte
- Manipulation und unberechtigte Nutzung
- Installation nicht benötigter Betriebssystemkomponenten und Applikationen
- Fehlerhafte Administration oder Nutzung von Geräten und Systemen
- Fehlende Updates für Firmware, Betriebssystem und Anwendungen
- Software-Schwachstellen in vorinstallierten Anwendungen (Apps)
- Abhören von Räumen mittels Mikrofon und Kamera

Neben den allgemeinen Gefährdungslagen sind noch weitere spezifische Gefährdungen je nach Endgerät zu nennen:

Zusätzliche Gefährdungslagen für mobile Endgeräte:

- Beeinträchtigung durch Benutzerwechsel und wechselnde Einsatzumgebung
- Diebstahl und Verlust
- Webbasierte Angriffe auf mobile Browser
- Missbrauch von Ortungsdaten
- Missbrauch schutzbedürftiger Daten im Sperrbildschirm
- Rechteerhöhung durch Schwachstellen
- Gefahren durch private Nutzung dienstlicher mobiler Endgeräte
- Gefahren durch Bring Your Own Device (BYOD)

Folgende Vorkehrungen minimieren das Risiko eines Informationssicherheitsvorfalles durch oben genannte Gefährdungslagen.

Allgemeine Vorkehrungen:

- Die Anmeldung am Endgerät muss mit einer Benutzerkennung erfolgen.
- Es müssen Bildschirmsperren eingerichtet werden. Diese müssen bei Benutzerinaktivität nach einer angemessenen Zeit, in Abhängigkeit des Schutzniveaus (z.B. 10 min), automatisch den Bildschirm wieder sperren. Für die Entsperrung muss ein Gerätecode oder ein Kennwort eingetragen werden. Wird das Endgerät durch den Benutzer nicht mehr genutzt, so muss er sich vom diesem abmelden.
- Es dürfen nur Firmware, Betriebssysteme und Anwendungen (Apps) installiert werden, die Sicherheitsupdates unterstützen.
- Auto-Updates müssen im Bereich der Firmware, Betriebssystem und Anwendungen (Apps) aktiv sein. Ist dies nicht möglich, so müssen die Updates manuell eingespielt werden (manuelle Wartung oder zentrales Verteilungssystem).
- Es muss ein Schutzprogramm gegen Schadsoftware zum Einsatz kommen. Das Schutzprogramm soll dabei die Änderungen der sicherheitsrelevanten Einstellungen durch den Benutzer blockieren und die Daten beim Datenaustausch und Datentransfer überprüfen.
- Um Manipulationen zu vermeiden, müssen Boot-Vorgänge abgesichert werden. Des Weiteren dürfen Administratoren nur Zugriff auf das BIOS des Endgerätes besitzen. Im BIOS selbst müssen mindestens unnötige Funktionen deaktiviert sein.
- Für den regulären Betrieb nicht notwendige Cloud- und Online-Funktionen auf Betriebssystem- und Anwendungsebene (z.B. Cloudspeicherdienste, OneDrive, integrierte Online-Suche in Betriebssystemen) sind zu deaktivieren.
- Endgeräte dürfen nur verschlüsselt kommunizieren. Die verwendeten kryptischen Algorithmen und Schlüssellängen müssen dem Stand der Technik entsprechen.
- Nicht benötigte Schnittstellen und Programme müssen deaktiviert bzw. deinstalliert werden. Ein eingeschränkter Zugriff auf externe Schnittstellen zum Endgerät wird empfohlen.
- Werden externe Datenträger verwendet, so müssen diese aus einer vertrauenswürdigen Quelle stammen.
- Das Ausführen von Programmen und Skripten sollte durch „Whitelists“ geregelt sein.

- Mehrfach fehlerhafte Eingabe des Passwortes muss zur Sperrung des Gerätes führen.
- Bei Diebstahl oder Verlust des Gerätes, muss der Mitarbeiter dies umgehend den Zuständigen melden.
- Aufgefundene mobile Geräte müssen auf Manipulation und Änderungen untersucht werden. Aus Sicherheitsgründen muss das System (Betriebssystem inkl. eingesetzter Software) komplett neu aufgesetzt werden.

Zusätzliche Vorkehrungen für mobile Endgeräte:

- Einsatz- und Nutzungszweck der Geräte müssen genau definiert sein.
- Zuweisung der Endgeräte zu einem Nutzer muss nachvollziehbar sein.
- Die mobile Nutzung der Endgeräte muss durch eine aktive, möglichst restriktiv arbeitende Firewall gesichert sein. Mögliche Warnmeldungen durch die Firewall sind für Benutzer in verständlicher Sprache darzustellen.
- Die Kommunikation über öffentliche Netze darf nur über einen sicheren Kommunikationskanal ablaufen.
- Die Administration und Verwaltung mobiler Endgeräte muss zentral durchgeführt werden. Hier ist darauf zu achten, dass alle verwendeten Betriebssysteme unterstützt werden.
- Ist eine Nutzung im privaten Bereich vorgesehen, so muss dies genau definiert sein. Privat- und Arbeitsumgebung müssen dabei voneinander getrennt werden.
- Die Grundkonfiguration der Endgeräte sollte durch geeignete Schutzmechanismen und Einstellungen bereits ein angemessenes Schutzniveau erfüllen.
- Sperrbildschirme dürfen keine vertraulichen Informationen anzeigen. Dies muss deaktiviert werden.
- Codes zum Entsperren des Gerätes und Passwörter sollten sich nicht nach kurzer Zeit wiederholen.
- Geräte ohne Sicherheitsupdates durch den Hersteller müssen ausgesondert werden.
- Zugriffe auf Kamera, Mikrofon und Ortungsdaten muss den organisationsinternen Datenschutz- und Sicherheitsvorgaben entsprechen.
- Sicherheitsrelevante Berechtigungseinstellungen dürfen nicht durch den Benutzer geändert werden. Liegen dazu keine technischen Maßnahmen vor, so muss dies regelmäßig geprüft werden.

- Es muss geregelt werden, welche Apps und Quellen der Benutzer verwenden darf. Nicht zugelassene Quellen müssen dazu blockiert werden.
- Eine Firewall sollte auf den Endgeräten installiert werden.

Mobile Betriebssysteme, Anwendungen und Webbrowser

Betriebssysteme

Gefährdungslagen für iOS Betriebssysteme:

- Risikokonzentration durch ein Benutzerkonto (Apple-ID) für alle Apple-Dienste
- Feste Integration von vorinstallierten Apps und deren Funktionen
- Missbräuchlicher Zugriff auf ausgelagerte Daten

Vorkehrungen für iOS Betriebssysteme:

- Kommt ein MDM-System zum Einsatz, so müssen die iOS Endgeräte darüber verwaltet werden. Aspekte wie Auswahl der Endgeräte, Datensicherung und Apps von Drittanbietern sind hier zu berücksichtigen. Auch sollte hier sichergestellt werden, dass sich die iOS Endgeräte nur mit diesem MDM-System verbinden.
- Es muss definiert werden, welche Cloud-Dienste zugelassen werden. Unnötige Funktionen und Dienste sind einzuschränken oder zu deaktivieren.
- Zur Registrierung der iOS Endgeräte sollte überprüft werden, ob dazu der Apple Business Manager verwendet werden kann.
- Das Löschen der Konfigurationsprofile muss durch organisatorische und technische Maßnahmen verhindert werden.
- Für Konfigurationsprofile sollte ein angemessener Wert bis zur ersten Codewiederholung festgelegt werden.
- Ist ein iOS Endgerät einen definierten Zeitraum offline, so sollte dies ohne externes Zutun die Konfigurationsprofile löschen.

Gefährdungslagen für Android Betriebssysteme:

- Deaktivieren von Sicherheitsfunktionen
- Schadsoftware für das Android-Betriebssystem

- Fehlende Updates für das Android-Betriebssystem
- Risiko durch Benutzerkonten (Google-ID) für Google-Dienste
- Vorinstallierte Apps und integrierte Funktionen bei Android-basierten Geräten

Vorkehrungen für Android Betriebssysteme:

- Es sollte die Entwicklerumgebung deaktiviert werden.
- Sicherheits-Apps sollten sich als „Trusted Agent" oder Geräteadministrator eintragen lassen.
- Zugriff auf Benutzerdaten sollte nur durch erlaubte Apps möglich sein.
- Es sollte überprüft werden, ob eine Multi-User-Mode verwendet werden soll. Dies wird empfohlen, wenn mehrere Benutzer sich ein Android Endgerät teilen.

Mobile Anwendungen

Gefährdungslagen für mobile Anwendungen:

- Ungeeignete Auswahl von Apps
- Zu weitreichende Berechtigungen
- Ungewollte Funktionen in Apps
- Software-Schwachstellen und Fehler in Apps
- Unsichere Speicherung lokaler Anwendungsdaten
- Ableitung vertraulicher Informationen aus Metadaten
- Abfluss von vertraulichen Daten
- Unsichere Kommunikation mit Backend-Systemen
- Kommunikationswege außerhalb der Infrastruktur der Institution

Vorkehrungen für mobile Anwendungen:

- Kontroll- und Einflussmöglichkeiten müssen auf Betriebssystemebene gegeben sein.
- Sicherheitsrelevante Einstellungen dürfen nur durch den Administrator oder das Fachpersonal geändert werden. Sollte dies nicht möglich sein, müssen die Einstellungen geprüft und neu gesetzt werden.
- Neue Apps dürfen nur die notwendigen Berechtigungen besitzen. Alle anderen sind der jeweiligen App zu entziehen.

- Wird mit der App auf interne Dokumente des Unternehmens zugegriffen, so muss die lokale Datenhaltung der App abgesichert werden.
- Zugriffsschlüssel sind in der App verschlüsselt zu speichern.
- Eine Auslagerung von vertraulichen Daten durch das Betriebssystem auf andere Speicherorte darf nicht erfolgen.
- Die App-Kommunikation muss soweit eingeschränkt werden, das keine Daten mit vertraulichen Inhalten versendet oder Profile über den Benutzer erstellt werden. Dies muss in einem Test- und Freigabeverfahren geprüft werden.
- Protokollierungs- und Hilfsdateien der App sollten auf vertrauliche Inhalte geprüft werden.

Webbrowser

Gefährdungslagen für Webbrowser:

- Ausführung von Schadcode durch Webbrowser
- Exploit Kits - Individuelle automatisierbare Schadsoftware
- Mitlesen der Internetkommunikation
- Integritätsverlust in Webbrowsern
- Verlust der Privatsphäre

Vorkehrungen für Webbrowser:

Folgende Punkte und Funktionen **muss** der Webbrowser beinhalten:

- Die Unterstützung von Content Security Policy, Same-Origin-Policy und Subresource
- Unterstützung von TLS (Transport Layer Security) und HTTP Strict Transport Security (HSTS)
- Deaktivierungsmöglichkeit von unsicheren TLS Versionen.
- Verwaltung von eigenen Wurzelzertifikaten nur durch autorisiertes IT-Personal
- Widerrufen von Zertifikaten
- Prüfung auf Gültigkeit und Sperrstatus der Zertifikate
- Signalisierung bei fehlenden, ungültigen oder widerrufenen Zertifikaten
- Verbindungsaufbau bei problematischen Zertifikaten nur nach Benutzerbestätigung
- Die Nutzung des Kennwort-Mangers im Webbrowser muss unterbunden werden

- Prüfung, ob DNS-Over-HTTPS (DoH) unterstützt wird. Benutzung von DoH bei nicht vertrauenswürdigen Netzen.

Neben den Muss-Kriterien sind **weitere** Aspekte zur Erhöhung der Datensparsamkeit des Benutzers **sinnvoll**, die einen erweiterten Schutz bieten:

- Sperrung von Cookies, die seitenübergreifende Aktivitäten verfolgen
- Möglichkeit zur Deaktivierung oder Löschung der Autovervollständigung im Webbrowser
- Deaktivierung von Cloud-Diensten
- Verwendung von Mikrofon und Webcam, nur wenn es notwendig ist
- Möglichkeit zur Deaktivierung und Konfiguration von WebRTC, HSTS und JavaScript
- Löschung von lokalen Webbrowserdaten, nach dem Beenden
- Prüfung der Internetseiten auf schädliche Inhalte durch den Webbrowser
- Blockierung des Verbindungsaufbaus bei schädlichen Verbindungen

Passwortrichtlinie

- Es sind ausschließlich individuelle Kennungen und Passwörter zu verwenden. Jeder Benutzer erhält ein eigenes Passwort, das nur von ihm benutzt werden darf. Passwörter, die von mehreren Personen benutzt werden (Gruppenpasswörter), sind nicht zulässig.
- Ein Passwort ist geheim zu halten. Es darf nirgendwo aufgeschrieben und keiner anderen Person mitgeteilt werden. Wenn möglich, sollte ein externer Passwortmanager verwendet werden.
- Triviale Passwörter sind zu vermeiden.
- Ein Passwort muss aus mindestens acht Zeichen bestehen.
- Innerhalb des Passworts sollte mindestens ein Sonderzeichen enthalten sein. Es sollten sowohl Groß- als auch Kleinbuchstaben sowie Ziffern in Verwendung sein (4 aus 4 Kriterien-Regel).
- Ein Passwort darf bei der Eingabe nicht am Bildschirm angezeigt werden.
- Eine Speicherung von Passwörtern darf nur verschlüsselt durchgeführt werden.
- Initial vergebene Passwörter müssen auf sicherem Wege dem Benutzer mitgeteilt werden. Der Benutzer muss nach der ersten Anmeldung aufgefordert werden sein Passwort zu ändern.

- Ein Passwort ist regelmäßig zu ändern und das neue Passwort sollte sich von den früher verwendeten unterscheiden (Wiederverwendung vermeiden durch Ausschluss von (z.B. 5) Passwortgenerationen).
- Ein Passwort muss umgehend geändert werden, wenn der Verdacht besteht, dass es einer anderen Person bekannt wurde.
- Passwort-Änderungen müssen von den jeweiligen Benutzern selbst durchgeführt werden können.
- Nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung muss die Kennung mindestens temporär für die weitere Benutzung gesperrt werden.
- Alle Passwörter von System- oder Anwendungssoftware, die vom Hersteller voreingestellt wurden, sind nach der Installation des Systems umgehend zu ändern.

Nutzung von mobilen Arbeitsplätzen

Gefährdungslagen:

- Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze
- Beeinträchtigung durch wechselnde Einsatzumgebung
- Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz
- Verzögerungen durch temporär eingeschränkte Erreichbarkeit
- Ungesicherter Akten- und Datenträgertransport
- Ungeeignete Entsorgung der Datenträger und Dokumente
- Vertraulichkeitsverlust schützenswerter Informationen
- Diebstahl oder Verlust von Datenträgern oder Dokumenten

Vorkehrungen:

- Für einen sicheren Arbeitsplatz müssen Arbeitsbedingungen definiert werden, die sich aus den hausinternen Richtlinien ableiten. Bei nicht vorhandenen Richtlinien müssen diese definiert werden.
- Es muss geregelt sein, wer Daten transportieren und bearbeiten darf und wie dies durchzuführen ist

- Bei starken Benutzerwechsel am Endgerät, müssen feste Regelungen definiert und der Benutzerwechsel nachvollzogen werden können. Dies muss in einem Berechtigungskonzept definiert sein.
- Durch die erhöhte Gefahr des Diebstahls oder des nicht autorisierten Zugriffs, sollten gesonderte Richtlinien im Punkt Sicherheit definiert werden. Mitarbeiter müssen durch regelmäßige Schulungen dafür sensibilisiert werden. Ein Einblick in die Richtlinien muss möglich sein. Mitarbeiter müssen über die Risiken bei der Verwendung mobiler Endgeräte und die erhöhte Sorgfalts- und Achtsamkeitspflicht sensibilisiert werden.

Implementierungsvorgaben

Dieses Konzept gilt ausschließlich für alle im TeleKasper Projekt einbezogenen Personen und Komponenten und kann keinesfalls als alleinstehendes Informationssicherheitskonzept einer einzelnen Klinik angesehen werden. Um alle vor Ort geltenden Vorgaben abzudecken, muss deshalb jedes Haus ein unabhängiges, individuelles Konzept erstellen. Hierzu sollten die jeweiligen Standorte eng mit ihren eigenen Partnern und Abteilungen zusammenarbeiten, die Hard- und Software bereitstellen oder diese verwalten und konfigurieren.

Darlegung der Restrisiken

Zusammenfassend kann das für das TeleKasper Projekt bestehende Restrisiko als gering eingestuft werden. Um das Restrisiko der einzelnen teilnehmenden Kliniken darzulegen, muss für alle Hard- und Softwarekomponenten der Häuser, deren Partner und evtl. Eigenentwicklungen eine geeignete Risikoanalyse eingefordert oder erstellt werden. Diese geeigneten Risikoanalysen lassen sich im Rahmen des für alle Kliniken vorgeschriebenen Betriebes eines Informationssicherheits-Managementsystems (ISMS) oder einer Zertifizierung zum Beispiel nach ISO27001 (Informationssicherheits-Managementsystems), nach BSI Grundschutz oder nach ISO31000 (einfache Risikoanalyse) ausarbeiten.

Quellen

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium, Edition 2021, ISBN: 978-3-8462-0906-6, abgerufen am 08.11.2021, IT-Grundschutz-Kompendium Edition 2021 (bund.de)

[2] Informationssicherheitsrichtlinien Universitätsklinikum Halle (Saale)

[3] Informationssicherheitskonzept Universitätsklinikum Halle (Saale)

[4] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), 07. Mai 2021, BSI - IT-Sicherheitsgesetz 2.0 (bund.de).

[5] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), 14. August 2009, BSI - BSI-Gesetz (bund.de)

[6] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung), 22. April 2016, BSI-KritisV - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (gesetze-im-internet.de)

[7] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, http://data.europa.eu/eli/reg/2016/679/2016-05-04

[8] Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus Version 1.1, 29. Oktober 2019, https://www.dkgev.de/

[9] Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NW) vom 22. Februar 1994 in der Fassung vom 07.09.2021, https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000495

[10] Krankenhausgesetz Sachsen-Anhalt (KHG LSA) in der Fassung der Bekanntmachung vom 14. April 2005, https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-KHGST2005V6P1

[11] Saarländisches Krankenhausgesetz in der Fassung der Bekanntmachung vom 6. November 2015 (Amtsbl. I S. 857), zuletzt geändert durch Artikel 4 des Gesetzes vom 22. August 2018 (Amtsbl. I S. 674), SKHG,SL - Saarländisches Krankenhausgesetz - Gesetze des Bundes und der Länder (lexsoft.de)

[12] Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen (KHGG NRW) vom 11. Februar 2007 in der Fassung vom 07. September 2021, https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000483

[13] Bayerisches Krankenhausgesetz (BayKrG) in der Fassung der Bekanntmachung vom 28. März 2007 (GVBl. S. 288, BayRS 2126-8-G), das zuletzt durch § 1 Abs. 149 der Verordnung vom 26. März 2019 (GVBl. S. 98) geändert worden ist, https://www.gesetze-bayern.de/Content/Document/BayKrG?fontsize=large

[14] Landeskrankenhausgesetz (LKG) vom 28. November 1986, zuletzt geändert durch Artikel 11 des Gesetzes vom 19.Dezember 2018 (GVBl. S. 448), Landesrecht Rheinland-Pfalz (rlp.de)

Anhang

- Studienprotokoll
- Berechtigungskonzept
- Verzeichnis für Verarbeitungstätigkeiten
- Stellungnahme zur datenschutzrechtlichen Zulässigkeit der Verarbeitung personenbezogener Daten
- Datenschutzrechtliche Einschätzung zur Nutzung des Videokonferenzsystems „Zoom“
- Technische und organisatorische Maßnahmen des UKHs
- Technische und organisatorische Maßnahmen MEKmedia GmbH