Beispielhafter Umgang mit der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) Am Beispiel eines Krankenhaus-Informationssystems

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.

Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Autoren

Sabine Fock	Klinikum und Seniorenzentrum Itzehoe
Christoph Isele	Cerner Deutschland GmbH
Pierre Kaufmann	
Michael Letter	5medical management GmbH
Mark Rüdlin	Rechtsanwalt + Datenschutzbeauftragter
Jörg Schecker	Agfa HealthCare GmbH
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Stefan Wunschel	Sana Kliniken AG

Stand: 14.12.2019

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:

- Teilen: Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: Das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-sa/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-sa/4.0/legalcode

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
>
> Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
>
> Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Vorwort

Der Umgang mit der Datenschutz-Folgenabschätzung ist bisher in Deutschland weitestgehend unbekannt. Eine auf das Gesundheitswesen ausgerichtete Praxishilfe[1] wurde erarbeitet und basierend auf dieser Praxishilfe soll das vorliegende Beispiel eine Hilfestellung bieten, wie eine Datenschutz-Folgenabschätzung umgesetzt werden kann.

Dieses Beispiel besteht aus verschiedenen Teilen:

1) Eine Beschreibung des Beispiel-Krankenhauses und des darin eingesetzten Krankenhaus-Informations-Systems; beides entspringt vollständig der Phantasie, wobei selbstverständlich darauf geachtet wurde, dass die Beschreibung reellen Anwendungen aus der täglichen Praxis entspricht.
2) Eine Umsetzung einer Datenschutz-Folgenabschätzung, basierend auf der beispielhaften Beschreibung. Diese Folgenabschätzung basiert auf zwei Teilen:
   (1) Der textuellen Beschreibung der zugrundeliegenden Sachverhalte.
   (2) Einer Excel-Tabelle, in welcher die Risiken sowie die Behandlung der Risiken beschrieben werden.

   In der Excel-Tabelle können aus Platzgründen die technisch-organisatorischen Maßnahmen nicht vollumfänglich beschrieben werden; die Übersicht ginge verloren, wenn dies in der tabellenhaften Darstellung erfolgen würde. Daher wurde die ausführlichere Beschreibung dieser Maßnahmen in den Anhang der textuellen Beschreibung eingefügt.

Eine Datenschutz-Folgenabschätzung soll gemäß Art. 35 Abs. 7 lit. a DS-GVO eine „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung“ beinhalten. Dies beinhaltet natürlich nicht, dass alles von Grund auf erklärt werden muss; in der Praxis gelebte und anerkannte Verfahren bedürfen keiner Erklärung. Zum Beispiel kann davon ausgegangen werden, dass bekannt ist, was unter einer medizinischen Untersuchung zu verstehen oder was HL7 ist. Auch diejenigen, die eine Datenschutz-Folgenabschätzung lesen und ggf. beurteilen, müssen die entsprechende Fachkenntnis aufweisen, zumindest in dem Rahmen, wie man es bei auch bei einem Datenschutzbeauftragten entsprechend den Vorgaben von Art. 37 Abs. 5 DS-GVO („auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens“) erwarten kann.

Eine systematische Beschreibung des geplanten Verarbeitungsvorgangs erfordert eine Erläuterung

- des Datenverarbeitungsprozesses,
- der hierfür eingesetzten Technik sowie
- Art, Umfang und Umstände der Datenverarbeitung.[2]

Und dies erfolgte in Teil 2 in der textuellen Komponente.

[1] bvitg, DKG, GMDS: Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. Online, zitiert am 2019-11-10; Verfügbar unter https://gesundheitsdatenschutz.org/html/dsfa.php

[2] Jandt, in: Kühling/Buchner, Kommentar zur Datenschutz-Grundverordnung, Art. 35 DS-GVO, Rn. 35

Art. 35 Abs. 1 S. 2 DS-GVO sieht vor, dass für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung vorgenommen werden kann. Die Autoren hoffen, dass dieses Beispiel einen Anreiz bieten kann, dass für die verschiedenen in Deutschland eingesetzten Krankenhaus-Informationssysteme jeweils eine gemeinsame Datenschutz-Folgenabschätzung durchgeführt wird, z. B. durch die jeweiligen Anwendergruppen.

Neben der Betrachtung des Gesamtrisikos adressiert die Möglichkeit einer gemeinsamen DSFA entsprechend ErwGr. 92 insbesondere auch „ökonomische“ sowie „vernünftige“ Gesichtspunkte. D. h. eine gemeinsame DSFA soll auch den ökonomischen und pragmatischen Zielen entsprechen. Auch unter diesen Gesichtspunkten kann es nicht wünschenswert sein, dass jedes Krankenhaus für sich eine Datenschutz-Folgenabschätzung für das von ihm eingesetzte Informationssystem durchführt, wenn hunderte anderer Krankenhäuser dasselbe System einsetzen und somit diese anderen Krankenhäuser praktisch für dieselben Risiken ebenfalls eine Datenschutz-Folgenabschätzung durchführen. Diese ökonomische Belastung für alle Krankenhäuser ist vom europäischen Gesetzgeber nicht gewollt und muss auch dem Wortlaut der DS-GVO folgend nicht passieren.

In diesem Sinne hoffen die Autoren, dass die vorliegende Arbeit in mancherlei Hinsicht bei dem praktischen Umgang mit der Datenschutz-Folgenabschätzung eine Unterstützung darstellt.

Inhaltsverzeichnis

Beschreibung des Muster-Krankenhauses

Beim Krankenhaus „Himmelstor“ handelt es sich um ein Schwerpunktkrankenhaus. Neben den Fachrichtungen Chirurgie und Innere Medizin umfasst das Versorgungsangebot auch die Fachrichtungen Gynäkologie und Geburtshilfe, Augenheilkunde und Orthopädie. An nicht bettenführenden Abteilungen werden Apotheke, Anästhesie, Laboratoriumsmedizin und Radiologie geführt.

Das Krankenhaus hat 600 Betten, davon insgesamt 32 Intensivbetten. Jährlich werden im Krankenhaus etwa 22.000 Fälle mit einer durchschnittlichen Verweildauer von 7,5 Tagen versorgt, darunter jährlich etwa 790 Entbindungen sowie ca. 2300 ambulante Operationen nach § 115b SGB V. Das Krankenhaus verfügt über 3 Großgeräte, 2 Computertomographen sowie einen Kernspintomographen.

Im Krankenhaus arbeiten 1.395 Beschäftigte, davon 197 im ärztlichen Dienst, 1198 im nichtärztlichen Dienst. 21 Beschäftigte sind im technischen Dienst eingesetzt, 4 davon bilden die IT-Abteilung, welche die Betreuung der eingesetzten informations- und kommunikationstechnischen Systeme („IKT-Systeme“) gewährleisten.

1. Zusammenfassung

- Randzahlen
  - 600 Betten, inkl. 32 Intensivbetten
  - 22.000 Fälle
  - durchschnittlichen Verweildauer von 7,5 Tagen
  - etwa 790 Entbindungen
  - ca. 2300 ambulante Operationen
- Beschäftigte
  - 197 im ärztlichen Dienst
  - 1198 im nichtärztlichen Dienst
  - 21 im technischen Dienst, davon 4 in der IT-Abteilung
- Fachrichtungen
  - Chirurgie
  - Innere Medizin
  - Gynäkologie und Geburtshilfe
  - Augenheilkunde
  - Orthopädie
  - Apotheke
  - Anästhesie
  - Laboratoriumsmedizin
  - Radiologie

2. Administrative Daten

Krankenhaus „Himmelstor“

Anstalt öffentlichen Rechts
Ust-IdNr.: DE0815471

Anschrift:
Gottes Acker 23
04711 Himmelshausen

Kontaktdaten
E-Mail: info@Gott-sei-bei-uns.de

Personen
Geschäftsführerin: Frau Luise Gottesstrafe
Datenschutzbeauftragter: Frank T. Eufel
IT-Leiterin: Luise B. Eelzebub

3. KIS „Complete Recovery“

Das Krankenhaus-Informationssystem (KIS) dient der Verarbeitung der administrativen Vorgänge, insbesondere der Abrechnung der erbrachten Leistungen.

3.1 Beschreibung der Verarbeitungen

Das Krankenhaus-Informationssystem (KIS) dient der Verarbeitung der administrativen Vorgänge, insbesondere der Abrechnung der erbrachten Leistungen. Dazu werden alle hierzu benötigten Daten erhoben. Dies umfasst

- Patientenstammdaten, beinhaltend Name, Anschrift, Kontaktdaten wie Telefon usw.
- Versichertendaten (Krankenkasse, Versichertennummer usw.)
- Erbrachte Leistungen (Diagnosen, Prozeduren usw.)
- Versorgungszeitraum inkl. wann welche Leistung von wem erbracht wurde
- Die Dokumentation erfolgt insbesondere elektronisch, da die elektronische Übermittlung der Abrechnungsdaten gesetzlich vorgeschrieben ist.
- Des Weiteren dient das KIS der Erfüllung gesetzlicher Dokumentationspflichten, insbesondere der aus dem Behandlungsvertrag i. V. m. § 630f BGB resultierenden Dokumentationspflichten hinsichtlich der erfolgten, geplanten oder empfohlenen medizinischen Versorgung unserer Patienten.

Die Speicherdauer erfolgt entsprechend den gesetzlichen Vorgaben, d. h. entsprechend § 630f BGB grundsätzlich 10 Jahre soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Allerdings erfolgt nach einer Risikobewertung eine längere Aufbewahrung von bis zu 30 Jahren (§ 199 Abs. 2 BGB), damit im Falle eines Zivilprozesses die Möglichkeit des Nachweises einer „state-of-the-art“ entsprechenden Behandlung geführt werden kann.

Auf die Daten können während des Behandlungsprozesses nur an der Behandlung beteiligte Personen zugreifen, zuzüglich das administrative Personal, das zur Erbringung ihrer Leistung auf die Daten zugreifen muss (z. B. IT-Personal im Falle von Supportleistungen oder das Personal in der Abrechnungsabteilung). Nach Beendigung des Behandlungsfalles werden die Daten bis zum Zeitpunkt der physikalischen Löschung für alle gesperrt. Die Sperre aufheben können

- Personal der Abrechnungsabteilung, sofern Nachfragen seitens der Krankenkasse bzw. des MDK vorliegen
- Medizinisches Personal
  a) bei Rückfragen nachbehandelnder Einheiten
  b) bei Wiederaufnahme des Patienten, sofern die Daten zur Behandlung benötigt werden

- Personal des Krankenhauses zu Forschungszwecken, sofern die Forschung seitens der Krankenhausleitung genehmigt wurde
- in Regressfällen durch die mit dem Regressfall betrauten bzw. involvierten Beschäftigten.

Eine Übermittlung der Daten erfolgt ausschließlich im Rahmen der gesetzlichen Vorgaben. Dies schließt insbesondere ein:

- Eine Weitergabe von Behandlungsdaten an den Hausarzt § 73 SGB V (nur mit schriftlicher Einwilligung)
- Eine Übermittlung der Leistungsdaten entsprechend SGB V, insbesondere entsprechend § 301 SGB V
- Falls erforderlich eine Weitergabe an den medizinischen Dienst der Krankenkassen (MDK) entsprechend (§ 275 SGB V)
- Im Bedarfsfall erfolgt ein Antrag auf Kostenübernahme beim Sozialamt (SGB XII)
- Eine Übermittlung zur Ermöglichung der gesetzlich vorgeschriebenen Qualitätssicherung (§ 137a SGB V).

Das KIS ist dabei mit den im Krankenhaus eingesetzten Subsystemen elektronisch verbunden. Dies sind das Bildarchiv („Picture Archiving and Communication System“, PACS) sowie das Labor-Informationssystem. Dabei werden die Stammdaten mittels HL7 untereinander ausgetauscht und im Bedarfsfall Aktualisierungen ausgetauscht. Desgleichen werden von den Subsystemen behandlungs- und abrechnungsrelevante Daten an das KIS gesendet.

3.2 Beschreibung der Module des KIS

- Patientenaufnahme
  Aufnahme der Stammdaten eines Patienten sowie Zuweisung einer Station bei Patientenaufnahme. Ggf. Zugriff auf Alt-Daten, falls Patient zuvor im Krankenhaus behandelt wurde, zwecks Übernahme der Stammdaten.
- Arzt-Arbeitsplatz
  Medizinische sowie gesetzlich geforderte Dokumentation (z. B. Qualitätssicherung, Kodierung für Abrechnung) der ärztlichen Behandlung
- Ambulanzmodul
  Dokumentation der ambulanten Behandlung, ggf. der Aufnahme eines Patienten resultierend aus dem Ambulanzbesuch
- Stationsmodul
  Dokumentation der medizinischen Behandlung eines Patienten sowie des Terminmanagements
- Abrechnungsmodul
  Controlling und Abrechnung der erbrachten Leistungen

3.3 Verarbeitungszwecke

a) Patientendaten

Die Verarbeitung der Daten erfolgt zur

- Behandlung der Patienten
- Abrechnung der erbrachten Leistungen
- Gewährleistung einer Nachvollziehbarkeit der Patientenbehandlung
- Bereitstellung aller zur Mit- und/oder Nachbehandlung erforderlichen Informationen

sowie der Erfüllung der damit verbundenen gesetzlichen Anforderungen, z. B. der Nachweispflicht, welche Person bzw. welche Personengruppe Zugriff auf Patientendaten hatte.

b) Beschäftigtendaten

Die Verarbeitung erfolgt zur

- Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses
- Gewährleistung erforderlicher Sicherheitsmaßnahmen zur Aufrechterhaltung eines geschützten Geschäftsbetriebes
- Beachtung gesetzlicher Vorgaben, insbesondere im Bereich des Steuer-und Sozialversicherungsrechts
- Umsetzung von Pflichten aus dem Recht der sozialen Sicherheit und des Sozialschutzes, wie z. B. Angabe von Gesundheitsdatengegenüber der Krankenkasse, Erfassung der Schwerbehinderung wegen Zusatzurlaub und Ermittlung der Schwerbehindertenabgabe
- Aufklärung von Straftaten i.S.v. § 26 Abs. 1 S. 2 BDSG

Im Kontext des KIS werden Daten zur Umsetzung des Berechtigungskonzeptes verarbeitet (Name des Beschäftigten, Organisationszugehörigkeit) sowie zur Protokollierung zur Gewährleistung der IT-Sicherheit sowie zum Nachkommen datenschutzrechtlicher Pflichten insbesondere dem Auskunftsrecht.

3.4 Verarbeitete Daten

Es werden sowohl Beschäftigten- als auch Patientendaten verarbeitet.

- Arten von Beschäftigtendaten
  - Identifizierende Daten
    - Personalnummer
  - Stammdaten
    - Name/Vorname
    - Titel
  - Organisationsspezifische Daten
    - Ausbildungsstand (z. B. examinierte Pflegekraft oder in Ausbildung befindlich)
    - Beruflicher Einsatz, wie z. B. ärztlicher oder pflegerischer Dienst, MTA/MTRA
    - Einsatzort (Station oder Abteilung wie z. B. Radiologie oder Anästhesie)
  - Administrative Daten
    - IP-Adresse (Beim Zugriff auf Patientendaten)
    - Datum/Uhrzeit von Zugriffen (An-/Abmelden vom System, Zugriff auf Patientendaten)
  - Biometrische Daten
    - Fingerprint (ausschließlich von Beschäftigten, die Zugang zu definierten Hochsicherheitsbereichen wie z. B. Rechenzentrum benötigen)
- Arten von Patientendaten
  - Identifizierende Daten
    - Krankenversicherungsnummer
    - Patient-ID aus Informationssystem
  - Stammdaten
    - Name/Vorname
    - Geburtsname
    - Geburtsdatum
    - Geburtsort

    - Geschlecht
    - Alter
    - Religionszugehörigkeit
    - Anschrift
    - Kontaktdaten (Telefon, Fax, Dann, …)
    - Kontaktdaten von Angehörigen der Patienten, usw.
    - Titel
    - Krankenkasse
- Gesundheitsdaten
    - Physiologische Auffälligkeiten
    - Klinische Informationen
- Biometrische Daten
    - DANN-Profil (im Rahmen der Patientenbehandlung z. B. zur Typisierung eines Tumors oder von Patienten, die ihre DANN der Biodatenbank spenden)

3.5 Datenerhebung: Beschäftigtendaten

Die Beschäftigtendaten werden bei Einstellung erhoben und in das KIS eingetragen, wenn ein Vorgesetzter der beschäftigten Person einen Antrag auf Zugriff von im KIS gespeicherten Daten stellt. Während der Arbeit erfolgt eine Protokollierung aller schreibenden Daten im KIS. Desgleichen wird jeder Zugriff auf Patientendaten protokolliert, der von außerhalb der Behandlungseinheit des Patienten erfolgt. Protokolliert werden:

- User-ID des an- und abmeldenden Anwenders
- Zeitpunkt der An- und Abmeldung
- Änderung und Löschung von Daten
    - User-ID,
    - Zeitpunkt,
    - KIS-ID des Patienten,
    - welche Datenarten geändert wurden, z. B. Arztbrief
- Datenexport
    - User-ID,
    - Zeitpunkt,
    - welche Datenarten exportiert wurden, z. B. Arztbrief
- Ausdruck von Patientendaten
    - User-ID,
    - Zeitpunkt,
    - welche Datenarten gedruckt wurden, z. B. Arztbrief
- Notfallanmeldung
    - User-ID,
    - Zeitpunkt,
    - Begründung der Notfallanmeldung)
- Datenverarbeitung im Rahmen einer Notfallanmeldung
    - User-ID,
    - Zeitpunkt,
    - auf welche Datenarten von welchem Patienten (nur KIS-ID wird gespeichert) wann zugegriffen wurde

- Veränderung am Regelwerk zur Protokollierung
    - User-ID,
    - Zeitpunkt,
    - Begründung der Änderung
- Zugriff auf Protokolldaten
    - User-ID,
    - Zeitpunkt,
    - Begründung der Änderung
- Zugriff mit „Super-User“- / Administrator-Rechten außerhalb der Arbeit an der Systemkonfiguration
    - User-ID,
    - Zeitpunkt,
    - ggf. auf welche Datenarten von welchem Patienten (nur KIS-ID wird gespeichert) wann zugegriffen wurde)

3.6 Datenerhebung: Patientendaten

Die Patientenstammdaten werden bei Aufnahme des Patienten erhoben (entweder direkt beim Patienten oder – im Falle einer Nicht-Ansprechbarkeit – bei Angehörigen oder anderen, den Patienten begleitenden Personen), alle anderen im Rahmen der Patientenbehandlung auftauchenden Daten werden zum Zeitpunkt ihres Anfallens im KIS gespeichert, sofern dies im Behandlungskontext erforderlich ist.

Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

für das Krankenhaus-Informations-System (KIS) „Complete Recovery“

Dokumenten-Historie

Version	Datum	Bearbeiter	Bearbeitung
1.0	14.12.2019	– James Tiberius Kirk (DSB) – Leonard McCoy (Chefarzt) – Montgomery Scott (IT-Leiter) – Pavel Andreievich Chekov (IT-Sicherheitsbeauftragter)	Erstellung/Initialisierung

Inhaltsverzeichnis

1 Stammdaten des Unternehmens/der Organisation

Die Gesamtverantwortung für den Prozess des Datenschutz-Risikomanagements trägt die Geschäftsführung des Unternehmens.

Es ist organisatorisch sichergestellt, dass es im Bereich DS-Risikomanagement zu keinem Interessenskonflikt kommt und die Unabhängigkeit der Kontroll- und Prüfungsaufgabe gewahrt bleibt, indem

- z. B. eine Trennung zwischen IT und Datenschutz bis hin zur GF besteht
- externe, weisungsunabhängige Prüfstellen eingeschaltet werden
- etc.

Die Geschäftsführung beauftragt persönlich und fachlich geeignete Personen, interne und ggf. externe Stellen mit der Durchführung dieses Prozesses.

1.1 Namen und die Kontaktdaten des Verantwortlichen

Name / Bezeichnung der datenverarbeitenden Stelle	Krankenhaus „Himmelstor“
Straße Hausnummer	Gottes Acker 23
PLZ / Ort	04711 Himmelshausen
Telefon	+49 815 666 - 0
Telefax	+49 815 666 - 99
E-Mail-Adresse	info@Gott-sei-bei-uns.de
Internet-Adresse	https://Gott-sei-bei-uns.de

Angaben zur geschäftlichen Korrespondenz

Rechtsform der Gesellschaft	Anstalt öffentlichen Rechts
Handelsregisternummer	
Umsatzsteueridentifikationsnummer	DE0815471
Wirtschafts-Identifikationsnummer	

1.2 Persönliche Nennung der verantwortlichen Personen

1.2.1 Geschäftsführung

Vollständiger Name (n)	Frau Luise Gottesstrafe
Telefon	+49 815 666 - 116
Telefax	+49 815 666 - 117
E-Mail-Adresse	L.Gottesstrafe@Gott-sei-bei-uns.de

1.2.2 Leitung der Datenverarbeitung

Vollständiger Name (n)	Luise B. Eelzebub
Telefon	+49 815 666 - 112
Telefax	+49 815 666 - 113
E-Mail-Adresse	L.Eelzebub@Gott-sei-bei-uns.de

1.2.3 Angaben zur Person des Datenschutzbeauftragten

Vollständiger Name (n)	Frank T. Eufel
Telefon	+49 815 666 - 110
Telefax	+49 815 666 - 111
E-Mail-Adresse	F.Eufel@Gott-sei-bei-uns.de

2 Beschreibung des Verarbeitungsverfahrens

Das Krankenhaus-Informationssystem (KIS) dient der Verarbeitung der administrativen Vorgänge, insbesondere der Abrechnung der erbrachten Leistungen. Dazu werden alle hierzu benötigten Daten erhoben. Dies umfasst

- Patientenstammdaten, beinhaltend Name, Anschrift, Kontaktdaten wie Telefon usw.
- Versichertendaten (Krankenkasse, Versichertennummer usw.)
- Erbrachte Leistungen (Diagnosen, Prozeduren usw.)
- Versorgungszeitraum inkl. wann welche Leistung von wem erbracht wurde
- Die Dokumentation erfolgt insbesondere elektronisch, da die elektronische Übermittlung der Abrechnungsdaten gesetzlich vorgeschrieben ist.
- Des Weiteren dient das KIS der Erfüllung gesetzlicher Dokumentationspflichten, insbesondere der aus dem Behandlungsvertrag i. V. m. § 630f BGB resultierenden Dokumentationspflichten hinsichtlich der erfolgten, geplanten oder empfohlenen medizinischen Versorgung unserer Patienten.

Eine ausführliche Beschreibung des KIS und seiner Module ist in den jeweiligen Handbüchern zu finden, desgleichen die Schnittstellenbeschreibung zur Kommunikation mit anderen IT-Systemen.

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 DS-GVO nur für Verarbeitungen, nicht für IT-Systeme vorgesehen. Bei der Nutzung unseres KIS können drei grundsätzliche Behandlungen aufgetreten werden, dessen Risiken betrachtet werden müssen.

1) Die administrative Aufnahme. Hier werden die Patienten im Krankenhaus aufgenommen und basierend auf dieser Patientenaufnahme im späteren Verlauf alle Daten zugeordnet. Hier können beispielsweise Risiken für den Patienten auftreten, wenn eine falsche Zuordnung erfolgt, z. B. wenn zu einem Patienten die Versichertenkare eines anderen Patienten eingelesen wird oder bei einer erneuten Aufnahme ein ähnlich klingender Name aus den vorhandenen Altdaten des KIS ausgewählt wird, der nicht der Identität des jeweiligen Patienten entspricht.
2) Die Patientenbehandlung. Auch während der eigentlichen Patientenbehandlung können grundsätzlich Risiken existieren, wenn Daten einem Patienten falsch zugeordnet werden, beispielsweise wenn bei der Anamnese der falsche Patient im KIS aufgerufen und unter dieser falschen Identität dann Befunde einem anderen Patienten zugeordnet werden können. Oder wenn beispielsweise für eine Behandlung notwendige Daten nicht in der erforderlichen Zeitspanne zur Verfügung stehen.
3) Die Abrechnung. Werden Abrechnungsdaten einem falschen Patienten zugeordnet und der falsche Patient erhält die Daten, so erfolgt evtl. eine unbefugte Offenbarung. Desgleichen können einem Patienten durch eine Falschzuordnung finanziellem Schaden zugefügt werden, wenn eine Versicherung nach einer besonders kostenintensiven Behandlung den Versicherungsbeitrag des Patienten erhöht, diese kostenintensive Behandlung aber ein anderer Patient erhielt.

Die Verarbeitungen und die daraus resultierenden Betrachtungen bzgl. des Risikos für die Rechte und Freiheiten der Patienten sind für alle Module des KIS identisch, so dass diese Module nicht separat betrachtet werden müssen. Bzgl. der Betrachtung der Risiken für die Rechte und Freiheiten der Patienten gibt es neben den den oben genannten Verarbeitungen innewohnenden Risiken auch allgemeine Risiken, die ebenfalls betrachtet werden müssen.

Die Speicherdauer erfolgt entsprechend den gesetzlichen Vorgaben, d. h. entsprechend § 630f BGB grundsätzlich 10 Jahre soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Allerdings erfolgt nach einer Risikobewertung eine längere Aufbewahrung von bis zu 30 Jahren (§ 199 Abs. 2 BGB), damit im Falle eines Zivilprozesses die Möglichkeit des Nachweises einer „state-of-the-art“ entsprechenden Behandlung geführt werden kann.

Auf die Daten können während des Behandlungsprozesses nur an der Behandlung beteiligte Personen zugreifen, zuzüglich das administrative Personal, das zur Erbringung ihrer Leistung auf die Daten zugreifen muss (z. B. IT-Personal im Falle von Supportleistungen oder das Personal in der Abrechnungsabteilung). Nach Beendigung des Behandlungsfalles werden die Daten bis zum Zeitpunkt der physikalischen Löschung für alle gesperrt. Die Sperre aufheben können

- Personal der Abrechnungsabteilung, sofern Nachfragen seitens der Krankenkasse bzw. des MDK vorliegen
- Medizinisches Personal
  c) bei Rückfragen nachbehandelnder Einheiten
  d) bei Wiederaufnahme des Patienten, sofern die Daten zur Behandlung benötigt werden
- Personal des Krankenhauses zu Forschungszwecken, sofern die Forschung seitens der Krankenhausleitung genehmigt wurde
- in Regressfällen durch die mit dem Regressfall betrauten bzw. involvierten Beschäftigten.

Eine Übermittlung der Daten erfolgt ausschließlich im Rahmen der gesetzlichen Vorgaben. Dies schließt insbesondere ein:

- Eine Weitergabe von Behandlungsdaten an den Hausarzt § 73 SGB V (nur mit Einwilligung)
- Eine Übermittlung der Leistungsdaten entsprechend SGB V, insbesondere entsprechend § 301 SGB V
- Falls erforderlich eine Weitergabe an den medizinischen Dienst der Krankenkassen (MDK) entsprechend (§ 275 SGB V)
- Im Bedarfsfall erfolgt ein Antrag auf Kostenübernahme beim Sozialamt (SGB XII)
- Eine Übermittlung zur Ermöglichung der gesetzlich vorgeschriebenen Qualitätssicherung (§ 137a SGB V).

Das KIS ist dabei mit den im Krankenhaus eingesetzten Subsystemen elektronisch verbunden. Dies sind das Bildarchiv („Picture Archiving and Communication System“, PACS) sowie das Labor-Informationssystem. Dabei werden die Stammdaten mittels HL7 untereinander ausgetauscht und im Bedarfsfall Aktualisierungen ausgetauscht. Desgleichen werden von den Subsystemen behandlungs- und abrechnungsrelevante Daten an das KIS gesendet.

2.1 Beurteilung Notwendigkeit hinsichtlich Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, ist eine DSFA durchzuführen (Art. 35 DS-GVO).

Weiteres siehe zu dieser DSFA gehörende Excel-Tabelle

2.2 Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien

In unserem Krankenhaus gilt stets der Grundsatz, dass ein Schaden für den Patienten so gut wie möglich ausgeschlossen werden muss, d. h. der Patient bekommt in unserem Krankenhaus die von unserer Seite aus bestmögliche zu erbringende medizinische Versorgung. Daher werden alle Daten dokumentiert, die hierzu erforderlich sein können. Dies erfordert ggf. auch die Verarbeitung von Daten, die nur potentiell zur Behandlung benötigt werden, wie z. B. Allergien.

2.2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Patientenbehandlung wird im KIS dokumentiert, so dass die Behandlung bei Bedarf dem Patienten gegenüber nachvollziehbar dargelegt werden kann. Eine entsprechende Protokollierung ermöglicht in Verbindung mit dem Berechtigungskonzept die Darstellung, welche Daten des Patienten von welchem Beschäftigten verarbeitet wurden.

2.2.2 Zweckbindung

Die Daten werden ausschließlich zu den in Abschnitt 4 dargestellten Zwecken verarbeitet.

2.2.3 Datenminimierung

Im Rahmen der Patentenbehandlung werden nur notwendige bzw. potentiell notwendige Daten verarbeitet.

2.2.4 Richtigkeit

Grundlegend für die medizinische Behandlung ist die Korrektheit der erhobenen Daten. Daher ist eine unverzügliche Berichtigung nach Bekanntwerden fehlerhaft gespeicherter Daten unumgänglich und liegt im direkten Interesse sowohl der behandelten Patienten als auch aller im Krankenhaus beschäftigten Personen. Um die Richtigkeit der Daten zu gewährleisten gilt für uns:

- Bei der direkten Erhebung beim Betroffenen oder bei der Erhebung über Bevollmächtigte/Vertreter/Sonstige vertrauen wir auf die Richtigkeit der Daten durch die persönliche Bekanntgabe. Bei Unverständnis fragen wir vor Dokumentation nach.
- Im Bereich der indirekten Erhebung installieren wir Freigabe-Szenarien, um eine Kontrolle auf Korrektheit vorzunehmen.
- Daten von staatlichen Quellen unterliegen einer sensiblen Eigenüberprüfung der Instanzen. Bei Problemen fragen wir bei diesen schriftlich oder telefonisch nach.
- Daten aus öffentlich verfügbaren bzw. nicht-öffentlich verfügbaren Quellen nutzen wir für unsere Systeme nicht.

2.2.5 Speicherbegrenzung

Die Speicherung richtet sich nach dem Grundsatz der Erforderlichkeit. Neben dem Erfordernis bzgl. der Patientenbehandlung gelten ebenfalls die Erfordernisse den rechtlichen Aufbewahrungspflichten zu genügen, desgleichen im Bedarfsfall die ordnungsgemäße Behandlung nachweisen zu können

2.2.6 Integrität und Vertraulichkeit

Der Zugriff auf die Daten erfolgt nur nach den im Berechtigungskonzept dargestellten Prinzipien, d. h. es erhalten nur Beschäftigte Zugriff auf die Patientendaten, die diese zur Erfüllung ihrer dienstlichen Pflichten benötigen. Entsprechend dem Backupkonzept erfolgt eine tägliche Sicherung, so dass in Folge eines unbeabsichtigten Verlusts, einer unbeabsichtigten Zerstörung oder unbeabsichtigten Schädigung die Daten wieder hergestellt werden können.

2.2.7 Zusammenfassung

Die Verarbeitung erfolgt ausschließlich für festgelegte, eindeutige und legitime Zwecke:	☒
Die Verarbeitung ist rechtmäßig.	☒
Die Datenverarbeitung ist dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt:	☒
Eine begrenzte Speicherfrist liegt vor, und zwar	☒

3 Welche Daten werden verarbeitet?

3.1 Welche Datenarten werden verarbeitet?

- Patientendaten
    - Stammdaten
        - Name/Vorname
        - Geburtsname
        - Geburtsdatum
        - Geburtsort
        - Geschlecht
        - Alter
        - Religionszugehörigkeit
        - Anschrift
        - Kontaktdaten (Telefon, Fax, E-Mail, …)
        - Ethnische Zugehörigkeit
        - Ausbildung
        - Titel
    - Identifizierende Daten
        - Patient-ID aus Informationssystem
    - Administrative Daten
        - Aufnahme-, Entlassdatum und -uhrzeit
        - Aufnahmeart (Einweisung, Arbeitsunfall, Notfall, usw.)
        - Aufnahmegrund (vollstationär, teilstationär usw.)
        - Versichertenart (privat oder gesetzlich versichert) sowie ggf. Zuzahlungskennzeichen
        - Krankenversicherung/Krankenkasse sowie Versichertenart (Mitglied, Familie usw.)
        - Ggf. Krankenversicherten-Nr. sowie Gültigkeit der Versichertenkarte
        - Versorgende Abteilungen (Fachabteilunge, Station(en) usw.)
    - Medizinische Daten
        - Physiologische Auffälligkeiten
        - Klinische Daten aus Anamnese, Diagnose, Therapie
        - Follow-Up-Daten
- Daten von Anwendern des Systems
    - Stammdaten
        - Name/Vorname
        - Geburtsdatum
        - Abteilung
    - Identifizierende Daten
        - Nutzer-ID aus des XDS-Informationssystem
    - Beschäftigtendaten
        - Job-Beschreibung (z. B. Administrator, Oberärztin)
        - Dienstliche Anschrift
        - Dienstliche Kontaktdaten (Telefon, Fax, E-Mail, …)
        - (Fach-) Abteilung
    - Biometrische Daten (Nur bzgl. Zugang zu Serverräumlichkeiten)

        - Fingerprint
        - Fotos (Gesicht)
    - Im Rahmen Protokollierung
        - User-ID (auch aus Fremd-Systemen
        - IP-Adresse
        - Datum/Uhrzeit von Zugriffen (An-/Abmelden vom System, Zugriff auf bestimmte Daten)

3.2 Wo werden die Daten erhoben?

Die Beschäftigtendaten werden bei Einstellung erhoben und in das KIS eingetragen, wenn ein Vorgesetzter der beschäftigten Person einen Antrag auf Zugriff von im KIS gespeicherten Daten im Rahmen der im Berechtigungskonzept vorgeschriebenen Rahmenbedingungen stellt. Während der Arbeit erfolgt eine Protokollierung aller schreibenden Daten im KIS. Desgleichen wird jeder Zugriff auf Patientendaten protokolliert, der von außerhalb der Behandlungseinheit des Patienten erfolgt. Protokolliert werden (weitere Informationen hierzu finden sich im Protokollierungskonzept):

- User-ID des an- und abmeldenden Anwenders
- Zeitpunkt der An- und Abmeldung
- Änderung und Löschung von Daten
    - User-ID,
    - Zeitpunkt,
    - KIS-ID des Patienten,
    - welche Datenarten geändert wurden, z. B. Arztbrief
- Datenexport
    - User-ID,
    - Zeitpunkt,
    - welche Datenarten exportiert wurden, z. B. Arztbrief
- Ausdruck von Patientendaten
    - User-ID,
    - Zeitpunkt,
    - welche Datenarten gedruckt wurden, z. B. Arztbrief
- Notfallanmeldung
    - User-ID,
    - Zeitpunkt,
    - Begründung der Notfallanmeldung)
- Datenverarbeitung im Rahmen einer Notfallanmeldung
    - User-ID,
    - Zeitpunkt,
    - auf welche Datenarten von welchem Patienten (nur KIS-ID wird gespeichert) wann zugegriffen wurde
- Veränderung am Regelwerk zur Protokollierung
    - User-ID,
    - Zeitpunkt,
    - Begründung der Änderung
- Zugriff auf Protokolldaten
    - User-ID,

    - Zeitpunkt,
    - Begründung der Änderung
- Zugriff mit "Super-User"- / Administrator-Rechten außerhalb der Arbeit an der Systemkonfiguration
    - User-ID,
    - Zeitpunkt,
    - ggf. auf welche Datenarten von welchem Patienten (nur KIS-ID wird gespeichert) wann zugegriffen wurde

Die Patientenstammdaten werden bei Aufnahme des Patienten erhoben (entweder direkt beim Patienten oder – im Falle einer Nicht-Ansprechbarkeit – bei Angehörigen oder anderen, den Patienten begleitenden Personen), alle anderen im Rahmen der Patientenbehandlung auftauchenden Daten werden zum Zeitpunkt ihres Anfallens im KIS gespeichert, sofern dies im Behandlungskontext erforderlich ist.

3.3 Darstellung der potenziellen Risiken

Insbesondere den Patientendaten kann ein hohes Risiko bei der unbefugten Kenntnisnahme durch Dritte innewohnen. Für Patienten bestehen insbesondere die folgenden Risiken:

- Diskriminierung, z. B. durch Bekanntwerden ansteckender oder stigmatisierender Erkrankungen
- Finanzieller Verlust, z. B. durch Verlust des Beschäftigungsverhältnisses durch Bekanntwerden einer chronischen Erkrankung, welche z. B. häufige längerfristige krankheitsbedingte Ausfälle im Berufsleben beinhaltet
- Rufschädigung, z. B. durch Bekanntwerden des Vorliegens einer sexuell übertragbaren Erkrankung.

Die genaue Darstellung der Risiken findet sich in der zu dieser DSFA gehörende Excel-Tabelle.

4 Zwecke und Mittel der Verarbeitung

4.1 Begründung, warum die Informationen verarbeitet werden müssen

- Patientendaten

  Die Behandlung eines Patienten muss nachvollziehbar erfolgen, so dass für den Patienten eine größtmögliche Transparenz bzgl. der medizinischen Behandlung gegeben ist. Zugleich müssen alle medizinischen Daten, die in Folge einer Nach- und/oder Weiterbehandlung erforderlich sein könnten, dokumentiert werden. Weiterhin müssen die Leistungen abgerechnet werden, damit unser Krankenhaus existieren und seine Versorgungsdienstleistung anbieten kann. Daher werden diese Daten im KIS verarbeitet.

  Neben der Versorgung des Patienten durch unser Krankenhaus können die Daten auch noch folgenden Zwecken dienen:

  - Nutzung durch die behandelte Person
    - Selbstversorgung und Pflege der eigenen Gesundheit
    - Häusliche Pflege
    - Information von Familie und/oder interessierten Dritten über die Krankengeschichte (Z. B. Einholung einer Zweitmeinung)
    - Übergabe der Gesundheitsversorgung an einen anderen Erbringer (z. B. zum Zwecke der Nach- oder Weiterbehandlung)
  - Gesundheitsversorgung durch Mit- und/oder Nachbehandler
    - Ambulante Versorgung
    - Klinische Versorgung
    - Notfallversorgung
  - Forschung
    - Retrospektive Studien
    - Durchführung von Rekrutierungsmaßnahmen für klinische Versuche oder sonstige Forschungsstudien
- Daten von Anwendern des Systems

  Gesundheitsdaten gehören entsprechend den Vorgaben der DS-GVO zu den besonders sensiblen Daten, die einen entsprechend hohen Schutzbedarf aufweisen. Demgemäß dürfen nur Personen Zugriff auf diese Daten bekommen, die ein legitimes Interesse aufweisen können. Daraus folgt die Notwendigkeit der Identifizierung entsprechender Personen.

  Weiterhin muss nachvollziehbar sein, sofern Änderungen der Daten erfolgen. Entsprechend werden Änderungen sowohl der Patientendaten selbst als auch der Protokollierungsregeln für Zwecke der aus Art. 5 Abs. 2 DS-GVO resultierenden Rechenschaftspflicht festgehalten.

  Daher werden für diese administrative Zwecke folgende Daten verarbeitet:

  - Authentifizierung des Anwenders bzgl. An- und Abmeldung am System
  - Zuweisung an Zugriffsrechten
  - Nachverfolgbarkeit wer wann auf welche Daten zugegriffen hat

4.2 Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung

- Beschäftigtendaten

  Die User-ID ist zwingend zur Identifikation erforderlich. Da die User-ID nur im KIS bekannt ist, müssen die zur Identifikation der beschäftigten Person erforderlichen Stammdaten ebenfalls im KIS gespeichert werden.

Zur Gewährleistung der Rechenschaftspflicht ist es erforderlich, dass die hierzu relevanten Ereignisse erfasst und dokumentiert werden und hierbei die Zuordnung zu der jeweils das Ereignis auslösenden Person möglich ist. Daher werden sowohl die Ereignisse als auch Zeitpunkt und User-ID protokolliert.

Die Protokolldaten enthalten sensible Informationen, insbesondere über die Beschäftigten. Daher muss ein Zugriff auf die Protokolldaten im Sinne des Schutzes der Beschäftigten gleichermaßen nachvollziehbar sein. Entsprechend erfolgt hierzu eine Protokollierung.

- Patientendaten

  Eine Zuordnung der Gesundheitsdaten zum jeweiligen Patienten ist allein schon aus medizinischen Gründen unabdingbar. Daher müssen die Patientenstammdaten im KIS gespeichert werden. Weiterhin ist zur Abrechnung der erbrachten Leistungen erforderlich, dass die hierzu notwendigen administrativen Daten vorliegen.

  Im medizinischen Kontext erfolgt die Behandlung immer durch ein Behandlungsteam. Bei der Vielzahl der behandelten Patienten ist eine mündliche Weitergabe der benötigten Daten nicht praktikabel, eine entsprechende Datenmenge könnte kein Mensch im Gedächtnis behalten. Entsprechend ist eine Dokumentation unabdingbar. Um eine schnelle Zugriffsmöglichkeit gewährleisten zu können, ist eine elektronische Dokumentation, die potentiell von jedem Arbeitsplatz des Klinikums zeitgleich genutzt werden kann, das Mittel der Wahl. Daneben müssen alle Leistungen elektronisch erfasst werden, die zu Abrechnungszwecken an die jeweiligen Kostenträger übermittelt werden.

4.3 Darstellung der Erlaubnistatbestände

Grundsätzlich regeln die Datenverarbeitung für alle Betroffenen der Art. 6 Abs. 1 DS-GVO, für Beschäftigte im Besonderen der § 26 BDSG-neu sowie für besondere Kategorien von personenbezogenen Daten, z. B. Gesundheitsdaten, der Art. 9 Abs. 2 DS-GVO.

4.3.1 Beschäftigtendaten

Die Verarbeitung erfolgt im Rahmen der beruflichen Tätigkeit. Erlaubnistatbestand ist daher Art. 6 Abs. 1 lit. b DS-GVO i.V.m. § 26 Abs. 1 BDSG (= Verarbeitung ist für die Erfüllung der aus dem Arbeitsvertrag resultierenden Pflichten des Beschäftigten erforderlich).

4.3.2 Patientendaten

Die Daten werden zur Patientenbehandlung sowie zur Abrechnung der erbrachten Leistungen benötigt, Erlaubnistatbestand für diese Zwecke ist Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 DS-GVO i. V. m. § 630a ff. BGB sowie § 10 Abs. 1 GDSG NW.

Zur Mit- und Weiterbehandlung werden die hierfür erforderliche Daten an Mit-/Nachbehandler weitergegeben. Rechtsgrundlage hierfür ist Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 DS-GVO sowie § 11 Abs. 1 GDSG NW. Erfolgt die Mit- und Weiterbehandlung durch einen Hausarzt i.S.v. § 73 Abs. 1a SGB V, d.h.

- Allgemeinärzte,
- Kinder- und Jugendärzte,
- Internisten ohne Schwerpunktbezeichnung, die die Teilnahme an der hausärztlichen Versorgung gewählt haben,
- Ärzte mit der Bezeichnung „Praktischer Arzt“, wenn diese auf Grund von landesrechtlichen Vorschriften zur Ausführung des Art. 30 der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von

Berufsqualifikationen (ABl. EU Nr. L 255 S. 22, 2007 Nr. L 271 S. 18) bis zum 31. Dezember 1995 erworben wurden,

- Ärzte mit einer Eintragung in das Arztregister für Vertragsärzte, welche auf Grund eines Ausbildungsnachweises über eine inhaltlich mindestens den Anforderungen nach Art. 28 der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22, 2007 Nr. L 271 S. 18) entsprechende besondere Ausbildung in der Allgemeinmedizin sind und dieser Ausbildungsnachweis in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Vertragsstaat, dem Deutschland und die Europäische Gemeinschaft oder Deutschland und die Europäische Union vertraglich einen entsprechenden Rechtsanspruch eingeräumt haben, ausgestellt worden ist, erfolgte,
- Ärzte, die am 31. Dezember 2000 an der hausärztlichen Versorgung teilgenommen haben,

so erfolgt die Weitergabe nur bei Vorliegen einer Zustimmung des Patienten gemäß § 73 Abs. 1b SGB V.

Unser Krankenhaus arbeitet an der stetigen Optimierung der Versorgungsqualität. Hierzu ist ein Qualitätsmanagement etabliert und die zur Qualitätssicherung erforderlichen Daten werden auf Grundlage von Art. 9 Abs. 2 lit. i DS-GVO i. V. m. § 299 SGB V i. V. m. § 136 SGB V bzw. den Richtlinien des G-BA verarbeitet.

Im Rahmen der gesetzlichen Pflichten sind wir gezwungen, Daten an gesetzliche Stellen wie Krebsregister zu melden. Rechtsgrundlage hierfür ist Art. 9. Abs. 2 lit. h, i DS-GVO i.V.m. mit dem entsprechenden Meldegesetz.

Weiterhin werden zur Abrechnung die hierfür erforderlichen Daten genutzt. Rechtsgrundlage hierfür ist Art. 9 Abs. 2 lit. f, h DS-GVO i. V. m. z. B. § 301 SGB V sowie § 11 Abs. 1 lit. d GDSG NW.

In seltenen Fällen kann es vorkommen, dass Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen wie beispielsweise der Verteidigung der behandelnden Person vor Gericht oder der Einklagung ausstehender Bezahlungen von erbrachten Leistungen verarbeitet werden müssen. In diesen seltenen Fällen besteht die Rechtgrundlage in Art. 9 Abs. 2. lit. f DS-GVO.

4.4 Darstellung der Speicherdauer

Da die Verarbeitung der Beschäftigtendaten zur Gewährleistung der Rechenschaftspflicht bzgl. der Verarbeitung der Patientendaten erfolgt, richtet sich die Speicherdauer der Beschäftigtendaten nach der Speicherdauer der entsprechenden Patientendaten.

Die Speicherdauer der Patientendaten richtet sich nach den gesetzlichen Vorgaben, d. h. i.d.R. zehn Jahre entsprechend § 630f BGB, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Allerdings kann nach einer Risikobewertung eine längere Aufbewahrung von bis zu 30 Jahren (§ 199 Abs. 2 BGB) erfolgen, damit im Falle eines Zivilprozesses die Möglichkeit des Nachweises einer ordnungsgemäßen Behandlung geführt werden kann.

Weitere Informationen finden sich im Archivierungs- sowie im Löschkonzept.

4.5 Darstellung der potenziellen Risiken

Die detaillierte Darstellung der aus den Zwecken und Mitteln der Verarbeitung resultierenden Risiken ist in der zu dieser DSFA gehörenden Excel-Tabelle beschrieben.

5 Weitergabe der Daten

5.1 Mit wem werden die Daten geteilt?

Empfänger	Art der Weitergabe			
	Fall-zu-Fall	Vollständige Übermittlung	Direkter Zugriff	Andere (spezifizieren)
Innerhalb der Legaleinheit	X		X	
Innerhalb des Konzerns	-	-	-	-
Staatliche Empfänger (spezifizieren)	X			
Nicht-staatliche Empfänger (spezifizieren)	X			

Innerhalb der Legaleinheit

- Alle an der Behandlung beteiligten Personen, z. B.
    - Konsiliarisch tätiges medizinisches Personal
    - Mitbehandelnde Einheiten
- Alle an der Abrechnung der erbrachten Leistungen beteiligten Personen
- Controlling und Qualitätssicherung nutzen die zur Erbringung ihrer Leistungen erforderliche Daten im Rahmen der rechtlichen Erlaubnistatbestände
- Auftragsverarbeiter
- Im Rahmen von Rechtsstreitigkeiten: alle im Krankenhaus durch den Rechtsstreit involvierten Personen

Staatliche Empfänger können z. B. sein:

- Auskünfte an die Polizei/ Staatsanwaltschaft; Rechtsgrundlage ist im Einzelfall zu prüfen, mögliche Erlaubnistatbestände können z. B. in folgenden Vorgaben zu finden sein
    - § 68 SGB X
    - § 34 StGB
    - § 138 StGB
    - § 16 Abs. 2 MRRG
    - § 32 BMG
- Gesundheitsamt (meldepflichtigen Erkrankungen entsprechend IfSG)
- Auskünfte an gesetzliche Unfallversicherungen (§§ 199,200, 201, 202, 203 SGB VII)
- Datenaustausch mit den gesetzlichen Krankenkassen (§ 301 SGB V, Landesverträge gemäß § 112 SGB V)
- Pflegekassen (§§ 93, 104, 114, 114a SGB XI)
- Medizinischer Dienst der Krankenkassen sofern öffentlich-rechtlich organisiert (§ 276 Abs. 2 S. 2 SGB V)

Nicht-staatliche Empfänger sind insbesondere:

- Leistungsträger wie z. B. Krankenkassen

- Medizinischen Dienst der Krankenkassen sofern privatrechtlich organisiert (§ 276 Abs. 2 S. 2 SGB V)
- Mit-/nachbehandelnde Ärzte entsprechend § 73 SGB V
- Mit-/nachbetreuende Seelsorger, sofern der Patient dies wünscht
- Mit-/nachbehandelnde ambulante Pflegedienste, sofern der Patient dies wünscht
- Mit-/nachbehandelnde Pflegeheime, sofern der Patient dies wünscht
- Mit-/nachbehandelnder Sozialdienst, sofern der Patient dies wünscht
- Freunde oder Familienangehörige des Patienten, sofern der Patient dies wünscht
- Epidemiologische und klinische Krebsregister entsprechend den gesetzlichen Vorgaben

5.2 Datenkommunikation mit anderen Systemen

Innerhalb des Krankenhauses ist das KIS das „führende Systeme“, d.h. hier werden Patienten bei der Aufnahme erfasst und in diesem System wird auch die Entlassung dokumentiert. Neben dem KIS werden noch andere Systeme eingesetzt. Die Kommunikation mit diesen Systemen erfolgt über den Kommunikationsserver „Himmelswolke“ der Firma „Benedicere“. Der Kommunikationsserver nimmt HL7-Nachrichten von allen medizinischen Informationssystemen entgegen und leitet diese an die für den Empfang vorgesehenen Systeme in der vom Empfänger bevorzugten KL7-Version weiter. Wenn im Folgenden die Kommunikation beschrieben wird, erfolgt die Kommunikation zwischen den Systemen jeweils unter dem Einsatz des Kommunikationsservers. Eingesetzte IT-Systeme sind:

- Picture Archiving and Communication System (PACS), Firma Ecce
- Labor-Informations-System (LIS), Firma Examinare
- Patientendatenmanagementsystem (PDMS), Firma Curare

Die Kommunikation der Systeme ist der nachfolgenden Tabelle 1 zu entnehmen.

Sender	Was wird gesendet?	HL7-Nachricht	Empfänger
KIS	Administrative Daten	ADT entsprechend dt. Spezifikation[3]	PACS, LIS, PDMS
PDMS	Administrative Daten	ADT entsprechend dt. Spezifikation[3]	KIS
LIS	Untersuchungsergebnis	OBX entsprechend dt. Spezifikation[4]	KIS
LIS, PACS, PDMS	Untersuchungsergebnis als pdf-Dokument	MDM entsprechend dt. Spezifikation[5]	KIS
LIS, PACS, PDMS	Abrechnungsrelevante Diagnosen- und Prozedurendaten	BAR wie bei HL7-D beschrieben[6]	KIS

Tabelle 1: Mit dem KIS über Kommunikationsserver verbundene Systeme

[3] HL7 Deutschland: deutsche Nachrichtenprofile: ADT-Profil zur Patientenaufnahme. Online, zitiert am 2019-11-07; Verfügbar unter http://wiki.hl7.de/index.php?title=HL7v2-Profile_Aufnahme i.V.m. https://wiki.hl7.de/index.php?title=HL7v2-Profile_gemeinsame_Elemente

[4] HL7 Deutschland: Segment OBX. Online, zitiert am 2019-11-07; Verfügbar unter https://wiki.hl7.de/index.php?title=Segment_OBX i.V.m. https://wiki.hl7.de/index.php?title=HL7v2-Profile_gemeinsame_Elemente

[55] HL7 Deutschland: deutsche Nachrichtenprofile: Dokumentenmanagement. Online, zitiert am 2019-11-07; Verfügbar unter https://wiki.hl7.de/index.php?title=HL7v2-Profile_MDM-Nachrichten i.V.m. https://wiki.hl7.de/index.php?title=HL7v2-Profile_gemeinsame_Elemente

[6] HL7 Deutschland: deutsche Nachrichtenprofile: gemeinsame Elemente. Online, zitiert am 2019-11-07; Verfügbar unter https://wiki.hl7.de/index.php?title=HL7v2-Profile_gemeinsame_Elemente

5.3 Datenübermittlung in Drittstaaten

Variante 1:

Eine Verarbeitung der Daten in Drittstaaten kommt nur in den folgenden Ausnahmefällen vor:

1. Im Rahmen der Auftragsverarbeitung, wenn Supportleistungen von Dienstleistern aus Drittstaaten zur Aufrechterhaltung der Funktionalität der eingesetzten IT-Systeme zwingend erforderlich ist. Rechtsgrundlage hierfür sind Standardvertragsklauseln (sogenannte „Controller - Processor Vertragsklauseln[7]) gemäß Art. 46 Abs. 2 lit. c DS-GVO.
2. In Ausnahmefällen kann es auf Grund der Weiterentwicklung der medizinischen Versorgung vorkommen, dass Leistungen weltweit nur von wenigen Akteuren erbracht werden. Dies ist z. B. im Rahmen der Bildverarbeitung so, wo einige Verarbeitungsalgorithmen in der ersten Zeit weltweit nur in wenigen Krankenhäusern eingesetzt werden, bevor diese Verarbeitungen überall verfügbar sind. Entscheidet eine Ärztin oder ein Arzt, dass ein derartiges Verfahren für die Behandlung eines Patienten eingesetzt werden sollte (z. B. zur besseren Planung einer erforderlichen Operation), so erfolgt die Verarbeitung im Drittland nach entsprechender Aufklärung des Patienten auf Grund des Erlaubnistatbestandes von Art. 49 Abs. 1 lit. b DS-GVO.
3. In seltenen Fällen, insbesondere bei besonders seltenen Erkrankungen, erfolgt eine gemeinsame Verarbeitung, wobei Partner-Krankenhäuser auch in Drittstaaten existieren. Diese Kooperationen beinhalten sowohl die Konsultationen von Spezialisten der entsprechenden Erkrankungen als auch die Erbringung medizinschier Leistungen wie z. B. Spezialuntersuchungen in Laboren. Diese Mit-Behandlung erfolgt auf Grundlage von Standardvertragsklauseln (sogenannte „Controller - Controller Vertragsklauseln[8]) gemäß Art. 46 Abs. 2 lit. c DS-GVO.

Einige Ärzte veröffentlichen regelmäßig die Ergebnisse ihrer Forschungsarbeit in Fachzeitschriften. Einige Fachzeitschriften verlangen die Veröffentlichung der Rohdaten für die Forschung, damit die Forschungsergebnisse von jedem nachgeprüft werden können, d.h. diese Rohdaten stehen weltweit Fachpersonal zur Verfügung. Bei diesen Rohdaten kann es sich um personenbezogene Daten i.S.v. Art. 4 Abs. 1 DS-GVO handeln, z. B. wenn das Rohmaterial aus Biomaterial besteht, welches die vollständige Gensequenz von Patienten beinhaltet. Hier für existiert keine Rechtsgrundlage. Sollten Ärzte dennoch ohne Einwilligung der Betroffenen entsprechende Veröffentlichungen vornehmen, würden sie gegen die ärztliche Schweigepflicht verstoßen. Eine Veröffentlichung von Forschungsergebnissen mit Personenbezug ohne Einwilligung des Betroffenen wurde daher durch den Krankenhausträger per Dienstanweisung untersagt.

Variante 2:

Findet eine Datenübermittlung in Drittstaaten außerhalb der EU statt?

[7] Klauseln der Kommission vom 5. Februar 2010: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087

[8] Klauseln der Kommission vom 27. Dezember 2004: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915

☐ Nein ☐ Ja und zwar:		
Abteilungen/Bereiche/Kliniken	**Art der Daten**	**Zweck /Legitimationsgrundlage**

5.4 Darstellung der potenziellen Risiken

Die detaillierte Darstellung der aus der Weitergabe der Daten resultierenden Risiken ist in der zu dieser DSFA gehörenden Excel-Tabelle beschrieben.

6 Wahrung der Betroffenenrechte

Im KIS werden neben den Patientendaten auch Beschäftigtendaten gespeichert. Die Beschäftigtendaten dienen der Gewährleistung der gesetzlichen Anforderungen am Betrieb eines KIS, z. B. dem Nachweis, wer wann auf welche Patientendaten zu welchem Zeitpunkt zugegriffen hat. Im Nachfolgenden werden daher die Betroffenenrechte aus Sicht der Patienten beschrieben.

Gleichwohl haben selbstverständlich auch Beschäftigte entsprechende Rechte, allerdings werden sie bei der Einstellung auf diese Rechte hingewiesen und erfahren hierbei auch, wie sie diese Rechte wahrnehmen können.

Im Rahmen der Datenschutzschulung erfolgte u. A. eine Schulung des entsprechenden Personals im Umgang mit Betroffenenrechten, so dass eine sach- und fachgerechte Abarbeitung entsprechender Anfragen gewährleistet ist. Zugleich erfahren in diesen Schulungen unsere Beschäftigten ebenfalls, wie sie ihre eigenen Rechte wahrnehmen können.

6.1 Transparenzerfordernis

Transparenz bei Betroffenen durch Erfüllung der Informationspflichten schaffen.	**Ja**	**Nein**
Bedarf die aktuelle Verarbeitungstätigkeit erweiterter Informationspflichten über die bereits etablierten hinweg? **Falls ja, untere Fragen beantworten. Falls nein, Auskunftsende hier.**	☒	☐
Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Beschäftigte?	☐	☒
Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Bewerber?	☐	☒
Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für ambulante Patienten?	☒	☐
Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Notfall-/stationäre Patienten?	☒	☐
Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für sonstige Betroffene? Wenn ja, welche Betroffenen? ∅	☐	☒

6.2 Information des Betroffenen

Bei Aufnahme erhält jeder Patient eine Information, in welcher die notwendigen Angaben entsprechend Art. 13 resp. Art. 14 DS-GVO enthalten sind.
Auf dieser Information befindet sich auch ein Link auf die Internetseite unseres Krankenhauses, welche die von uns beauftragten Auftragsverarbeiter enthält:

- Namen des Auftragsverarbeiters
- die Tätigkeit (z. B. Betreuung Krankenhausinformationssystem)
- wann das Vertragsverhältnis begann
- ggfs. wann das Vertragsverhältnis endete (offenes Enddatum = Vertragsverhältnis dauert an).

Sofern die Weitergabe von Daten nicht alle Patienten betrifft wie z. B. die Weitergabe von Daten an ein Krebsregister, wird der betroffene Patient hierüber individuell informiert. Hierzu werden ggf. Formulare der datenempfangenden Stelle genutzt.

Die Informationen werden dabei stets in einer klaren und einfachen Sprache vermittelt, wie es Art. 12 DS-GVO fordert.

6.3 Auskunftsrecht

Die betroffene Person hat das Recht, von uns eine Bestätigung darüber zu verlangen, ob personenbezogene Daten verarbeitet werden. Dies wird ihm im Rahmen der unter Abschnitt 6.2 genannten Information mitgeteilt. In dieser Information wird hierzu sowohl eine Telefonnummer als auch eine spezielle nicht-personalisierte E-Mailadresse, die somit auch bei einem Wechsel des zuständigen Sachbearbeiters erhalten bleibt, genannt.

Unser KIS gewährleistet die Möglichkeit, dem Patienten die eigenen Daten in einem gängigen, maschinenlesbaren und interoperablen Format (= pdf-Format) zu übergeben, so dass jederzeit die technische Möglichkeit gegeben ist, dem Auskunftsersuchen einer betroffenen Person Folge zu leisten.

6.4 Widerspruchsrecht

Jeder Patient wird auf sein Recht zum Widerspruch gegen eine Datenverarbeitung hingewiesen (Information gemäß Abschnitt 6.2). Zugleich wird der Patient darauf hingewiesen, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

6.5 Recht auf Berichtigung und Vervollständigung

Die betroffene Person hat ein Recht auf Berichtigung und/oder Vervollständigung, sofern die verarbeiteten personenbezogenen Daten, die sie betreffen, unrichtig oder unvollständig sind. Zugleich wird jeder Patient darauf hingewiesen, dass ggf. auch ein Recht auf die Vervollständigung unvollständiger personenbezogener Daten (u. U. auch mittels einer ergänzenden Erklärung) besteht. Beides erfolgt durch die o. g. Information.

Das eingesetzte KIS ermöglicht die Korrektur fehlerhafter Daten. Im Rahmen der Protokollierung wird den aus § 630f Abs. 1 BGB resultierenden Pflichten genügt.

6.6 Recht auf Löschen („Vergessenwerden“)

Die betroffene Person hat das Recht auf Löschung ihrer personenbezogenen Daten gemäß den Richtlinien nach Art. 17 DS-GVO. Der Patient wird im Rahmen des Informationsschreibens gemäß Abschnitt 6.2 darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen, eingeschränkt wird.

Das eingesetzte KIS kann ausschließlich Fallbasiert löschen, d.h. alle Daten eines einzelnen Aufenthaltes eines Patienten.

6.7 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Die Voraussetzungen ergeben sich aus Art. 18 DS-GVO.

Der Patient wird im Rahmen des Informationsschreibens gemäß Abschnitt 6.2 darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Verarbeitungszwecke wie beispielsweise der Verarbeitung im Rahmen der gesetzlichen Qualitätssicherung entsprechend § 137a SGB V, eingeschränkt wird.

Das eingesetzte KIS besitzt die Möglichkeit der Sperrung von Zugriffen auf Patientendaten. Für die Entsperrung von Patientendaten ist das KIS dergestalt konfiguriert, dass eine Entsperrung nur nach Eingabe einer Begründung erfolgen kann. Allerdings besteht keine Möglichkeit zu prüfen, ob vor der Entsperrung eine Unterrichtung der betroffenen Person nach Art. 18 Abs. 3 DS-GVO erfolgte.

6.8 Recht auf Datenübertragbarkeit

Die betroffene Person hat ferner das Recht, ihre personenbezogenen Daten, die sie uns bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Außerdem hat sie das Recht, diese Daten an Dritte zu übermitteln. Ferner hat sie gemäß Art. 20 Abs. 1 DS-GVO das Recht, dass ihre personenbezogenen Daten direkt von uns an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch möglich ist und die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

Unser KIS kann Daten von betroffenen Personen mittels des international im Gesundheitswesen eingesetzten HL7-Standards an andere Informationssysteme weitergeben. Unser KIS ermöglicht weiterhin Daten in einem gängigen, maschinenlesbaren und interoperablen Format (= pdf-Format) zu exportieren, so dass die Daten in diesem Format übergeben werden können.

6.9 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Die betroffene Person hat jederzeit das Recht, gegen die Verarbeitung ihrer personenbezogenen Daten (die aufgrund von Art. 6 Abs. 1 lit. e oder f erhoben wurden) Widerspruch einzulegen. Dies gilt ebenso für das auf diesen Bestimmungen, sofern zutreffend, geschütztes Profiling. Die Daten werden im Falle eines Widerspruchs nicht weiterverarbeitet, es sei denn, es liegen zwingende schutzwürdige sowie nachweisbare Gründe vor, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

6.10 Fazit

☒ Die Betroffenenrechte werden seitens des Verantwortlichen gewährleistet.

☐ Die Betroffenenrechte werden seitens des Verantwortlichen nur unvollständig berücksichtigt.

☐ Die Betroffenenrechte werden seitens des Verantwortlichen nicht berücksichtigt.

7 Risikoanalyse, Gewährleistung der Sicherheit der Daten, Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken / Restrisikobewertung

7.1 Risikostufen

Die DS-GVO definiert den Begriff „Risiko“ nur indirekt. In Art. 24 Abs. 1 S. 1 DS-GVO findet sich: „Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie **der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken** für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um“. Auch in ErwGr. 75 und 76 werden Risiken als abhängige Größe von der Eintrittswahrscheinlichkeit und der Schwere der Beeinträchtigung der Rechte und Freiheiten der betroffenen Person beschrieben. Daraus folgt, dass die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 35 DS-GVO somit in Abhängigkeit von „Eintrittswahrscheinlichkeit“ und „Schadensschwere“ darzustellen ist[9].

Die Definition eines Risikos aus Sicht der DS-GVO kann daher lauten:

> „Risiko = Produkt aus Eintrittswahrscheinlichkeit und Schwere einer Beeinträchtigung der Rechte und Freiheiten natürlicher von der Verarbeitung betroffener Personen

Nach ErwGr. 76 sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person „in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung“ bestimmt werden. Dabei kennt die DS-GVO verschiedene Grade bzgl. eines Risikos[10]:

Kategorie	Fundort DS-GVO
Hohes Risiko / hohen Risiken	ErwGr. 76, 84, 85, 86, 89, 90, 91, 94 Art. 34 Abs. 1, Abs. 3(b) und Abs. 4, Art. 35 Abs. 1, Art. 36 Abs. 1, Art. 70 Abs. 1(h)
Ernsthaftes Risiko / Erhebliche Risiken	ErwGr. 9, 15, 51
Risiko / Risiken	ErwGr. 28, 38, 39,71, 74, 75, 76, 77, 81, 83, 94, 96, 98, 122 Art. 4 Ziff. 22, Art. 4 Abs. 2(g), Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 30 Abs. 5, Art. 32 Abs. 1,2, Art. 33 Abs. 1
Voraussichtlich kein Risiko	Art. 27. Abs. 2(a)
Kein Risiko	ErwGr. 80

Tabelle 2: In der DS-GVO verwendete Grade bzgl. eines Risikos für Rechte und Freiheiten von Personen

Daraus lässt sich eine Abstufung bzgl. der Einteilung von Risiken herleiten:

- Hohes Risiko
- Erhebliches Risiko

[9] Martini M. Art. 35 Rn. 15 in Plath (Hrsg.) BDSG/DS-GVO: Kommentar zum BDSG und zur DS-GVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4

[10] Vergleiche hierzu aber auch die Ausführungen im Kurzpapier 18 der DSK (Online, zitiert am 2019-08-23; Verfügbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html), welches auf Seite 5 in der Risikomatrix davon ausgeht, dass bei jeder Verarbeitung mindestens ein geringes Risiko für die Rechte und Freiheiten betroffener Personen existiert.
Demgegenüber ist jedoch Erwägungsgrund 80 DS-GVO (https://ds-gvo.gesundheitsdatenschutz.org/html/ds-gvo_2016_erwgr_080.php) zu entnehmen, dass es Verarbeitungen gibt, welche wahrscheinlich kein Risiko beinhalten.

- (Normales) Risiko
- Voraussichtlich kein Risiko
- Kein Risiko

Das Risiko soll anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung kein Risiko, voraussichtlich kein Risiko, ein normales (im Sinne des „Lebensrisikos“[11]), erhebliches oder ein hohes Risiko in sich birgt.

7.2 Festlegung Schutzbedarf

Gemäß ErwGr. 51 DS-GVO beinhaltet die Verarbeitung der besonderen Kategorien von personenbezogenen Daten, dies sind

- Daten, aus denen die rassische und ethnische Herkunft, hervorgeht,
- Daten bzgl. politischer Meinungen,
- Daten hinsichtlich religiöser oder weltanschaulicher Überzeugungen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung,

immer einen besonderen Schutz verdienen, da „im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.“. Daraus folgt zweierlei:

1) Es muss bei der Verarbeitung dieser Daten ein „besonderer“ Schutz vorhanden sein; Standardmaßnahmen, wie sie für den Schutz bei der Verarbeitung „normaler“ Daten ausreichen, müssen durch zusätzliche Maßnahmen ergänzt werden, die der Anforderung bzgl. des „besonderen“ Schutzbedarf genügen.
2) In ErwGr. 75 und 76 werden Risiken als abhängige Größe von der Eintrittswahrscheinlichkeit und der Schwere der Beeinträchtigung der Rechte und Freiheiten der betroffenen Person beschrieben Risiken. Die in ErwGr. 51 dargestellten möglichen erheblichen Risiken basieren somit einerseits aus der Schwere der Beeinträchtigung, die einer Verarbeitung dieser besonders sensiblen Daten innewohnt, andererseits aus der Wahrscheinlichkeit, mit welcher die Beeinträchtigung der der Rechte und Freiheiten der betroffenen Personen eintreten *könnte*.

Der in ErwGr. 51 DS-GVO angesprochene „besondere“ Schutz muss also geeignet sein, die Eintrittswahrscheinlichkeit soweit zu reduzieren, dass durch diese Maßnahmen für die Dauer der Verarbeitung **kein** hohes Risiko vorliegt. Andernfalls muss der Verantwortliche, wenn auf die Verarbeitung nach Feststellung des Ergebnisses nicht verzichtet wird, vor Beginn der Verarbeitung gemäß Art. 36 Abs. 1 die zuständige Aufsichtsbehörde konsultieren.

7.3 Risikominimierung

Zur Risikominimierung sind technische (in der Regel IT-bezogene) und organisatorische (z. B. Dienstanweisungen) Maßnahmen zu treffen. Gemäß Art. 32 DS-GVO werden im Anhang „Technische und organisatorische Maßnahmen“ Maßnahmen zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit detailliert beschrieben.

[11] Bzgl. Lebensrisiko siehe auch: BGH Urt. V. 1993-05-04, AZ VI ZR 283/92. Online, zitiert am 2019-08-23; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993&Aktenzeichen=VI%20ZR%20283/92

7.4 Gewährleistung der Sicherheit der Daten

Die Erfüllung der Anforderungen von Art. 32 DS-GVO wird detailliert in der zu dieser DSFA gehörenden Excel-Tabelle dargestellt. Im Nachfolgenden wird eher ergänzend auf einige Punkte eingegangen.

7.4.1 Pseudonymisierung personenbezogener Daten

Standardmäßig ist eine Pseudonymisierung im KIS nicht möglich, ohne hierbei zugleich eine Gefährdung der Gesundheit von Patienten zu riskieren. Durch das Rollen- und Berechtigungskonzept ist gewährleistet, dass auf Patientendaten nur Berechtigte Zugriff haben. Bedingt durch die Notwendigkeit, sich bei der medizinischen Behandlung eines Patienten untereinander zu besprechen, müssen die Patientendaten in identifizierender Form vorliegen.

In wenigen Fällen besonderer Personengruppen, z. B. Personen des öffentlichen Lebens („Very Important Person, VIP“) oder Angestellten unseres Krankenhauses selbst, kann eine Pseudonymisierung trotz der damit verbundenen Risiken, die dies für die jeweilige Person bedeutet, sinnvoll sein. Ob dann eine Pseudonymisierung erfolgt und die damit verbundenen gesundheitlichen Risiken in Kauf genommen werden, wird nach entsprechender Aufklärung in Abstimmung mit der betroffenen Person entschieden.

Für die Testdatenbank, welche für Schulungszwecke eingesetzt wird, wird ein Anonymisierungstool verwendet, welches u. A. die nachfolgen Funktionen hat:

- Anonymisierung von Personendaten wie Vorname, Name, Geburtsdatum etc.
- Anonymisierung von Adressdaten wie Straße, Hausnummer, Postleitzahl, Ort etc.
- Generierung neuer Patientenidentifikatoren (PIDs)
- Generierung neuer Fallnummern
- Umbenennung bzw. Sperrung von Applikationsbenutzern
- Anonymisierung oder Umbenennung von Organisationseinheiten
- Löschen von Schnittstellen- und Auditdaten

7.4.2 Verschlüsselung personenbezogener Daten

Bei elektronischer Übertragung von Patientendaten an externe Empfänger erfolgt regelmäßig eine Verschlüsselung. Im Rahmen von gesetzlich vorgeschriebenen Übermittlungen sind die rechtlichen Vorgaben bindend.

Bei einem elektronischen Export (z. B. als pdf-Datei) von Patientendaten entscheidet der jeweilige Anwender, ob eine Verschlüsselung erfolgen soll oder nicht, da die Nutzung einer Verschlüsselung nur abhängig von den Möglichkeiten des Empfängers der Daten entschieden werden kann; grundsätzlich wird die Verschlüsselung hierbei empfohlen.

Verbindliche Vorgaben der betroffenen Person werden beachtet.

Bzgl. der Verschlüsselungstechnik können nur die Möglichkeiten unseres KIS-Herstellers genutzt werden, der sich an den Vorgaben des BSI orientiert[12].

[12] BSI: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Online, zitiert am 2017-09-03; Verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

7.4.3 Zugriff auf die personenbezogene Daten

Der Zugang zu den Daten erfolgt entsprechend der Vorgaben, die in unserem Berechtigungskonzept dargestellt wurden. Grundsätzlich richtet sich der Zugriff auf personenbezogene Daten nach dem „Need-to-know“-Prinzip.

Gegenüber externen Zugriffen ist das Netzwerk durch den Einsatz einer Firewall geschützt. Ein Intrusion Detection System achtet zudem darauf, ob innerhalb unseres Netzwerkes nicht legitimierte Vorgänge erfolgen. Beide Systeme benachrichtigen bei Bedarf das entsprechende Personal, so dass auch von extern nur legitime Zugriffe möglich sind.

Im Berechtigungskonzept ist dargestellt, welche Rechte welcher Rolle zugeteilt werden und wer die jeweilige Entscheidung der Zuteilung von Rollen auf beschäftigte treffen darf.

7.4.4 Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten

Näheres siehe Archivierungs- und Backupkonzept, hier erfolgt nur eine kurze Beschreibung zur Darstellung der getroffenen Maßnahmen.

Einsatz eines Spiegelservers:

Alle Daten werden auf einen anderen Server „gespiegelt“, d. h. es wird also ein 1:1-Abbild erstellt. Der Spiegelserver steht dabei in einem anderen Brandabschnitt als der eigentliche Server. Die Synchronisierung erfolgt asynchron, daher ist das „Spiegelbild“ nicht immer aktuell. Vielmehr erfolgt die Spiegelung stündlich.

Bei einem Zwischenfall erfolgt hierdurch einerseits nur ein möglichst geringer Datenverlust, andererseits wird der Produktivverlust begrenzt, da seitens der Anwender die Ausfallzeit minimiert wird.

Backup:

Ein Sicherungs-System wird zentral bereitgestellt. Dabei erfolgt eine Datensicherung nach dem „Generationenprinzip“. D. h. es wird gewährleistet, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen („Großvater“, „Vater“ und „Sohn“, daher Generationenprinzip) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu haben. Die Tagessicherung entspricht dabei dem „Sohn“, die Wochensicherung dem „Vater“ und die Monatssicherung dem „Großvater“

Die Langzeitsicherung erfolgt grundsätzlich auf entsprechenden Bändern oder einem vergleichbaren Sicherungsmedium. Die Lagerung der Bandsicherungen erfolgt in einem anderen Brandabschnitt als dem Standort der Server.

Eine „Rücksicherung wird probehalber quartalsweise für einzelne Datensätze, 1xjährlich für die gesamte Datenbank in einem Testsystem durchgeführt.

7.4.5 Beschreibung des Verfahrens zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen

Dies wird durch den Einsatz des Spiegelservers wie auch des Backup-Konzepts gewährleistet

7.4.6 Beschreibung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Interne Prüfungen der Einhaltung der vorliegend definierten Standards können zu jeder Zeit, auch unangekündigt, durch den Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten durchgeführt werden. Grundsätzlich erfolgen interne Prüfungen regelmäßig. Die Ergebnisse einer entsprechenden Prüfung werden dem zuständigen IT Verantwortlichen und dem zuständigen Geschäftsführer in Berichtform übersendet.

Zur Ergänzung interner Prüfaktivitäten können auch externe Prüfungen durch den Verantwortlichen veranlasst werden. Die Vorgehensweise bei externen Prüfungen ist vergleichbar mit dem Vorgehen bei internen.

7.5 Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung

Grundsätzlich stellt jede Verarbeitung von personenbezogenen Daten für die betroffenen Personen ein Risiko bzgl. des Missbrauchs ihrer Daten dar. Bedingt durch die Sensibilität sowohl von Gesundheitsdaten als auch von genetischen Daten, die bei der Patientenbehandlung zwangsläufig verarbeitet werden müssen, ist auch das Risiko für die betroffenen Personen entsprechend hoch.

Daher wurden Maßnahmen getroffen, die das Risiko für betroffene Personen minimieren:

- Ein Berechtigungskonzept beschränkt den berechtigten Zugriff auf die Personen, die entsprechend dem „Need-to-know“-Prinzip Zugriff auf die Daten benötigen
- Pseudonymisierung wird dort eingesetzt, wo es möglich ist.
- Wann immer es angebracht ist, werden Daten verschlüsselt. Eine elektronische Übermittlung erfolgt nur verschlüsselt.
- Sicherheitskonzepte wie der Einsatz eines Spiegelungsservers als auch ein differenziertes Backupkonzept gewährleisten eine Minimierung von Ausfallzeiten und die Wiederherstellbarkeit der Daten.
- Eine Firewall bewacht den Datenverkehr nach extern.
- Ein Intrusion Detection System überwacht den internen Netzbereich auf unerwünschte Vorgänge.
- Regelmäßige Schulungen unserer Beschäftigten zu Fragen bzgl. Datenschutz und IT-Sicherheit gewährleisten eine entsprechende Awareness bei dem bei uns eingesetzten Personal.

Sämtliche Maßnahmen zur Gewährleistung der Sicherheit der Daten wurden dabei stets aus dem Blickwinkel „Safety first“ gewählt. D. h. an erster Stelle steht in unserem Krankenhaus immer die Sicherheit der Patientenversorgung und die Minimierung von Risiken für die Gesundheit unserer Patienten.

Eine detaillierte Darstellung der Maßnahmen sowie der Risikobewertung erfolgt in der zu dieser DSFA gehörenden Excel-Tabelle.

8 Begleitende Unterlagen

- ☐ Archivierungskonzept bzw. Archivordnung
- ☒ Berechtigungskonzept
- ☐ Backupkonzept
- ☐ Datenschutzkonzept bzw. Datenschutzrichtlinie
- ☐ IT-Sicherheitskonzept
- ☒ Löschkonzept
- ☐ Notfall-Handbuch
- ☒ Protokollierungskonzept
- ☒ Verfahrensverzeichnis der verantwortlichen Stelle bzw. Verzeichnis von Verarbeitungstätigkeiten
- ☒ Vertrag zur Auftragsverarbeitung mit KIS-Hersteller
- ☒ Musterdokumente
  - ☒ Patienteninformation bzw. Patientenaufklärung bzgl. Betroffenenrechte
  - ☐ Patienteneinwilligungen soweit für Verarbeitung im KIS relevant

9 Fazit

9.1 Zusammenfassung

Die Durchführung der DSFA, einschließlich der Risikoanalyse,

- erfolgte korrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen. Die DSFA verlief positiv. ☒
    - **Empfehlung: Nutzung der Verarbeitungstätigkeit**
- erfolgte korrekt. Die festgelegten Maßnahmen entsprechen allerdings im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend. ☐
  Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.
- erfolgte unter Punkt [ ] unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen und sind ausreichend. ☐
  Eine erneute Betrachtung mit einhergehender Nach-Folgenabschätzung unter Punkt [ ] ist notwendig.
- erfolgte unter Punkt [ ] unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend. Weitere Maßnahmen sind ausgeschlossen. Die DSFA verlief negativ. ☐
    - **Empfehlung: Meldung Aufsichtsbehörde**

9.2 Bewertung

Das Gremium der DSFA kommt zu folgendem Ergebnis:

☒ Die DSFA, einschließlich Risikoanalyse, verlief **positiv**. Die Verarbeitungstätigkeit geht unter Umsetzung der technisch-organisatorischen Maßnahmen in die Nutzung über.

☐ Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.

☐ Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung ist nicht möglich.

9.3 Entscheidung bzgl. Information Aufsichtsbehörde

Variante 1

Die Einbeziehung der Aufsichtsbehörde

- ☐ ist auf Grund des Ergebnisses der DSFA und der Tatsache, dass die Verarbeitungstätigkeit trotz des Ergebnisses durchgeführt werden soll, notwendig.
- ☐ ist nicht notwendig, da die Verarbeitungstätigkeit auf Grund des Ergebnisses der DSFA nicht durchgeführt wird.
- ☒ ist nicht notwendig, weil entsprechende Maßnahmen zur Eindämmung des Risikos getroffen wurden.

9.4 Nächster Prüfungstermin

Die nächste Prüfung erfolgt alle 3 Jahre bzw. vorher, wenn sich Begleitumstände, die eine erneute DSFA erforderlich erscheinen lassen, ändern.

Anhang 1: Technisch-Organisatorische Maßnahmen

1.1 Organisatorische Maßnahmen

1.1.1 Allgemeine Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Personalverwaltungssoftware zur Erfassung der Verpflichtungen aller Beschäftigten ☐ Anderes:	☒ Es wurde ein Datenschutzbeauftragter benannt und dieser verfügt über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe ☐ Der Schutzbedarf der Daten wurde festgelegt und die Daten entsprechenden Schutzklassen zugeordnet ☒ Folgende Verpflichtungen werden bei allen Beschäftigten durchgeführt: ☒ Verpflichtungen auf das Datengeheimnis ☒ Verpflichtungen auf die berufliche Schweigepflicht ☐ Verpflichtungen auf das Fernmeldegeheimnis ☐ Verpflichtungen auf die Wahrung von Geschäftsgeheimnissen ☐ Anderes

1.1.2 Schulungsmaßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz einer eLearning-Plattform ☐ Personalverwaltungssoftware zur Ermittlung, Benachrichtigung und Erfassung der Teilnahme von Datenschutz-Schulungen ☐ Anderes:	☒ Jeder Mitarbeiter erhält jährlich eine Unterweisung im Datenschutzrecht ☐ Jeder Mitarbeiter erhält jährlich eine bereichsspezifische Unterweisung bzgl. der Umsetzung datenschutzrechtlicher Anforderungen ☐ Es werden jährlich Maßnahmen zur Steigerung der Awareness bzgl. Datenschutz durchgeführt ☐ Es werden jährlich Maßnahmen zur Steigerung der Awareness bzgl. IT-Sicherheit durchgeführt ☐ Anderes

1.1.3 Dokumentation

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☒ Es existiert ein Datenschutzkonzept für das Krankenhaus ☐ Es existiert ein Berechtigungskonzept für das Krankenhaus ☒ Es existiert ein IT-Sicherheitskonzept für das Krankenhaus ☐ Es existiert ein Notfall-Handbuch für das

Technische Maßnahmen	Organisatorische Maßnahmen
	Krankenhaus ☐ Es existiert ein Backupkonzept für das Krankenhaus ☒ Es existiert ein Archivierungskonzept für das Krankenhaus ☐ Es existiert ein Löschkonzept für das Krankenhaus ☐ Es existiert ein Protokollierungskonzept für das Krankenhaus ☒ Es existiert ein Verzeichnis der Verarbeitungstätigkeiten für das Krankenhaus

1.2 Spezielle Technisch-Organisatorische Maßnahmen

1.2.2 Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zur Zuordenbarkeit erforderlichen zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass der Verantwortliche keinen Zugriff auf diese Informationen hat.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Bei einer Pseudonymisierung werden Zuordnungsdaten in einem getrennten und abgesicherten System aufbewahrt, auf welche die pseudonymen Daten verarbeitende Personen keinen Zugriff haben ☒ Bei einer Pseudonymisierung werden Zuordnungsdaten in verschlüsselt aufbewahrt und die pseudonymen Daten verarbeitende Personen haben keinen Zugriff auf die Schlüssel ☐ Eine Pseudonymisierung erfolgt immer im jeweiligen Quellsystem ☐ Eine Prüfung auf Inplausibilitäten und Dopplungen im Vorfeld einer Pseudonymisierung erfolgt grundsätzlich automatisiert	☒ Es werden alle Daten pseudonymisiert verarbeitet oder es existiert eine Begründung, warum eine pseudonyme Verarbeitung nicht möglich ist

1.2.3 Verschlüsselung

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Automatische Verschlüsselung von Daten, die auf über USB angeschlossene externe Datenträger gespeichert werden ☒ Verschlüsselung von Notebooks	☒ Es ist gewährleistet, dass die Erzeugung des Schlüssels bzw. Schlüsselmaterials ein sicherer Prozess ist ☐ Es ist gewährleistet, dass der Erzeugung des

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Verschlüsselung von Tablets ☐ Verschlüsselung von Smartphones ☐ Elektronische Signatur von allen E-Mails ☐ Verschlüsselung von E-Mails, wenn Schlüssel des Empfängers bekannt sind ☐ Anderes	Schlüssels bzw. Schlüsselmaterials eine qualitativ hochwertige Zufallszahlenquelle zugrunde liegt ☒ Es ist sichergestellt, dass der Salt und/oder der Schlüssel bzw. das Schlüsselmaterial derart erzeugt werden, dass diese weder vorhersagbar sind noch erraten werden können ☒ Es ist gewährleistet, dass die Vertraulichkeit des Schlüssels bzw. des Schlüsselmaterials während des vollständigen Lebenszyklus der verarbeiteten personenbezogenen Daten gewährleistet ist ☒ Es ist sichergestellt, dass der Zugriff auf den Salt und/oder den Schlüssel bzw. das Schlüsselmaterial auf ein absolutes Minimum vertrauenswürdiger Anwender beschränkt ist ☒ Es werden ausschließlich Standard-Verschlüsselungsalgorithmen entsprechend den Empfehlungen anerkannter Organisationen verwendet ☒ Es ist sichergestellt, dass das verwendete Verfahren eine hinreichende Stärke sowie keinerlei bekannte Schwächen aufweist ☒ Es ist gewährleistet, dass der Schlüssel geheim gehalten wird ☒ Es ist sichergestellt, dass ausschließlich Standard-Hash-Funktionen verwendet werden, für die es keine bekannten Schwachstellen gibt ☒ Es ist sichergestellt, dass bei Verwendung von Hash-Funktionen ein Salt benutzt wird ☐ Es ist sichergestellt, dass der Salt von ausreichender Qualität ist? (Mindestentropie von 100 Bit) ☒ Es ist gewährleistet, dass der Salt geheim gehalten wird ☒ Es liegt ein Konzept zum Schlüsselmanagement vor und dieses enthält Informationen sowohl zum Schlüsseltausch als auch zur Feststellung von Vorgehensweisen bei Kompromittierung ☐ Anderes:

1.2.4 Vertraulichkeit

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, schützen

personenbezogene Daten vor unbefugtem physischen Zugriff. D.h. unbefugte Personen erhalten keinen physischen Zugriff auf Datenträgern, auf denen personenbezogene Daten gespeichert sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude ☒ Sicherheitstür(en) ☒ Magnetkarte ☒ Chipkarte ☐ Transponderkarte ☒ Schlüssel / Manuelles Schließsystem ☐ Schließsystem mit Codesperre ☒ Einbruchmeldeanlage ☒ Brandmeldeanlage ☒ Videoüberwachung ☐ Biometrische Verfahren ☐ Elektronische Signatur ☐ Andere: ☐ Der Zutritt zum Rechenzentrum ist wie folgt gesichert ☒ Alarmanlagen ☐ Vergitterte Fenster/Sicherheitsfenster, -schlösser, -türen mit einer definierten Widerstandsklasse ☐ Lichtschächte ☐ Lüftungsöffnungen ☐ Rollos gegen Hochschieben gesichert ☐ Feuerleiter ☐ Bewegungsmelder ☐ Andere: ☐ Die Server befinden sich in abschließbaren Serverschränken ☐ Gelagerte Notebooks befinden sich unter Verschluss in gesicherten Räumen ☐ Die Aufbewahrung von Datensicherungen (z. B. Bänder, CDs) erfolgt in zutrittsgeschützten Safes oder Räumen ☐ Anderes:	☒ Es existiert ein Zutrittskontrollsystem, in welchem die zutrittsberechtigten Mitarbeiter festgelegt sind ☒ Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude ☒ Empfang / Rezeption / Pförtner ☐ Besucherbuch / Protokoll der Besucher ☒ Verschließen von Türen und Fenstern, sobald Personal nicht im Raum ☒ Mitarbeiterausweise ☐ Besucherausweise ☒ Werkschutz/Wachpersonal ☐ Andere: ☐ Es bestehen Regelungen für den Zutritt von Fremdpersonal, Reinigungspersonal, Besucher ☐ Die Begleitung von Gästen im Gebäude ist in einer Richtlinie geregelt ☐ Differenzierte Sicherheitsbereiche/-zonen (z. B. für Server, Großrechner, Archiv) sind festgelegt ☐ Die Datenträger sind Bestandteil des Zutrittsschutzkonzepts ☐ Es liegt eine Anweisung zur Ausgabe von Schlüsseln vor ☐ Anderes:

Zugangskontrolle

Maßnahmen zur Zugangskontrolle dienen der Verhinderung der unbefugten Nutzung von Anlagen/Systemen, mit welchen (personenbezogene) Daten verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Die unbefugte Nutzung von IT-Systemen wird wie folgt verhindert ☒ User-ID ☒ Benutzername/Passwort ☐ Biometrische Kontrolle ☐ Automatische Bildschirmsperre mit Passwortaktivierung	☒ Es existiert eine Benutzerverwaltung, in welcher Benutzern Authentifizierungsmöglichkeiten zugewiesen werden ☐ Es gibt eine Richtlinie zur Vergabe und Nutzung von Passwörtern ☒ Jeder Berechtigte verfügt über ein eigenes

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Sperrung des Kontos nach 3-maligen Fehlversuchen, erneute Anmeldung erst nach 10 Minuten möglich ☐ Vollständige Sperrung des Kontos nach 3aufeinanderfolgenden Fehlversuchen mit kurzfristiger Kontensperrung ☐ Sonstige: ☐ Zwei-Faktor-Authentifizierung, die zwei Faktoren sind ☐ Benutzername/Passwort (statisch) ☐ Einmal Passwort / Hardware Token ☐ Einmal Passwort / Mobiltelefon ☐ PKI / zertifikatsbasierte Anmeldung ☐ SMS Passwort ☐ Sicherheitsfragen ☐ Geo-Lokalisation ☐ Verhaltensbasierend ☐ Geräte-Identifikation ☐ Virtuelle Smartcards ☐ Anderer Faktor: ☐ Passwörter werden ausschließlich verschlüsselt gespeichert ☐ Es existiert ein Mobile-Device-Management-System ☒ Über alle Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt ☐ Die Nutzung von IT-Systemen mithilfe von Einrichtungen der Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert oder zumindest nachvollziehbar gemacht: ☐ Standleitung ☐ Wählleitung mit automatischem Rückruf ☐ Teilnehmerkennung ☐ Ausweisleser ☐ Protokollierung der Systemnutzung und Protokollauswertung ☐ Sonstige: ☒ Automatische Aktivierung eines Sperrbildschirms, wo dies den Arbeitsablauf nicht unzulässig behindert ☐ Sperrung/Deaktivierung von nicht benötigten USB-Ports ☒ Sperrung/Deaktivierung von nicht benötigten Bluetooth-Schnittstellen ☐ Sperrung/Deaktivierung von nicht benötigten WLAN-Schnittstellen ☐ Anderes:	nur ihm bekanntes Passwort ☒ Es existiert ein Mobile-Device-Richtlinie, in welcher der Umgang mit mobilen Geräten festgelegt ist ☒ Neue Schwachstellen in den IT-Systemen werden nach Bekanntwerden gemeldet, analysiert und ggf. behoben, um das Eindringen seitens unbefugter Dritter in die IT-Systeme zu verhindern ☐ Es gibt definierte und erprobte/wirksame Verfahren für die Fachabteilungen und Technik im Fall eines (erfolgten) externen Angriffs auf relevante Daten und Systeme ☐ IT-Systeme werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet ☐ Penetrationstests erfolgen ☐ Jährlich ☐ Alle 2 Jahre ☐ Alle ___ Jahre ☐ Anderes:

Zugriffskontrolle

Hierunter fallen Maßnahmen, welche dafür Sorge tragen sollen, dass die zur Benutzung eines Informationssystems Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und eine unberechtigte Verarbeitung verhindert wird.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Discretionary Access Control (DAC) ☒ Mandatory Access Control (MAC) ☐ Type Enforcement (TE) ☐ Multi-Level Security (MLS) ☒ Role Based Access Control (RBAC) ☐ Attribute-based access control (ABAC) ☐ Context-Based Access Control (CBAC) ☐ Media Access Control ☒ Es liegt eine eindeutige Zuordnung zwischen jedem Datenträger (Laufwerk etc.) und Berechtigten vor (insb. bei Gruppenlaufwerken) ☒ Die Programm- und Dateibenutzung wird protokolliert und stichprobenartig ausgewertet ☐ Werden sog. „Superuser“ Accounts eingesetzt, so erfolgt ein Monitoring sowie eine regelmäßige Kontrolle von Aktivitäten, die mithilfe dieser Benutzerkonten durchgeführt werden ☐ Andere:	☒ Es besteht ein dokumentiertes Berechtigungsmanagement (Berechtigungskonzept), in dem verbindlich geregelt ist, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden ☒ Für jedes eingesetzte Datenbanksystem ist im Berechtigungssystem die Rechte an Datenbanktransaktionen festgehalten ☐ Im Rahmen dieses Berechtigungsmanagements ist manipulationssicher nachweisbar, wer wann welche Berechtigungen innehatte ☒ Es bestehen differenzierte Berechtigungen (z. B. für Lesen, Löschen, Ändern) ☒ Es bestehen differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem ☒ Es besteht eine funktionelle/personelle Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (techn.) ☒ Es existiert eine Benutzerverwaltung, über die Berechtigungen verwaltet werden ☐ Es liegt ein Konzept der Laufwerksnutzung und -zuordnung vor ☐ Die Wiederherstellung von Daten aus Backups ist in einem verbindlichen Verfahren geregelt (wer darf wann auf wessen Anforderung Backup-Daten einspielen?) ☐ Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung ☐ Andere:

Weitergabekontrolle

Hierbei handelt es sich um Maßnahmen, die verhindern, dass Daten unbefugt weitergegeben werden. Insbesondere soll verhindert werden, dass Daten bei einer elektronischen Übertragung bzw. Transport nicht unbefugt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es erfolgt eine Legitimationsprüfung der Berechtigten	☒ Für Übermittlung/Transport der Daten sind Befugte festgelegt

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Folgende Versendungsart(en) personenbezogener Daten besteht/bestehen ☒ Datenträgertransport (z. B. Post, zuverlässiger Boten/Kurier) ☐ Verpackungs- und Versandanschrift ☐ Transportbegleitung und geschlossene Behältnisse ☐ Datenverschlüsselung ☐ E-Mail, ☐ FTP ☒ SSH ☒ VPN (Verschlüsselung) ☒ Sicheres Web-Formular / -Portal ☐ Gesicherte/Verschlüsselte Datenleitung ☒ § 301 FTAM over IP ☐ Sektorenübergreifende Qualitätssicherung nach Sektorenübergreifende Qualitätssicherung ☐ Die Daten werden beim Transport nicht zwischengelagert ☒ Der Versand bzw. Transport der Datenträger wird dokumentiert (z. B. Protokoll wer wann welche Informationen erhalten hat) ☒ Eingang und Ausgang der Datenträger lückenlos dokumentiert ☐ Anderes:	☒ Es ist sichergestellt, dass Transportdienstleister sorgfältig in Hinblick auf Zuverlässigkeit und Sicherheit beim Transport ausgewählt werden ☒ Es ist sichergestellt, dass die Transportbehälter gesichert sind und nur von den berechtigten Stellen geöffnet werden ☒ Folgende ergänzende Maßnahmen sind für Übermittlung/Transport von Daten festgelegt ☒ Entgegennahme und Rückmeldung ☒ Vollständigkeitsprüfung ☐ Richtigkeitsprüfung ☒ Protokollierung (z. B. Datenträger-Begleitzettel) ☒ Betroffene Mitarbeiter sind darüber informiert, wie Datenträger zu transportieren sind ☐ Es ist geregelt, was passieren muss, wenn beim Datenträgertransport Fehler (z. B. Verlust von Datenträgern) auftreten ☐ Es ist geregelt, wer in welcher Art und Weise Zugang zu/Zugriff auf diese Eingangs-/Ausgangs- und Versandprotokolle hat ☐ Es existiert eine Übersicht über alle regelmäßigen elektronischen Übertragungen ☐ Anderes:

Trennungskontrolle

Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Die Daten verschiedener Mandanten werden physisch getrennt verarbeitet ☒ Die Daten verschiedener Mandanten werden logisch getrennt verarbeitet ☐ Die Datensicherungen verschiedener Mandanten erfolgen auf separaten Datenträgern ☐ Es existiert eine Trennung zwischen Test- und Produktivdaten ☐ Sandboxing ☐ Anderes:	☐ Die Daten anderer Mandanten werden von unterschiedlichen Mitarbeitern beim Auftragnehmer verarbeitet, so dass die Gefahr der Weitergabe von Geschäftsgeheimnissen minimiert wird ☐ Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Daten anderer Mandanten Rechnung trägt ☐ Anderes:

Zweckbindung

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Es werden nur solche Daten verarbeitet, die unmittelbar dem eigentlichen Zweck dienen und die zur Erfüllung der Aufgabe oder Durchführung des Prozesses notwendig sind

1.2.5 Integrität

Eingabekontrolle

Diese Maßnahmen sollen dafür sorgen, dass man nachträglich feststellen kann, ob und wenn ja von wem personenbezogene Daten in informationstechnischen Systemen eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung eingegeben hat ☐ Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung geändert hat ☐ Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung gelöscht hat ☐ Es erfolgt eine Protokollierung der Administratorentätigkeiten insbesondere von Anlegen von Benutzern, sowie des Änderns von Benutzerrechten ☐ Anderes:	☐ Es existiert eine Übersicht, welche IT-Systeme die Erfassung personenbezogener Daten ermöglichen ☐ Es sind Benutzerberechtigungen festgelegt und diese sind wie folgt differenziert ☐ Lesen ☐ Ändern ☐ Löschen ☐ Teilzugriff auf Daten bzw. Funktionen ☐ Feldzugriff bei Datenbanken ☐ Andere: ☐ Es sind gesetzlich bestimmte (HGB u. A.) oder unternehmenseigene Aufbewahrungsfristen festgelegt ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden ☐ Es existiert ein Archivierungskonzept in welchem festgelegt ist, welche Daten wie lange aufzubewahren sind und wer unter welchem Umständen Zugriff auf archivierte Daten erhalten darf bzw. muss ☐ Es existiert ein Löschkonzept. In welchem festgelegt ist, wer welche Daten zu welchen Zeitpunkten auf welche Weise löschen darf bzw. muss ☐ Anderes:

Auftragskontrolle

Hierunter fallen Maßnahmen, welche gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es existiert eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen	☒ Auftragsverarbeiter werden ausschließlich nach einer Überprüfung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig

Technische Maßnahmen	Organisatorische Maßnahmen
Arbeitsschritte gewährleistet ☐ Es erfolgen regelmäßig Audits bei Dienstleistern ☐ Jährlich ☐ Alle 2 Jahre ☐ Alle ___ Jahre ☐ Es werden automatisch Nachweise bzgl. der Sicherheit der Verarbeitung (Art. 32 DS-GVO) bei Dienstleistern angefordert ☐ Jährlich ☐ Alle 2 Jahre ☐ Alle ☐ Anderes:	ausgewählt ☐ Es werden nur Auftragsverarbeiter ausgewählt, die einen qualifizierten Datenschutzbeauftragten benannt haben und bei denen der Datenschutzbeauftragte über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe verfügt ☒ Es existiert ein Vertrag zur Auftragsverarbeitung, der den Anforderungen der DS-GVO genügt ☒ Im Vertrag zur Auftragsverarbeitung wird jeder Auftragsverarbeiter vertraglich verpflichtet, dass diese allen seinen Beschäftigten dieselben Geheimhaltungsverpflichtungen auferlegen, die auch für die Beschäftigten des Krankenhauses gelten ☐ Es wurde überprüft, dass der Auftragsverarbeiter ein Verzeichnis der Auftrags-Verarbeitungstätigkeiten führt ☒ Die Leistungsbeschreibung spezifiziert explizit die zulässigen Arbeiten ☒ Die weisungsbefugten Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt ☐ Die zur Entgegennahme und Ausführung von Weisungen des Auftraggebers beim Auftragnehmer befugten Personen sind benannt ☒ Alle Weisungen des Auftraggebers an den Auftragnehmer erfolgen schriftlich ☐ Mitarbeiter des Auftragnehmers erhalten folgende schriftliche Datenschutz-Informationen ☐ Merkblatt ☐ Gesetzestext ☐ Kopie der Verpflichtungserklärung ☐ Andere: ☒ Wenn der Auftragnehmer einen Unterauftragnehmer zur Erfüllung der Auftragsverarbeitung einsetzt, ist gewährleistet ☐ Der Auftragnehmer informiert den Auftraggeber über alle eingesetzten Unterauftragnehmer, die Daten des Auftraggebers verarbeiten ☒ Mit Unterauftragnehmern werden Auftragsverarbeitungsverträge abgeschlossen und die Verträge des Auftragnehmers mit dem Unterauftragnehmern spiegeln die

Technische Maßnahmen	Organisatorische Maßnahmen
	Anforderungen des Auftraggebers an den Auftragnehmer wider ☒ Mit Unterauftragnehmern werden Datenschutzvereinbarungen abgeschlossen, die alle Geheimhaltungsvereinbarungen enthalten, die auch für die Beschäftigten des Auftraggebers gelten ☒ Erfolgt ein Verarbeitung durch den Auftragsverarbeiter oder durch Unterauftragnehmer außerhalb der EU, so wird ein angemessenes Datenschutzniveau gewährleistet durch ☒ EU-Standard-Vertragsklauseln ☐ Verarbeitung in Drittländer mit einem durch die EU-Kommission festgestelltem angemessenem Datenschutzniveau ☐ Privacy-Shield-Vereinbarung ☐ Individualvertrag mit Genehmigung durch die Aufsichtsbehörden ☐ Anderes: ☐ Die meldepflichtigen Vorfälle sind spezifiziert und sowohl den eigenen beschäftigten als auch allen vom Auftragnehmer eingesetzten Personen bekannt, inkl. Personen von ggf. existierenden Unterauftragnehmern ☐ Auf Anforderung kann belegt werden, dass der jeweilige Auftrag strikt nach den Weisungen des Auftraggebers durchgeführt wurde ☐ Anderes:

1.2.6 Verfügbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder zufälligen Verlust geschützt sind.

Backup- und Recoverykonzept

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es existiert ein Brandschutz, insbesondere Feuer- und Rauchmeldeanlagen ☒ Im Serverraum ist ein Feuerlöscher verfügbar ☒ Der Serverraum ist klimatisiert ☒ Im Serverraum erfolgt eine Überwachung von Temperatur und Feuchtigkeit ☒ Jeder Server ist mit einer unterbrechungsfreien Stromversorgung (USV) verbunden	☒ Es existiert ein angemessenes Backup- und Recoverykonzept ☐ Es ist festgelegt, welche Daten für welchen Zeitraum gesichert werden und die anschließende Löschung der Daten ist gewährleistet ☒ Das „Haltbarkeitsdatum“ der Sicherungsbänder wird beachtet ☐ Es gibt eine Vereinbarung bzgl. Übergabe der (Daten-)Sicherungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Ausgesuchte Clients, insbesondere Clients von Administratoren, sind mit unterbrechungsfreien Stromversorgung (USV) verbunden ☒ Es werden Hardware-RAID-Systeme eingesetzt ☒ Im Serverraum sind Schutzsteckdosenleisten im Einsatz ☐ Der Serverraum wird mit einer Videoanlage überwacht ☐ Es existiert eine Alarmanlage, welche ein unbefugtes Eindringen in den Serverraum meldet ☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.) ist vorhanden ☒ Backups werden regelmäßig auf Datenvollständigkeit kontrolliert ☐ Die Sicherung bezieht auch Notebooks und nicht vernetzte Systeme mit ein ☐ Es wird regelmäßig überprüft, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist ☐ Alte oder unbrauchbare Datenträger werden datenschutzrechtlich ordnungsgemäß vernichtet ☒ Es erfolgt eine Festplattenspiegelung ☐ Anderes:	☒ Eine katastrophensichere Aufbewahrung der Datenträger ist sichergestellt ☒ Backups werden (auch) geografisch an von den Servern unterschiedliche Speicherorte aufbewahrt ☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums ☐ Es existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (BCM-Konzept) ☐ Es existiert ein Notfallhandbuch mit Notfallplänen, Darstellung der Notfallorganisation – klare Regelung der Verantwortlichkeiten im Notfall ☐ Anderes:

1.2.7 Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet ☒ Es existiert eine redundante Benachrichtigungsfunktion (z. B. Mail, SMS), welche über Störungen/Ausfälle relevanter IT-Systeme informiert ☒ Es gibt eine unterbrechungsfreie Stromversorgung ☒ Es werden Hardware-RAID-Systeme eingesetzt ☒ Server sind mit redundanter Hardware (Netzteil, Netzwerkkarte, usw.) ausgestattet? ☐ Es sind Ausweich-Rechenzentren vorhanden	☒ Es wurden Single-Points-of Failure identifiziert und durch angemessene Maßnahmen behandelt ☒ Es wurden alle Konfigurationsparameter der benutzten Betriebssysteme und Anwendungen sowie der eingesetzten Protokolle dokumentiert ☐ Es wurden die maximalen Ausfallzeiten für die verschiedenen IT-Systeme (Client, Fileserver, Datenbankserver, usw.) festgelegt ☐ Die zu erreichende Verfügbarkeit für die verschiedenen IT-Systeme (Client, Fileserver, Datenbankserver, usw.) wurde festgelegt ☐ Es wurde festgelegt, welche Person bei welcher Störung oder welchem Ausfall zu

Technische Maßnahmen	Organisatorische Maßnahmen
(Hot- bzw. Cold Stand-by) ☐ Es übernehmen redundante Stand-By-Systeme bei Ausfällen wechselseitig die Prozesse ☐ Anderes:	benachrichtigen ist ☐ Es existiert ein Notfallplan mit Regelungen wie beispielsweise – Wohin können Anwendungen ggf. hin verlagert werden – Welche Server können/müssen ggf. geordnet heruntergefahren werden ☐ Anderes:

Server- und Client-Absicherung

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es existiert für jeden Client ein passendes Image, so dass bei Bedarf der Client jederzeit wiederhergestellt werden kann ☒ Es gibt Reserve-Clients (PC, Laptop, Tablet, Smartphone, …), so dass bei einem Ausfall der Client ausgetauscht und die Arbeit schnellstmöglich wieder aufgenommen werden kann ☒ Folgende Sicherheitssysteme schützen Soft- und/oder Hardware vor Angriffen ☒ Virenscanner ☒ Firewalls ☒ Spamfilter ☐ Verschlüsselungsprogramme ☒ Intrusion-Detection-System ☐ Intrusion-Prevention-System ☐ Andere:	

1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1.3.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Datenschutz-Management-IT-System im Einsatz ☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte nach Bedarf / Berechtigung ☒ Intranet ☐ Wiki ☐ Interne Social Media Platform wie bspw. Blog ☒ Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig durchgeführt	☒ Verantwortlichkeiten sind eindeutig zugewiesen ☒ Rechenschaftspflicht (Nachweis über Einhaltung datenschutzrechtlicher Vorgaben) ☒ Benannter Datenschutzbeauftragter ☐ Extern ☒ Intern ☒ Beschäftigte geschult und auf Vertraulichkeit/Geheimhaltung verpflichtet ☐ Regelmäßige Sensibilisierung der Mitarbeiter ☒ Datenschutz durch Technikgestaltung

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Halbjährlich ☐ Jährlich ☒ Alle zwei Jahre ☐ Alle ____ Jahre ☐ Anderes:	(„Privacy by Design) wird bei allen Verarbeitungsprozessen umgesetzt ☒ Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default) wird bei allen Verarbeitungsprozessen umgesetzt ☒ Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt ☒ Betroffenenrechte werden gewährleistet ☒ Verzeichnis von Verarbeitungstätigkeiten existiert und ist auf dem jeweils aktuellen Stand ☒ Dokumentation aller Verletzungen des Schutzes personenbezogener Daten ☐ Anderes:

1.3.2 Incident-Response-Management (IT-Störungsmanagement)

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet ☒ Intrusion-Detection-System ☐ Intrusion-Prevention-System ☐ Anderes:	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen ☒ Team zum Umgang mit Sicherheitsvorfällen gebildet und Team beinhaltet ☒ Mitglied der Geschäftsführung ☒ IT-Leiter ☒ Datenschutzbeauftragter ☐ IT-Sicherheitsbeauftragter ☒ Mitglied der Pressestelle/Öffentlichkeitsarbeit ☒ Im Vorfall involvierte Personen ☒ Dokumentation von Sicherheitsvorfällen und Datenpannen ☐ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen beschrieben und etabliert ☐ Anderes:

1.4 Ergänzende Maßnahmen

☐ Zertifizierung nach ISO 27001

☐ Zertifizierung nach ISO 27701

☐ Zertifizierung nach IT-Grundschutz

☐ Verhaltensregeln nach Art. 40 DS-GVO: _____

Verarbeitung Krankenhaus-Informations-System (KIS) „Complete Recovery“ **Datum: 13.12.2019**

Beurteilung Erforderlichkeit einer Datenschutz-Folgenabschätzung: **DSFA erforderlich**

Frage / Prüfung	Ja/Nein
Birgt die Verarbeitung der personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten der Betroffenen?	Ja
Insbesondere prüfen (mehr als 2 Kriterien legen Vermutung nahe, dass DSFA erforderlich ist):	
Einsatz neuer Verarbeitungstechnologien, d. h. Technologien, zu denen der Verantwortliche noch keine DSFA durchgeführt hat	
Einsatz neuer Verarbeitungen, d. h. Verfahren der Verarbeitung personenbezogener Daten, zu denen der Verantwortliche noch keine DSFA durchgeführt hat	
Verarbeitung großer Datenmengen	Ja
Verarbeitung von Daten einer großen Anzahl betroffener Personen	Ja
Verarbeitungen, welche betroffenen Personen die Wahrnehmung ihrer aus der DS-GVO resultierenden Rechte erschweren	
Soll mit der Verarbeitung die Persönlichkeit des Betroffenen systematisch und automatisiert bewertet werden, sodass rechtliche oder andere intensive Eingriffe für den Betroffenen daraus resultieren bzw. resultieren können?	
Sollen umfangreiche Mengen von Daten, die zu den besonderen Kategorien gehören, verarbeitet werden?	Ja
Sollen umfangreiche Mengen von Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden?	
Sollen öffentlich zugängliche Räume überwacht werden?	
Befindet sich die Verarbeitung auf der vom EU Datenschutz-Ausschuss genehmigten Blacklist der nationalen Aufsichtsbehörde?	
Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfin- dung mit Rechtswirkung oder ähn- lich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	
Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, , wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfin- dung mit Rechtswirkung oder ähn- lich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	
Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS- GVO handelt	
Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	
Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können	
Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden	

Verarbeitung Krankenhaus-Informations-System (KIS) „Complete Recovery“ **Datum: 13.12.2019**

Beurteilung Erforderlichkeit einer Datenschutz-Folgenabschätzung: **DSFA erforderlich**

Frage / Prüfung	Ja/Nein
Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	
Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	
Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	
Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	
Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	
Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	
Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	
Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	
Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte	
Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	
Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen.	
Ausnahmetatbestand: Liegt eine Datenschutz-Folgenabschätzung im Sinne des Art. 35 Abs. 10 DS-GVO vor und wurde seitens des für den Verantwortlichen geltenden Mitgliedsstaates keine darüber hinausgehende DSFA angeordnet?	Nein
Azsnahmetatbestand: Existiert eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohem Risiko i.S.v. Art. 35 Abs. 1 Satz 2 DS-GVO?	Nein
Ausnahmetatbestand: Steht die Verarbeitung auf einer „White-List“ gemäß Art. 35 Abs. 5 DS-GVO?	Nein

Verarbeitungstätigkeit:						Riskoanalyse VOR Maßnahmenfestlegung				
lfd. Nr.	Risiko-ursprung	Risiken	Risikobeispiele	Risiko-quellen	Risiko-verantwort-licher	Schadens-höhe	Eintritts-wahrschein-lichkeit	Risiko-bewertung	Risiko-bewäl-tigung	Maß-nahmen
		nach Erwägungsgrund 83 DS-GVO				- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko	Risiko-vermeidung, minimierung, handhabung,	
		Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatisch	Bitte Auswahl anklicken	Bitte Auswahl anklicken
1.	Allgemein	Informationsfehlerhaftigkeit	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness
2.	Allgemein	Informationsfehlerhaftigkeit	Unbefugtes Eindringen in IT-Systeme	Hacker, Lust am „Spielen“		Normal	Niedrig		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, Firewall
3.	Allgemein	Informationsfehlerhaftigkeit	Schadprogramm	Software, Schaden		Hoch	Hoch		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, Virenscanner, Backup
4.	Allgemein	Verlust personenbezogener Daten	Diebstahl von Geräten, Datenträgern und Dokumenten	Hardware, Verlust		Hoch	Mittel		Risikominimierung	Verfügbarkeit / Backupkonzept, Verschlüsselung auf Datenträger
5.	Allgemein	Veränderung personenbezogener Daten	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Hoch	Niedrig		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness
6.	Allgemein	Unbefugter Zugang zu personenbezogenen Daten	Offenlegung schützenswerter Informationen	Hacker, Finanzieller Vorteil		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, Firewall
7.	Allgemein	Unbefugte Offenlegung personenbezogener Daten	Offenlegung schützenswerter Informationen	Beschäftigter, Vorsatz		Hoch	Niedrig		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz
8.	Allgemein	Dauerhafte Verfügbarkeit (negativer) Informationen	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Protokollierung
9.	Allgemein	Schamgefühl und Ansehensverlust	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Protokollierung
10.	Allgemein	Finanziellen Verlust	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz
11.	Allgemein	Arbeitsrechtlicher Kontext	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz
12.	Allgemein	Gesellschaftlich-politische Risiken	Missbrauch personenbezogener Daten	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz
13.	Allgemein	Diskriminierung	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung	Vertraulichkeit / Zugriffskontrolle, und Verarbeitungskontrolle, Protokollierung Schulung / Informationssystem, Datenschutz
14.	Allgemein	Informationsfehlerhaftigkeit	Ausfall von Geräten oder Systemen	Hardware, Verlust		Sehr hoch	Mittel		Risikohandhabung	Belastbarkeit / Ausfallsicherheit / Technische Maßnahmen: Wiederherstellbarkeit in Zeitspanne, die keine Gefährdung der Patientenbehandlung sicherstellt, gewährleistet und Verfahren wird regelmäßig aufFunktionsfähigkeit geprüft; Prüfung wird dokumentiert Backup garantiert eine zusätzliche Möglichkeit der Wiederherstellung, allerdings mit einem höheren Zeitaufwand
15.	Aufnahme	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness, Prüfung der richtigen Zuordnung bei Gesprächen mit Patienten in allen Behandlungseinrichtungen
16.	Aufnahme	Falsche Zuordnung von Daten	Falsches Einlesen der Krankenversichertenkarte	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness, Aufnahmekraft spricht jeden Patienten mit den Namen der Versichertenkarte ab
17.	Behandlung	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Übermüdung/Überlastung		Hoch	Mittel		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness, Verfahrensanweisung: dass Identitäts-Daten aus dem KIS grundsätzlich mit Patienten abgestimmt werden
18.	Abrechnung	Falsche Zuordnung von Daten	Fehlerhafte Dokumentation/Dateneingabe	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung	Beschäftige prüfen im Rahmen der Plausibilität grundsätzliche alle abrechnungsrelevanten Informationen und halten im Zweifellsfall Rücksprache mit den für die Behandlung verantwortlichen Beschäftigten
19.	Allgemein	Enttäuschung von Vertraulichkeitserwartungen	Ausfall oder Störung von Kommunikationsnetzen	Hardware, Überlastung: Ausfall Stromversorgung		Normal	Mittel		Risikominimierung	Belastbarkeit / Ausfallsicherheit / Technische Maßnahmen: Untebrechungsfreie Stromversorgung
20.								x		
21.								x		
22.								x		
23.								x		

Verarbeitungstätigkeit:						Riskoanalyse NACH Maßnahmenfestlegung				
lfd. Nr.	Risiko-ursprung	Risiken	Risikobeispiele	Risiko-quellen	Risiko-verantwort-licher	Schadens-höhe	Eintritts-wahrschein-lichkeit	Risiko-bewertung	Risiko-bewäl-tigung	Maß-nahmen
		nach Erwägungsgrund 83 DS-GVO				- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko	Risiko-vermeidung, minimierung, handhabung,	
		Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatisch	Bitte Auswahl anklicken	Bitte Auswahl anklicken
1.	Allgemein	Informationsfehlerhaftigkeit	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
2.	Allgemein	Informationsfehlerhaftigkeit	Unbefugtes Eindringen in IT-Systeme	Hacker, Lust am „Spielen“		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
3.	Allgemein	Informationsfehlerhaftigkeit	Schadprogramm	Software, Schaden		Normal	Mittel		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
4.	Allgemein	Verlust personenbezogener Daten	Diebstahl von Geräten, Datenträgern und Dokumenten	Hardware, Verlust		Hoch	Niedrig		Risikohandhabung	Versicherung gegen Hardwareschaden sowie Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
5.	Allgemein	Veränderung personenbezogener Daten	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Niedrig	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
6.	Allgemein	Unbefugter Zugang zu personenbezogenen Daten	Offenlegung schützenswerter Informationen	Hacker, Finanzieller Vorteil		Normal	Mittel		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
7.	Allgemein	Unbefugte Offenlegung personenbezogener Daten	Offenlegung schützenswerter Informationen	Beschäftigter, Vorsatz		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
8.	Allgemein	Dauerhafte Verfügbarkeit (negativer) Informationen	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
9.	Allgemein	Schamgefühl und Ansehensverlust	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
10.	Allgemein	Finanziellen Verlust	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
11.	Allgemein	Arbeitsrechtlicher Kontext	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
12.	Allgemein	Gesellschaftlich-politische Risiken	Missbrauch personenbezogener Daten	Unbefugte Verarbeitung		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
13.	Allgemein	Diskriminierung	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
14.	Allgemein	Informationsfehlerhaftigkeit	Ausfall von Geräten oder Systemen	Hardware, Verlust		Normal	Mittel		Risikohandhabung	Verfügbarkeit / Recoverykonzept
15.	Aufnahme	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Fahrlässigkeit		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
16.	Aufnahme	Falsche Zuordnung von Daten	Falsches Einlesen der Krankenversichertenkarte	Beschäftigter, Fahrlässigkeit		Niedrig	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
17.	Behandlung	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Übermüdung/Überlastung		Niedrig	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
18.	Abrechnung	Falsche Zuordnung von Daten	Fehlerhafte Dokumentation/Dateneingabe	Beschäftigter, Fahrlässigkeit		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
19.	Allgemein	Enttäuschung von Vertraulichkeitserwartungen	Ausfall oder Störung von Kommunikationsnetzen	Hardware, Überlastung: Ausfall Stromversorgung		Normal	Niedrig		Risikohandhabung	Versicherung gegen Datenpannen, so dass Betroffenen finanzielle Schäden ersetzt werden können
20.								x		
21.								x		
22.								x		
23.								x		

Verarbeitungstätigkeit:						Ergebnis
lfd. Nr.	Risiko-ursprung	Risiken	Risikobeispiele	Risiko-quellen	Risiko-verantwort-licher	Verfahren kann durchgeführt werden
		nach Erwägungsgrund 83 DS-GVO				
		Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Freitext	Bitte Auswahl anklicken
1.	Allgemein	Informationsfehlerhaftigkeit	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Restrisiko akzeptabel
2.	Allgemein	Informationsfehlerhaftigkeit	Unbefugtes Eindringen in IT-Systeme	Hacker, Lust am „Spielen“		Restrisiko akzeptabel
3.	Allgemein	Informationsfehlerhaftigkeit	Schadprogramm	Software, Schaden		Restrisiko akzeptabel
4.	Allgemein	Verlust personenbezogener Daten	Diebstahl von Geräten, Datenträgern und Dokumenten	Hardware, Verlust		Restrisiko akzeptabel
5.	Allgemein	Veränderung personenbezogener Daten	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Restrisiko akzeptabel
6.	Allgemein	Unbefugter Zugang zu personenbezogenen Daten	Offenlegung schützenswerter Informationen	Hacker, Finanzieller Vorteil		Restrisiko akzeptabel
7.	Allgemein	Unbefugte Offenlegung personenbezogener Daten	Offenlegung schützenswerter Informationen	Beschäftigter, Vorsatz		Restrisiko akzeptabel
8.	Allgemein	Dauerhafte Verfügbarkeit (negativer) Informationen	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Restrisiko akzeptabel
9.	Allgemein	Schamgefühl und Ansehensverlust	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Restrisiko akzeptabel
10.	Allgemein	Finanziellen Verlust	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Restrisiko akzeptabel
11.	Allgemein	Arbeitsrechtlicher Kontext	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Restrisiko akzeptabel
12.	Allgemein	Gesellschaftlich-politische Risiken	Missbrauch personenbezogener Daten	Unbefugte Verarbeitung		Restrisiko akzeptabel
13.	Allgemein	Diskriminierung	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Restrisiko akzeptabel
14.	Allgemein	Informationsfehlerhaftigkeit	Ausfall von Geräten oder Systemen	Hardware, Verlust		Restrisiko akzeptabel
15.	Aufnahme	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Fahrlässigkeit		Restrisiko akzeptabel
16.	Aufnahme	Falsche Zuordnung von Daten	Falsches Einlesen der Krankenversichertenkarte	Beschäftigter, Fahrlässigkeit		Restrisiko akzeptabel
17.	Behandlung	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Übermüdung/Überlastung		Restrisiko akzeptabel
18.	Abrechnung	Falsche Zuordnung von Daten	Fehlerhafte Dokumentation/Dateneingabe	Beschäftigter, Fahrlässigkeit		Restrisiko akzeptabel
19.	Allgemein	Enttäuschung von Vertraulichkeitserwartungen	Ausfall oder Störung von Kommunikationsnetzen	Hardware, Überlastung: Ausfall Stromversorgung		Restrisiko akzeptabel
20.						
21.						
22.						
23.						

Risikomatrix **vor** Maßnahmenplanung

		Eintrittswahrscheinlichkeit					
Kein Risiko	x		hoch	0	0	1	0
Voraussichtlich kein Risiko	x						
(Normales) Risiko	x		mittel	0	1	13	1
Erhebliches Risiko	x						
Hohes Risiko	x		niedrig	0	1	2	0
Untragbares Risiko	x						
				niedrig	normal	hoch	sehr hoch
				Schadenshöhe			

Risikomatrix **vor** Maßnahmenplanung

		Eintrittswahrscheinlichkeit					
Kein Risiko	x		hoch	0	0	0	0
Voraussichtlich kein Risiko	x						
(Normales) Risiko	x		mittel	0	3	0	0
Erhebliches Risiko	x						
Hohes Risiko	x		niedrig	3	12	1	0
Untragbares Risiko	x						
				niedrig	normal	hoch	sehr hoch
				Schadenshöhe			