

Datenschutzkonzept

1. Präambel

Der Schutz der personenbezogenen Daten der Patienten der Rehabilitationsklinik HolsingVital unterliegt der höchsten Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz in der Rehabilitationsklinik berücksichtigt und umgesetzt, gelebt wird. Bei HolsingVital wird für die Datenverarbeitung nach folgendem Datenschutzkonzept verfahren:

Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung

der **Integrität** (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
der **Vertraulichkeit** (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
der **Verfügbarkeit** (z. B. Schutz vor Diebstahl oder Zerstörung)
gewährleistet werden.

Die Sicherheitsmaßnahmen werden in dem Datenschutzkonzept in die Bereiche

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Nutzung der Internetdienste
- Nutzung der Telekommunikationsdienste und
- Zusatzmaßnahmen für sensible personenbezogene Daten

gegliedert und geben mithin ein hohes Sicherheitsniveau vor. Die festgelegten Sicherheitsmaßnahmen gelten als Mindestanforderungen für HolsingVital.

2. Datenschutzrechtliche Rahmenbedingungen

Das Erheben und Verarbeiten personenbezogener Daten ist im Bundesdatenschutzgesetz, in der europäischen Datenschutzgrundverordnung und im Telemediengesetz geregelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (so genannter Betroffener).

Im Bereich der Rehabilitationsklinik gelten zusätzlich landesrechtliche Regelungen wie das Landesdatenschutzgesetz sowie bereichsspezifische Regelungen, die speziell für in Kliniken erhobene Gesundheitsdaten konzipiert wurden.

Generell gilt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn gesetzliche Vorschriften dies ausdrücklich zulassen oder der Betroffene ausdrücklich eingewilligt hat. Die Einwilligung ist nur wirksam, wenn der Nutzer über die Tragweite des Verfahrens informiert wurde, dies heißt, welche Daten zu welchem Zweck in welcher Form gespeichert und verarbeitet werden und die Einwilligung nicht in anderen Erklärungen versteckt worden ist.

Die Auftragserteilung erfolgt über Sozialleistungsträgern (§ 23 SGB I). Für diese gilt das Sozialgeheimnis, das konkret in den Vorschriften zum Sozialdatenschutz (§ 35 SGB I in Verbindung mit §§ 67 bis 85a SGB X) geregelt ist. Diese Vorschriften zur Wahrung des Sozialgeheimnisses sind von den Rehabilitationseinrichtungen in Bezug auf die Daten von Versicherten, die ihnen übermittelt wurden, grundsätzlich neben den Bestimmungen der DSGVO zu beachten (§ 78 SGB X).

Es gehört zu den gesetzlichen Aufgaben der DRV, Leistungen zur Prävention, zur medizinischen Rehabilitation, Leistungen zur Teilhabe am Arbeitsleben und zur Nachsorge zu erbringen (§ 23 Abs. 1 Nr. 1 Buchst. a SGB I in Verbindung mit §§ 14 ff SGB VI). Diese Leistungen zur Teilhabe kann die DRV in Einrichtungen durchführen lassen, mit denen Verträge nach § 97 SGB X und § 38 SGB IX in Verbindung mit § 15 Abs. 6 SGB VI abgeschlossen wurden.

Zur Durchführung der Leistungen werden Sozialdaten auch in Form von medizinischen Daten der Rehabilitandinnen / Rehabilitanden von den Rentenversicherungen und Krankenkassen an die Einrichtungen und von diesen regelmäßig in Form von Dokumentationen, Zwischenberichten, Belastungs-erprobungen, Stellungnahmen, Abschlussberichten oder Rehabilitations-entlassungsberichten – bei Zulässigkeit- an die Stellen übermittelt.

Die Übermittlung von Sozialdaten an die Rehabilitationseinrichtung ist zulässig nach § 69 Abs. 1 Nr. 1 SGB X. Danach dürfen Sozialdaten zur Erfüllung einer eigenen gesetzlichen Aufgabe übermittelt werden. Die gesetzliche Aufgabe ist hier die Erbringung von Leistungen zur Teilhabe im Sinne des

§ 23 Abs. 1 Nr. 1 Buchst. a SGB I in Verbindung mit §§ 14 ff SGB VI. Handelt es sich bei den zu übermittelnden Sozialdaten zusätzlich um medizinische Daten, ist neben § 69 Abs. 1 Nr. 1 SGB X auch § 76 SGB X zu beachten.

Bezüglich der Verarbeitung von medizinischen Daten durch die Einrichtungen wird insbesondere auf Art. 9 DSGVO in Verbindung mit den §§ 67 ff SGB X und § 22 BDSG verwiesen.

Verantwortlich für den vertraulichen und datenschutzkonformen Umgang mit allen personenbezogenen Daten der Rehabilitandinnen ist die

Rehabilitationsklinik Holsing Vital, die allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Art. 4 Nr. 7 DSGVO).

Die Rehabilitationseinrichtung hat sämtliche Aufgaben unter Beachtung der Regelungen der DSGVO und weiterer Datenschutzgesetze zu erfüllen, beispielsweise die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 und 2 DSGVO) sowie des Sozialdatenschutzes (§ 15 Abs. 3 Nr. 5 SGB VI), zu dem die Klinik sich vertraglich verpflichtet. Siehe auch Punkt 6.

3. Inhalt und Zweck des Konzeptes

Grundvoraussetzung für den Datenschutz ist die Datensparsamkeit. Daraus resultiert, dass nicht mehr Daten als benötigt verwendet werden. Als zweiten

zentralen Punkt sehen wir die Notwendigkeit, Daten so früh als möglich zu pseudonymisieren bzw. zu anonymisieren.

4. Beteiligte, speichernde Stelle im Sinne des Datenschutzes

Die beteiligte speichernde Stelle im Sinne des Datenschutzes ist die HolsingVital GmbH. Diese wird durch das Leitungsteam vertreten (s.u.), der Geschäftsführer ist Herr Jens Friedrich Holsing. Zum Zeitpunkt der Erstellung (bzw. Überarbeitung) dieses Konzeptes 14.11.2019 gehören dem Leitungsteam an:

- Jens F. Holsing, Geschäftsführer
- Bogumil Pajak, Chefarzt Orthopädie
- Gudrun Horbach, Chefärztin VOR

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt bei der Geschäftsführung.

5. Verpflichtung zum Datenschutz

HolsingVital eingeschlossen ihrer Mitarbeiter /-innen und Subunternehmer, verpflichten sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen haben eine entsprechende Datenschutzerklärung zur Geheimhaltungspflicht unterzeichnet. Siehe Punkt 6.

6. Beschreibung der personenbezogenen Daten und Angabe der jeweiligen Zweckbindung (Nutzungszweck)

6.1 Kundendaten / Patientendaten

Bei dem betroffenen Personenkreis handelt es sich um Patienten der Rehabilitationsklinik *HolsingVital*.

Bei den Daten handelt es sich einerseits um Daten des Patienten selbst (z.B. Geburtsdatum bzw. Alter zum Zeitpunkt der Aufnahme), andererseits um bei deren Diagnostik und Behandlung anfallende Daten als auch um Ortsdaten (z.B. Geburtsort, -land, Wohnort, -land) der von *HolsingVital* betreuten Patienten. Die Daten werden zu Zwecken der Patientenbehandlung, Forschung und der Qualitätssicherung eingesetzt, entsprechend den Aufgaben, welche unsere Rehabilitationsklinik zu erfüllen hat.

6.1.1 Rechtsgrundlage

Die Rechtsgrundlage zur Nutzung der erhobenen Patientendaten zu Patientenversorgung, Lehre, Forschung und Qualitätssicherung bilden die nachfolgend genannten Gesetze.

Bezüglich der Verarbeitung von medizinischen Daten durch die Einrichtungen wird insbesondere auf Art. 9 DSGVO und § 22 BDSG verwiesen. Medizinischen Daten sind besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO). Deren Verarbeitung ist ausschließlich unter den weiteren Bedingungen des Art. 9 (spez. Abs. 2) DSGVO in Verbindung mit den §§ 67 ff SGB X und nationaler Ausführungsgesetze (vor allem § 22 BDSG) möglich.

§ 67 Abs. 2 SGB X in Form von Zuweisungsunterlagen, diese Sozialdaten unterliegen durch die Zweckbindung und § 15 Abs. 3 Nr. 5 SGB VI weiterhin dem Sozialgeheimnis

§ 203 Strafgesetzbuch (StGB) Ärztinnen / Ärzte und sonstige Schweigepflichtige sind danach verpflichtet, über das zu schweigen, was ihnen die Rehabilitandinnen anvertraut haben.

Die personenbezogenen Daten von Rehabilitandinnen dürfen nur verarbeitet werden, wenn sie zur Durchführung der Prävention, medizinischen Rehabilitation, Leistungen zur Teilhabe am Arbeitsleben oder Nachsorge und zur Abrechnung mit der DRV erforderlich sind (Art. 6 Abs. 1 Buchst. c DSGVO, Art. 9 Abs. 2 Buchst. h DSGVO i. V. m. § 22 Abs. 1 Nr. 1 b BDSG) oder die Versicherten (nach entsprechender Information) ausdrücklich und freiwillig eingewilligt haben (Art. 6 Abs. 1 Buchst. a DSGVO, Art. 9 Abs. 2 Buchst. a DSGVO i. V. m. Art. 7 DSGVO)

§ 630f BGB, § 10 Abs. 1 MBO-Ä verpflichtende Norm zum Führen einer Patientenakte.

Patientenbehandlung: Siehe oben, sowie §§ 630a ff BGB, DSGVO

Qualitätssicherung: siehe oben, sowie §135a SGB V, §137 SGB V, Richtlinie gemäß § 137 Abs. 1 SGB V i. V. m. § 135 a SGB V über Maßnahmen der Qualitätssicherung für nach § 108 SGB V zugelassene Krankenhäuser

Forschung: Siehe oben, desweiteren ist eine Einwilligung der betroffenen Personen erforderlich. Die Einwilligung muss dabei freiwillig und informiert erfolgen und inhaltlich hinreichend bestimmt sein (Art. 7 DSGVO).

§ 30 der Gewerbeordnung (GewO): Konzession zum Betrieb der HolsingVital GmbH als Privatkrankenanstalt, Urkunde, Minden, 8.9.2006

Versorgungsvertrag nach § 111 SGB V: Medizinische Vorsorgeleistung, Anschlußheilbehandlung, Vertrag vom 28.11.1990

Zulassung zur Erbringung von Leistungen der ambulanten Rehabilitation nach § 40 SGB V: Leistungen zur ambulanten medizinischen Rehabilitation, Zulassung vom 1.09.2005

§ 125 SGB V: Abgabe ambulanter Heilmittel, Vertrag vom 14.05.1991

6.2 Mitarbeiterdaten

Gehaltsabrechnung

Mitarbeiterbeurteilung

QM-System / Organigramm

Stundendokumentation

6.3 Personenbezogene Daten für Geschäftszwecke entsprechend § 29 BDSG

7. Verfahrensbeschreibung

Für automatisierte Verfahren sind nach §4 BDSG unter anderem

der Zweck,

der wesentliche Inhalt,

die Ergebnisse der Vorabkontrolle.

die Technik mit Hard- und Software und

die Angaben zur Art der Verarbeitung sowie den Schutzmaßnahmen

in einer Verfahrensbeschreibung festzulegen und auf dem neuesten Stand zu halten.

Das Verzeichnis wird vom Datenschutzbeauftragten geführt, per Dienstanweisung ist geregelt, dass alle Führungskräfte den Datenschutzbeauftragten bei der Führung des Verzeichnisses größtmögliche Unterstützung geben.

Sowie in den technisch organisatorischen Maßnahmen (TOM) beschrieben.

8. Beschreibung der Gewährleistung von Betroffenenrechten

Rechte auf Auskunft (§§19, 34), Berichtigung, Löschung (Vergessenwerden) und Sperrung (§§20,35) ebenfalls im BDSG, Art. 13 DSGVO

*das Recht auf Information (Art. 13, 14 DSGVO),
das Recht auf Akteneinsicht (§ 630g BGB)
das Recht auf Auskunft über die gespeicherten Daten (Art. 15 DSGVO und § 10 Abs. 2 MBO-Ä, § 630g BGB)
das Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten (Art. 16 - 18 DSGVO),
das Recht auf Schadensersatz (Art. 82 DSGVO),
das Recht auf Widerspruch gegen die Verarbeitung von Daten (Art. 21 DSGVO)
das Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 77 DSGVO)*

*Entsteht durch eine unzulässige Verarbeitung personenbezogener Daten von Rehabilitandinnen / Rehabilitanden diesen ein materieller oder immaterieller Schaden,
haben die betroffenen Personen ein Recht auf Schadenersatz (Art. 82 DSGVO).*

Informationsrecht des Betroffenen hält fest, dass, der betroffenen Person v.a. die Kontaktdaten des Verantwortlichen der verarbeitenden Stelle, der Zweck (für jede einzelne Datenverarbeitung gesondert) und die Dauer der Datenverarbeitung sowie Auskunfts- und Widerspruchsrechte ebenso die Rechtsgrundlage der Datenverarbeitung und eine nachvollziehbare Interessenabwägung mitgeteilt werden. Allgemein muss der Betroffene über alle Betroffenenrechte informiert werden, also über das eines Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit.

Dabei ist zu berücksichtigen, dass der betroffenen Personen die Informationen sofort bei Datenerhebung übermittelt werden, dies geschieht im Aufnahme Gespräch und bei der Unterzeichnung des Klinikvertrages, wo er dies in der Datenschutzerklärung unterschreibt.

Auskunftsrecht (Art. 15 DSGVO) Dem Informationsrecht korrespondiert ein Auskunftsrecht des Betroffenen. Dieser kann in angemessenen Abständen Auskunft über die Datenverarbeitung, v.a über den Zweck, darüber welche Daten verarbeitet werden und über den Empfänger verlangen.

Das Recht auf Berichtigung (Art. 16 DSGVO) resultiert eine Datenverarbeitung in unrichtigen personenbezogen Daten des Betroffenen, so hat dieser ein Recht auf unverzügliche Berichtigung. Dabei ist jedoch der Zweck der Verarbeitung zu berücksichtigen, sodass etwa bei Datenverarbeitungen im öffentlichen Interesse eine längere Zeitspanne bis zur Berichtigung angesetzt werden kann.

Das Recht auf Datenlöschung, „Das Recht auf Vergessenwerden“ Art. 17 DSGVO regelt „Das Recht auf Vergessenwerden“. Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen. Allerdings greift diese Regelung nur ein, wenn einer der folgenden vier Gründe eingreift:

Das Speichern der Daten ist zur Zweckerreichung der Datenerhebung nicht mehr notwendig
Der Betroffene widerruft seine Einwilligung in die Datenverarbeitung
Die Daten wurden unrechtmäßig verarbeitet

Das Unternehmen ist aufgrund einer gesetzlichen Pflicht (aus dem EU-Recht oder dem nationalen Recht eines Mitgliedstaates) zur Löschung der Daten verpflichtet.

Unternehmen muss das Recht auf Vergessenwerden nicht umsetzen, wenn:

Die Meinungs- und Informationsfreiheit überwiegen
Das Speichern der Daten einer rechtlichen Verpflichtung entspricht
Das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt
Wissenschaftliche oder historische Forschungszwecke oder Archivzwecke überwiegen
Die Daten zur Wahrung von Rechtsansprüchen erforderlich sind

Das Recht auf Einschränkung der Verarbeitung Gemäß Art. 18 DSGVO hat der Betroffene ein Recht auf Einschränkung der Verarbeitung. Dieses Recht greift, wenn

der Betroffene die Richtigkeit der Daten in Frage stellt,
die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden nachdem der Zweck der Datenverarbeitung sich erledigt hat oder der Betroffene Widerspruch nach Art. 21 DSGVO eingelegt hat.

Recht auf Datenübertragbarkeit – Art. 20 DSGVO

Es beinhaltet für den Betroffenen die Möglichkeit gespeicherte Daten automatisch auf einen anderen Anbieter übertragen zu lassen.

9. Verfahren zur Pseudonymisierung und Anonymisierung inklusive Risikoabschätzung

Die Verfahren zur Pseudonymisierung und Anonymisierung werden nach dem jeweils nach dem aktuellen Stand der Technik durchgeführt.

Pseudonymisierung und Anonymisierung sind in der Regel immer dann notwendig, wenn Daten aus den klinischen Informationssystemen extrahiert und weitergegeben werden, es sei denn, es existiert eine gesetzliche Grundlage, die dies anders regelt oder der Patient willigte in der Weitergabe seiner Daten ein.

10. Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz

Entsprechend den datenschutzrechtlichen Bestimmungen (z.B. §78a SGB X in Verbindung mit der Anlage zu § 78a) sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität, siehe 10.2),

personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit, siehe 10.3),

jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität, siehe 10.4),

festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit, siehe 10.5),

die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz, siehe 10.06).

10.1 Vertraulichkeit

10.1.1 Zutrittskontrolle

Der Zugang zu den Räumlichkeiten ist nur autorisierten Personen möglich. Berechtigt sind alle Mitarbeiter/-innen von *HolsingVital*.

Die Sicherheit des Gesamtverfahrens, gewährleistet durch die organisatorischen Maßnahmen (TOM).

10.1.2 Zugangskontrolle

Der elektronische Zugang zu den Systemen von *HolsingVital* ist durch heutige technische Standards und Verschlüsselungen gesichert.

Zugangsdaten zur Administration und Wartung der Dienste sind Administratoren und verantwortlichen Mitarbeitern des Vertragspartners UKD bekannt. Die Passwörter werden regelmäßig geändert.

Die Sicherheit des Gesamtverfahrens, gewährleistet durch die organisatorischen Maßnahmen (TOM)

10.1.3 Zugriffskontrolle

Der Datenzugriff ist ausschließlich über unsere Softwarelösungen möglich und nach Mandanten getrennt. Die Mandantendaten sind logisch voneinander getrennt und
Version 2023, freigegeben durch Datenschutzbeauftragte

verfügen jeweils über eine eigenständige Benutzer- und Zugriffsverwaltung für die Vergabe individueller Zugriffsberechtigungen.

Die Sicherheit des Gesamtverfahrens, gewährleistet durch die organisatorischen Maßnahmen (TOM)

10.1.4 Weitergabekontrolle

Eine elektronische Weitergabe (Übertragung) von Daten erfolgt automatisiert mittels standardisierter Export-Schnittstellen innerhalb der Anwendungsumgebung. Der Zugriff auf Schnittstellen wird anwendungsseitig auf Basis der Berechtigungen gesteuert. Die Zugangskontrolle erfolgt anhand der eingesetzten technischen Komponenten.

Die Verfahren zur Übertragung an weitere Stellen (Dritte) werden anhand einer Schnittstellenspezifikation definiert und sind in der Ausführung durch den Auftraggeber steuerbar, die technischen Eigenschaften und Verfahren dann spezifisch in Abstimmung mit dem Auftraggeber definiert und innerhalb der Dokumentation berücksichtigt. In dieser Abhängigkeit sind ggfs. zusätzliche datenschutzrechtliche Regelungen mit Dritten zu vereinbaren.

10.2 Integrität

10.2.1 Eingabekontrolle

Anwendungsseitig ist gewährleistet, dass berechtigte Benutzer (i.d.R. Administratoren) nachträglich feststellen können, wann und von wem personenbezogene Daten erfasst, verändert oder entfernt worden sind. Die Dokumentation erfolgt zum Kundendatensatz und ist nicht manipulierbar.

10.2.2 Auftragskontrolle

Auf Basis der Datenschutzerklärung zur Auftragsdatenverarbeitung wird gewährleistet, dass die Verarbeitung von personenbezogenen Daten nur entsprechend den Weisungen des Vertragspartners (Nutzers) durchgeführt wird.

10.3 Verfügbarkeit

10.3.1 Verfügbarkeitskontrolle

Die Daten werden entsprechend per Backup gesichert.

10.4 Authentizität

Die Authentizität der Daten ergibt sich aus den in den verschiedenen Informationssystemen implementierten Verfahren, die eine Authentizität gewährleisten.

10.5 Revisionsfähigkeit

Die Revisionssicherheit der erhobenen Daten wird gewährleistet durch:

Die Ordnungsmäßigkeit der Datenerhebung und –verarbeitung.

Die Vollständigkeit der administrativen und medizinischen Dokumentation.

Die Sicherheit des Gesamtverfahrens, gewährleistet durch die organisatorischen Maßnahmen (TOM) sowie die entsprechenden Umsetzungen (Sicherheitskonzept).

Die Sicherung vor Verlust der Daten durch ein Backup-Konzept sowie dessen Umsetzung.

Die Gewährleistung, dass eine Nutzung der Daten nur durch Berechtigte erfolgt (Berechtigungskonzept).

Die Einhaltung der gesetzlich geforderten Aufbewahrungsfristen (Archivordnung).

Dokumentation der einzelnen Verfahren in entsprechenden Konzepten.

10.6 Transparenz

Dem Transparenzgebot wird durch dieses Datenschutzkonzept genügt, in dem die Methoden der Erhebung und Nutzung der Daten beschrieben wird. Einzelheiten zu den jeweiligen Studien werden in der jeweiligen Studiendokumentation festgehalten.

10.7 Trennungsgebot

Eine Trennung der Daten erfolgt nach Mandanten.