

- 1. Verantwortlicher:** Herniamed gemeinnützige GmbH
Neue Bergstr. 6
13585 Berlin
Geschäftsführer: Prof. Dr. med. Ferdinand Köckerling
- 2. Datenschutz-Beauftragter:** Datenschutz Winter
Bekscher Berg 16
33100 Paderborn
Tel. 05252 – 93 46 93
email@datenschutz-winter.de
- 3. Rechtsgrundlagen:** Bundesdatenschutzgesetz (BDSG) bis 24.05.2018
EU-Datenschutzgrundverordnung (DS-GVO) ab 25.05.2018
Telemediengesetz (TMG)
Telekommunikationsgesetz (TKG)

Version	Datum	Bearbeiter	Änderungsbeschreibung
1.0	31.01.2017	Datenschutz Winter	Neuerstellung des Dokuments

Inhalt

Datenschutzbeauftragter
Verpflichtung Datengeheimnis
Einwilligung
Betroffenenrechte
Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
Administration
Nutzungsverbot nicht freigegebener Hard- und Software
Zutrittskontrolle
Zugangskontrolle
Zugriffskontrolle
Weitergabekontrolle
Eingabekontrolle
Auftragskontrolle
Verfügbarkeitskontrolle

Einleitung

Das vorliegende Dokument gibt Auskunft über die bei HERNIAMED getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz und zu Datensicherheit, zu deren Gewährleistung sich HERNIAMED gemäß § 9 BDSG verpflichtet.

Regelung der Verantwortlichkeiten

Der/die betriebliche Datenschutzbeauftragte hat die Einhaltung der Regelungen des Datenschutzes sicherzustellen. Da sich im Bundesdatenschutzgesetz auch Vorschriften zur Datensicherheit finden, ist er/sie hierfür ebenfalls mit zuständig.

Für die Einhaltung der Maßnahmen im Bereich Datensicherheit ist primär der IT-Leiter der HERNIAMED verantwortlich.

Datenschutz vs. Datensicherheit

Zweck des Datenschutzes ist es, Kunden, Mitarbeiter und sonstige Betroffene vor Beeinträchtigungen ihres Persönlichkeitsrechts und ihrer Privatsphäre beim Umgang mit ihren personenbezogenen Daten zu schützen.

Datensicherheit bedeutet die Festlegung und Umsetzung technischer und organisatorischer Maßnahmen, um Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der IT-Systeme sowie der der darauf befindlichen Daten sicherzustellen.

Rechtsgrundlage

Die Rechtsgrundlage der Verpflichtung zur Datensicherheit bildet §9 BDSG unter besonderer Berücksichtigung der Anlage (zu § 9 Satz 1):

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Organisation

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (erster Satz der Anlage zu § 9 Satz 1 BDSG).

Maßnahmen

- Definition von Arbeits- und Verfahrensanweisungen sowie Zuständigkeitsregelungen für wesentliche Funktionen und Abläufe im Unternehmen
- Information der Mitarbeiter über die Regelungen
- Überprüfung der Anwendung und Einhaltung der Regelungen
- Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5 BDSG

Datenschutzbeauftragter

Gemäß § 4f, Abs.1 BDSG hat die HERNIAMED gemeinnützige GmbH einen externen Datenschutzbeauftragten schriftlich bestellt.

Die Kontaktdaten des DSB werden auf der WEB-Site des Unternehmens bekanntgegeben.

Name und die Kontaktdaten des DSB werden 2018 an die Aufsichtsbehörde gemeldet.

Verpflichtung Datengeheimnis

Alle Mitarbeiter/innen wurden schriftlich auf das Datengeheimnis verpflichtet.

Formulare

Verpflichtungserklärung für Mitarbeiter/innen der Herniamed gemeinnützige GmbH.

Einwilligung

Es werden keine personenbezogenen Daten der Mitarbeiter/innen veröffentlicht.

Damit Herniamed seine Leistung erbringen kann, verpflichtet sich die jeweilige Klinik/Praxis, eine entsprechende schriftliche Einwilligung der Patienten auf einem von Herniamed zur Verfügung gestellten Formular einzuholen.

Formulare

Einverständniserklärung und Patientenmerkblatt

Betroffenenrechte

Es ist gewährleistet, dass die Betroffenen ihre Rechte auf Auskunft, Berichtigung und Löschung ihrer Daten geltend machen können.

Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

Alle Papierunterlagen werden in einem verschlossenen Container (Deckel mit Schlitz) eines externen Entsorgers untergebracht.

Administration

Die gesamte Administration erfolgt über StatConsult. Die Aufgaben wurden in einem Vertrag festgelegt.

Nutzungsverbot nicht freigegebener Hard- und Software

Es wird keine private Hard- und/oder Software eingesetzt. Freigabe von Hard- und Software nur über die Geschäftsführung.

Zutrittskontrolle

Das Büro der Herniamed gemeinnützige GmbH wurde von der Vivantes GmbH zur Verfügung gestellt. Das Büro ist immer geschlossen und kann über Transponder geöffnet werden. Die Mitarbeiter/innen der Herniamed gemeinnützige GmbH haben über den Transponder bestimmte Zutrittsrechte, die von der Vivantes GmbH festgelegt wurden.

Die Zutrittskontrolle zum Gebäude liegt in der Verantwortung der Vivantes GmbH.

Reinigungsarbeiten erfolgen während der Arbeitszeiten.

Zugangskontrolle

Die Anmeldung am System bei Herniamed erfolgt über eine Benutzerkennung und das Passwort.

Die Software zur Datenerhebung im Projekt Herniamed wurde von der Firma StatConsult entwickelt und basiert auf den Bibliotheken des Studien Design Tools ClinWise-HealthCare.

Der Sensibilität dieser Daten wird mit einer Reihe von Maßnahmen Rechnung getragen. In ClinWise-HealthCare ist sichergestellt, dass alle als sensibel eingestuften Daten ausschließlich von den der entsprechenden Klinik zugewiesenen Mitarbeitern gelesen und verändert werden können. D.h., weder die Studienleitung noch die Administratoren des IT-Systems haben die Möglichkeit, diese Daten einzusehen. Dies führt im Umkehrschluss dazu, dass bei Passwortverlust aller Mitarbeiter einer Klinik die vertraulichen Daten nicht wiederhergestellt werden können. Die Patienten könnten dann nur noch über ihre studienspezifische Patientenkenntung zugeordnet werden.

Der Zugang zur Hardware ist auf autorisierte Personen beschränkt und wird protokolliert.

Der Zugang zur Studie ist nach Eingabe von Login, Passwort und der Auswahl der Klinik möglich. Die Zentren sowie die Zentrenadministratoren werden vom Studienadministrator angelegt. Der Zentrenadministrator muss nach dem Einloggen sein Passwort ändern. Anschließend werden automatisch die für dieses Zentrum geltenden Schlüssel erzeugt und mit dem Passwort des Studienadministrators verschlüsselt in der Datenbank gespeichert. Das Anlegen weiterer Nutzer für diese Klinik kann ausschließlich vom Zentrenadministrator vorgenommen werden.

Details in dem Datenschutzbericht „Auftragsdatenverarbeitung StatConsult, HL komm Telekommunikations GmbH“ und „Datenschutzkonzept ClineWise-Healthcare“.

Zugriffskontrolle

Der Zugriff auf das Betriebssystem ist ausschließlich geschulten Mitarbeitern der Firma StatConsult möglich. Diese sind je nach Aufgabenbereich für die Pflege und Wartung des Betriebssystems, der Datenbank und der entsprechenden ClinWise-Anwendung zuständig.

Zugriff auf sensible Daten: Alle entsprechend gekennzeichneten Daten werden nicht im Klartext in der Projektdatenbank gespeichert. Mittels Private/Public Key Verschlüsselungsalgorithmen (entsprechend den Vorgaben des BSI) ist dafür gesorgt, dass nur autorisierte Mitarbeiter der jeweiligen Klinik Zugriff auf diese Daten haben.

Zugriff auf sonstige Daten: Alle anderen Studiendaten werden in einem relationalen Schema in der Datenbank gespeichert. Diese Daten können von autorisierten Personen jederzeit zu Analyse Zwecken (Klinikadministrator: einzelne Klinik, Studienadministrator: gesamter Pool) exportiert werden.

Details in dem Datenschutzbericht „Auftragsdatenverarbeitung StatConsult, HL komm Telekommunikations GmbH“ und „Datenschutzkonzept ClineWise-Healthcare“.

Weitergabekontrolle

Details in dem Datenschutzbericht „Auftragsdatenverarbeitung StatConsult, HL komm Telekommunikations GmbH“ und „Datenschutzkonzept ClineWise-Healthcare“.

Eingabekontrolle

Details in dem Datenschutzbericht „Auftragsdatenverarbeitung StatConsult, HL komm Telekommunikations GmbH“ und „Datenschutzkonzept ClineWise-Healthcare“.

Auftragskontrolle

Ein schriftlicher Vertrag gem. § 11 BDSG wurde mit der StatConsult GmbH erstellt. QM-Zertifikat gem. DIN EN ISO 13485 wurde für StatConsult-IT Service GmbH erstellt. Im Januar 2016 wurden die technischen und organisatorischen Maßnahmen gem. § 9 BDSG der Fa. StatConsult und HL komm, Leipzig, geprüft.

Bei den Kooperationsverträgen mit den Kliniken handelt es sich um eine Funktionsübertragung. Bei der Funktionsübertragung werden der Herniamed gemeinnützige GmbH eigene Entscheidungsbefugnisse hinsichtlich des „Wie“ und der Auswahl der Daten zustehen. Herniamed erledigt die ihm übertragene Aufgabe selbstständig und die Kliniken können nicht mehr ohne Weiteres durch Weisungen Einfluss nehmen.

Vivantes Klinikum Spandau hat mit einem externen Entsorger von Datenträgern einen Vertrag gem. § 11 BDSG abgeschlossen.

Verfügbarkeitskontrolle

Die Daten werden in einer relationalen Datenbank auf einem Server in einem zertifizierten Rechenzentrum der HL komm in Leipzig gespeichert.

Gem. Audit-Report vom 04.11.2015 wurde die HL komm Telekommunikations GmbH in Leipzig von drei Mitarbeitern der StatConsult IT-Service GmbH geprüft.

Der Server ist mittels hard- und softwarebasierter Firewallssysteme gesichert. Geschulte Administratoren sorgen für eine permanente Überwachung und Aktualisierung des Systems.

Datentransport: Der Zugriff auf die Webanwendung erfolgt über eine mittels verifiziertem Zertifikat gesicherte Verbindung über das Internet (HTTPS).

Details in dem Datenschutzbericht „Auftragsdatenverarbeitung StatConsult, HL komm Telekommunikations GmbH“ und „Datenschutzkonzept ClineWise-Healthcare“.

Gewährleistungsausschluss:

Die Informationen, Daten und Inhalte werden ständig geprüft und aktualisiert. Trotz aller Sorgfalt können sich Angaben zwischenzeitlich verändert haben. Deshalb kann keine Haftung oder Garantie für Richtigkeit, Vollständigkeit und Aktualität übernommen werden.