Datenschutzmanagementsystem

der Hauskrankenpflege Behrens

1. Geltungsbereich

Das Datenschutzmanagementsystem gilt für alle Mitarbeiter, Patienten, Klienten und Zulieferer der Hauskrankenpflege Behrens. Sowie für alle Ärzte, Gesundheitseinrichtungen und Kranken- und Pflegekassen, mit denen eine Zusammenarbeit besteht.

2. Grundsätze des Datenschutzes und Begriffsdefinitionen

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ § 3 Abs. 1 BDSG

Dabei zählen Patientendaten ebenso zu den personenbezogenen Daten wie die Daten der Beschäftigten.

Für unseren Pflegedienst erfolgt die Erhebung und Verarbeitung folgender personenbezogener Daten:

- Name, Adresse, Geburtsdatum
- Telefonnummer
- Foto des Patienten
- Diagnosen und Krankheitsgeschichte
- Kontaktdaten der Angehörigen
- Hausarzt und weitere ärztliche Versorgung
- Biographie und Familienstand
- Versicherungsnummer
- Krankenkasse

Sowie weitere für die Versorgung notwendige körperliche Angaben.

<u>Zweck der Speicherung</u>

Die Erhebung und Speicherung personenbezogener Daten ist in unserem Unternehmen unerlässlich, da die Pflege auf diesen Daten aufbaut und für den täglichen Ablauf zwingend notwendig ist. Die erhobenen Daten dürfen nur für den vorgesehen Zweck verwendet werden. Des Weiteren werden diese Daten für die Zusammenarbeit mit Ärzten, Apotheken und anderen pflegerischen Stellen benötigt, um z.B. Medikamente nachzubestellen oder Verordnungen einzuholen.

Überprüfung und Schulung

Einmal im Jahr gibt es eine Datenschutzschulung für alle Mitarbeiter um Neuerungen bekannt zu geben und an die Einhaltung zu erinnern (ggf. mit Fallbeispielen). Diese wird mit einem Unterweisungsnachweis dokumentiert, welcher im Ordner Datenschutz abgelegt wird.

Die vom Patienten unterschriebene „Einverständniserklärung in die Erhebung und Verarbeitung von Daten durch die Hauskrankenpflege Behrens“ wird in der jeweiligen Patientenakte im Betriebsgebäude aufbewahrt.

Datenlöschung

Alle von uns erhobenen Daten werden vernichtet bzw. gelöscht, sobald sie für die Durchführung des Geschäftsverhältnisses nicht mehr erforderlich sind, das Geschäftsverhältnis beendet wurde und gesetzliche Aufbewahrungsfristen nicht mehr entgegenstehen.

3. Der betriebliche Datenschutzbeauftragte

Betriebliche Datenschutzbeauftragte ist mit Wirkung vom 01.05.2018 Frau Lucienne Kreschnak. Eine schriftliche Bestellung dazu wurde unterschrieben und ist in der Personalakte und im Datenschutzordner einsehbar. Die Aufgaben und Pflichten sind in dieser genau aufgelistet.

4. Erheben, Verarbeiten und Nutzen personenbezogener Daten

Übermittlung und Verarbeitung der Daten

Die Übermittlung von uns gespeicherter personenbezogener Daten ist an folgende Stellen notwendig:

- Kranken-und Pflegekasse des Patienten (z.B. Leistungsnachweise oder Abrechnung per Post)
- Datev und Steuerbüro (Mitarbeiterdaten für Lohnabrechnung, Buchhaltung)
- Medizinischer Dienst der Krankenversicherung (z.B. Wundprotokolle per Post)
- Hausarzt – Anfragen, Anforderungen Medikamentenplan, Verordnungen bestellen, Entlassbericht vom Krankenhaus oder anderen Einrichtungen
- Sozialleistungsträger und Versicherungen
- Meldung gemäß Bundesinfektionsschutzgesetz (bei übertragbaren Krankheiten; auch ohne Zustimmung) – ggf. anonymisiert
- Berufsgenossenschaft (bei Berufskrankheiten)
- Datenschutzbehörde (auch ohne Einwilligungserklärung)
- Sanitätshäuser, Apotheken und Zulieferer (für z.B. IKM)
- Rentenversicherungsträger
- Angehörigen

Die Hauskrankenpflege Behrens wird hiermit von der Schweigepflicht gegenüber diesen Stellen entbunden.

Weitere Angaben siehe Dokument „Einverständniserklärung in die Erhebung und Verarbeitung von Daten durch die Hauskrankenpflege Behrens“.

Datenerhebung

In der Hauskrankenpflege Behrens gelten folgende Grundsätze für das Erheben, Verarbeiten und Nutzen personenbezogener Daten:

Personenbezogene Daten werden grundsätzlich bei Neuaufnahme eines Patienten erhoben. Dies übernehmen Frau Annette Behrens, Frau Doris Walter und Frau Barbara Hundmaier. Die Daten werden im PC (Software Medifox) eingetragen und auf deren Grundlage eine Patientendokumentationsmappe erstellt. Sie wird bis zum Ablauf unserer Versorgung in der Patientenwohnung hinterlegt. Der Patient ist verantwortlich dafür, dass keine Unbefugten Zugang zu der Mappe haben.

Endet die Versorgung, holen wir die Mappe wieder ab und archivieren die Daten laut gesetzlicher Aufbewahrungsfrist 10 Jahre im Betriebsgebäude.

Bei Aufnahme des neuen Patienten wird dieser über die Datenschutzvorschriften belehrt und er unterzeichnet die „Einverständniserklärung in die Erhebung und Verarbeitung der Daten durch die Hauskrankenpflege Behrens“.

Alle Patienten, welche von der Hauskrankenpflege Behrens bereits vorsorgt werden, werden in der Zeit ab dem 14.05.2018 die Einverständniserklärung unterzeichnen. Das Original wird in der Patientenakte in den Räumen der Hauskrankenpflege Behrens aufbewahrt.

Datennutzung

Die personenbezogenen Daten werden von uns im Programm Medifox genutzt (arbeiten nach Bestimmung der DSGVO). Das ist Grundlage aller organisatorischen Arbeiten der Hauskrankenpflege Behrens.

Darüber hinaus werden die Daten schriftlich in der Patientenmappe verwendet sowie im Tourenhandy. Dies ist für die tägliche Versorgung notwendig.

5. Verpflichtung der Mitarbeiter auf das Datengeheimnis

Alle Mitarbeiter unterschreiben bei Aufnahme der Tätigkeit die Anweisung „Verpflichtung auf Einhaltung der Datenschutzvorschriften“, in dem alle Regelungen zum Umgang mit personenbezogenen Daten und der Schweigepflicht niedergeschrieben sind und verpflichten sich so zu deren Einhaltung.

Darüber hinaus findet einmal jährlich eine Schulung aller Mitarbeiter zum Thema Datenschutz statt. In dieser werden sie zusätzlich sensibilisiert, was den Umgang mit personenbezogenen Daten betrifft.

6. Maßnahmenplan

Die Daten sind technisch gegen Missbrauch gesichert. Diesem Gedanken ist dadurch Rechnung zu tragen, dass bei konventionellen Patientenakten und beim Einsatz von Datenverarbeitungstechniken gewährleistet ist, dass sowohl im Empfangsbereich, als auch in den Büroräumen unbefugte Dritte keinen Einblick oder sogar Zugriff in die Patientendaten erhalten.

Alle Daten werden unmittelbar nach ihrer Digitalisierung verschlüsselt. Die Datenbank wird durch eine Firewall geschützt und der Zugang zu den Daten ist durch persönliche Passwörter gesichert.

Alle Verletzungen des Schutzes personenbezogener Daten müssen gemeldet werden, es sei denn, das Risiko einer Verletzung persönlicher Rechte und Freiheiten ist unwahrscheinlich. Die Meldung hat binnen 72 Stunden nach Bekanntwerden der Verletzung zu erfolgen. In Deutschland ist der Bundesbeauftragte für Datenschutz die zuständige Aufsichtsbehörde. Zudem müssen die von einer Verletzung Betroffenen, mithin die Patienten, benachrichtigt werden.

Es sind verschiedene Ursachen möglich, bei denen Daten nach außen gelangen könnten, diese sind im Folgenden aufgeführt:

- das Diensthandy wird während der Tour beim Patienten vergessen -> Mitarbeiter wird nachgeschult und es wird eine schriftliche Ermahnung erteilt

- das Diensthandy oder die Patientenmappe wird verloren -> Mitarbeitergespräch und Abmahnung, da personenbezogene Daten nach außen gelangen

- Sämtliche vertrauliche Unterlagen, die im Dienstauto mitgeführt werden müssen (für oder von den Patienten, Arzt, Apotheke, etc.) sind verdeckt aufzubewahren, damit keiner von außen diese einsehen kann. Außerdem sind die Fenster während des Parkens geschlossen zu halten. Wird dagegen verstoßen hat dies eine Nachschulung des Mitarbeiters zur Folge.

- Zutrittschip für Betriebsgebäude verloren -> Für den Mitarbeiter wird eine neuer Zutrittschip erstellt. Der „verlorene“ wird aus dem System genommen und gesperrt, damit kein Unbefugter Zutritt zum Betriebsgebäude erlangen kann. Bei Beendigung des Arbeitsverhältnisses wird der Zutrittschip abgegeben und aus dem System entfernt.

- Die Daten im Betriebsgebäude könnten nur bei einem Einbruch unbefugt eingesehen werden. Dagegen ist das Gebäude durch Außenrollos und Gitter vor den Vorderfenstern weitestgehend geschützt.

- Falls der Patientenschlüssel verloren geht, ist an diesem kein Patientenname oder anderes lesbar, damit keine Daten nach außen gelangen können. Auf dem Schlüsselanhänger befindet sich nur die Telefonnummer der Hauskrankenpflege Behrens und die Schlüsselnummer. Im Idealfall wird der Schlüssel gefunden und wir werden angerufen und holen diesen beim Finder ab. Es entstand dann kein Schaden und es gelangten keine Daten nach außen. Wird der Schlüssel nicht wiedergefunden, werden andere geeignete Maßnahmen eingeleitet.

In jedem Fall wird die Verletzung der Datenschutzvorschriften in der vorgegebenen Frist bei der Aufsichtsbehörde gemeldet.

7. Hard- und Software

Die Beschaffung von Hard- und Software unterliegt ausschließlich dem Technischen Leiter. Dieser beachtet bei der Beschaffung die gesetzlichen Vorgaben.

Private Hard- und Software ist im Betrieb gestattet. Es wird zusätzlich geprüft, dass keine Firmendaten oder personenbezogenen Daten entwendet werden.

Im Verlustfall eines Diensthandys ist eine Sperrung möglich und wird je nach Einzelfall entschieden und ausgeführt. Das auf den Handys verlinkte OneDrive-Konto wird gelöscht, so dass im Verlustfall kein Zugriff auf Bilder mehr möglich ist.

Das Programm Medifox (ambulant) wird von uns für die Verarbeitung der Daten genutzt und ist mit einem Passwort geschützt. (siehe Anlage Datenschutzordner) Bei Verlust des Diensthandys kann der Zugriff vom Betriebsgebäude aus geschützt werden.

Der Mediendienst Whats App wird von unserem Betrieb für dienstliche Zwecke nicht genutzt. Arbeitsrelevante Fotos müssen in einem extra Ordner gespeichert werden und dürfen nicht per Whats App versendet werden. Stattdessen werden diese direkt am PC hochgeladen und sind dort geschützt. Fotos von anderen Handys werden per E-Mail an die Sekretärin geschickt, die diese Fotos dann ebenfalls im PC sichert.

Erstellt am: 23.05.2018

Erstellt von: Lucienne Kreschnak (Datenschutzbeauftragte)

Freigegeben von: