Datenschutzkonzept für das Forschungsvorhaben DART

Inhalt

Funktion	Name	Datum	Unterschrift
DART gGmbH Geschäftsführer und Datenschutz-beauftragter	PD Dr. Ralf Müller-Rath		

Einleitung

Das vorliegende Datenschutzkonzept beschreibt Maßnahmen zum Datenschutz für das Forschungsvorhaben DART der DART gGmbH. Das Ziel des Deutschsprachigen Arthroskopieregisters (DART) ist es, alle Patienten, welche eine Arthroskopie erhalten, in einem prospektiven, webbasierten, trinationalen Register (Deutschland, Österreich, Schweiz) multizentrisch, standardisiert, systematisch und pseudonymisiert zu erfassen und so den Langzeitverlauf des Eingriffs zu verfolgen.

Rechtsgrundlagen

BDSG/EU-DSGVO

Rechtliche Grundlage für die Verarbeitung der DART-Daten ist eine Einwilligung nach dem BDSG (Bundesdatenschutzgesetz). Ab 25. Mai 2018 ist die rechtliche Grundlage eine Einwilligung nach der EU-DSGVO (EU-Datenschutzgrundverordnung).

Deklaration von Helsinki

Nach der Deklaration von Helsinki (verabschiedet von der 18. World Medical Association (WMA)-Generalversammlung, Juni 1964 Helsinki, in der aktuell gültigen Version) ist für die Teilnahme von Personen an der medizinischen Forschung eine freiwillige, informierte Einwilligung vorzulegen. Dazu sind potentielle Teilnehmer angemessen über die Ziele, Methoden, Geldquellen, eventuelle Interessenkonflikte, institutionelle Verbindungen des Forschers, den erwarteten Nutzen und die potentiellen Risiken der Studie, möglicherweise damit verbundene Unannehmlichkeiten, vorgesehene Maßnahmen nach Abschluss einer Studie sowie alle anderen relevanten Aspekte der Studie zu informieren (aufzuklären). Der potentielle Teilnehmer muss über das Recht informiert (aufgeklärt) werden, die Teilnahme am Forschungsvorhaben zu verweigern oder eine einmal gegebene Einwilligung jederzeit zu widerrufen, ohne dass ihm irgendwelche Nachteile entstehen. Besondere Beachtung soll dem spezifischen Informationsbedarf der individuellen potentiellen Versuchspersonen sowie den für die Informationsvermittlung verwendeten Methoden geschenkt werden. Allen Teilnehmern medizinischer Forschung sollte die Möglichkeit gegeben werden, sich über den allgemeinen Ausgang und die allgemeinen Ergebnisse des Forschungsvorhabens zu informieren.

Grundsätze des Datenschutzes für das Forschungsvorhaben DART

Einwilligung, Widerruf

Die Teilnahme an Forschungsvorhaben DART basiert auf der freiwilligen informierten Einwilligung entsprechend der oben genannten Rechtsgrundlagen. Teilnehmer erhalten eine schriftliche Teilnehmerinformation, in der sie über das Forschungsvorhaben DART, Vor- und Nachteile der Teilnahme und den Datenschutz informiert werden.

Der Widerruf der Einwilligung ist jederzeit ohne Angaben von Gründen möglich. Nur der Teilnehmer selbst bzw. sein gesetzlicher Vertreter kann einen wirksamen Widerruf abgeben. Die Widerrufserklärung muss an den behandelnden Arzt oder die DART gGmbH erfolgen.

Einwilligungen gelten auch für den Fall, dass der Teilnehmer verstirbt, über seinen Tod hinaus.

Verantwortliche Stelle

Die datenschutzrechtlich gesamtverantwortliche Stelle für Daten des Forschungsvorhabens DART ist die DART gGmbH. Der Zweck der Datenverarbeitung ergibt sich aus den Zielen des Projektplans (siehe dort).

Personenbezogene Daten (Arten)

Zu den verarbeiteten personenbezogenen Daten des Forschungsvorhabens DART gehören:

Medizinische Daten:

- Alter
- Zeitpunkt der Arthroskopie
- Symptome bei Erstvorstellung und im Verlauf
- Internationale Klassifikationen von Erkrankungen
- Operationen- und Prozedurenschlüssel
- Befunde von Untersuchungen
- je nach Eingriff und Modul ggf. weitere Daten

Kontaktdaten:

- E-Mail-Adresse

Die E-Mail-Adresse wird in einem vom den medizinischen Daten getrennten Bereich in verschlüsselter Form gespeichert.

Pseudonymisierung

Für das Forschungsvorhaben erfolgt die Speicherung und Verarbeitung der medizinischen Registerdaten in pseudonymisierter Form. Für die Vergabe des Pseudonyms ist das lokale Behandlungsteam verantwortlich. Die Anzahl der Personen, welche von diesen Pseudonymen Kenntnis erlangen, ist begrenzt. Die Zuordnung des Pseudonyms zu identifizierenden Daten (z.B. Name, Alter, Geburtsjahr/-datum des Patienten) ist nur am Behandlungsort des Patienten (teilnehmendes Zentrum/Klinik) möglich.

Auswertedatensätze/Auswertung

Die wissenschaftliche Auswertung der erhobenen Daten kann im Rahmen von Forschungsprojekten durch Wissenschaftler innerhalb und außerhalb der DART gGmbH erfolgen, z.B. durch das Studienzentrum des Universitätsklinikums Freiburg. Dafür werden nur die für die jeweilige Forschungsfrage benötigten Daten unter besonderer Berücksichtigung des sich daraus ggf. ergebenden Re-Identifikationsrisikos zu einem projektbezogenen Auswertedatensatz zusammengestellt und für das Forschungsprojekt verfügbar gemacht. Heißt: Sollten personenbezogene Daten zur Auswertung an Dritte weitergegeben werden, erfolgt dies ausschließlich in anonymisierter Form. Über die Bereitstellung der Auswertedatensätze zur wissenschaftlichen Auswertung entscheiden die DART gGmbH.

Regelhafter Datensatz

Die erhobenen Daten werden regelmäßig in Grafiken oder Tabellen zur Übersicht in zusammengefasster Art und Weise für die teilnehmenden Zentren und Patienten zur Verfügung gestellt. Rückschlüsse auf Daten einzelner Patienten sind aus diesen Übersichten nicht möglich. Zudem hat jedes Zentrum Zugriff auf die Daten der jeweils eigenen Patienten. Zugriff auf den Gesamtdatensatz haben lediglich die DART gGmbH oder von der DART gGmbH Beauftragte, wie z. B. Mitarbeiter des Studienzentrums der Universitätsklinik Freiburg (für Hinweise zum Gesamtdatensatz s. Auswertedatensätze).

Datenzugriff und Verschlüsselung

Personenbezogene Daten des Forschungsvorhabens DART dürfen nur auf solchen Rechnern gespeichert werden, die eine Authentisierung von Nutzern voraussetzen

(Zugangsschutz) und der Zugriff auf die personenbezogenen Daten darf nur entsprechend authentisierten Nutzern möglich sein. Die Registerdaten des Forschungsvorhabens DART werden (solange sie nicht als Auswertedatensätze vorliegen) auf Rechnern der Uniklinik Freiburg gespeichert und verarbeitet. Für das Forschungsvorhaben DART werden die personenbezogenen Registerdaten auf dem System RDE-LIGHT des Studienzentrums des Universitätsklinikums Freiburg verarbeitet. Die Registerdaten werden auf dem System RDE-Light in verschlüsselter Form gespeichert. Eine Übermittlung sämtlicher Daten über das Internet findet nur verschlüsselt, nach dem aktuellen Stand der Technik statt. Dabei wird für die Übermittlung der Daten eine SSL verschlüsselte Verbindung genutzt (SHA-256 mit RSA-Verschlüsselung). Weiterhin findet die Datenspeicherung auf einem, vom Web-Server getrennten Datenbankserver statt. E-Mail Adressen der Patienten werden getrennt von den restlichen Daten gespeichert und zusätzlich in der Datenbank verschlüsselt (passwortbasiert, MD5 und Triple-DES) gespeichert.

Eine Speicherung von personenbezogenen Daten auf mobilen Datenträgern (z. B. USB-Speichersticks, DVDs) soll vermieden werden und ist nur zulässig, wenn die Daten/Dateien nach dem aktuellen Stand der Technik verschlüsselt sind und das Passwort geheim gehalten wird.

IT-System RDE-LIGHT

Das IT-System RDE-LIGHT ist ein elektronisches Dateneingabesystem für klinische Studien und andere Projekte in der klinischen Forschung, welches am Studienzentrum des Universitätsklinikums Freiburg entwickelt wurde. Die Erfassung der Daten erfolgt papierlos und direkt vor Ort in der jeweiligen Klinik über einen Webbrowser. Die webbasierte Eingabe der Daten erfolgt über eine nach Stand der Technik sichere Transportverschlüsselung (https). Das System verfügt über ein Rollen- und Rechtekonzept und erfüllt alle Anforderungen der Guten Klinischen Praxis (ICH-GCP). Entsprechende Zertifikate zur Datensicherheit liegen vor. Der Zugriff auf das System erfolgt unter Verwendung persönlicher Benutzerkennungen und der Verwendung von Passworten mit Passwortregeln (z. B. erzwungener Passwortwechsel nach erstem Login, Mindestkomplexität des Passwortes). Die Daten werden über Formulare im Webbrowser erfasst und in einem zentralen Server im Rechenzentrum des Universitätsklinikums Freiburg gespeichert. Eine tägliche Sicherung schützt vor Datenverlust. Die Betriebssysteme des Servers werden regelmäßig und bei Bedarf aktualisiert, so dass Sicherheitslücken, soweit sie bekannt sind, schnellstmöglich entfernt werden. Zur Nachvollziehbarkeit sämtlicher Änderungen bei der Eingabe von Daten in das System werden alle Änderungen im System protokolliert.

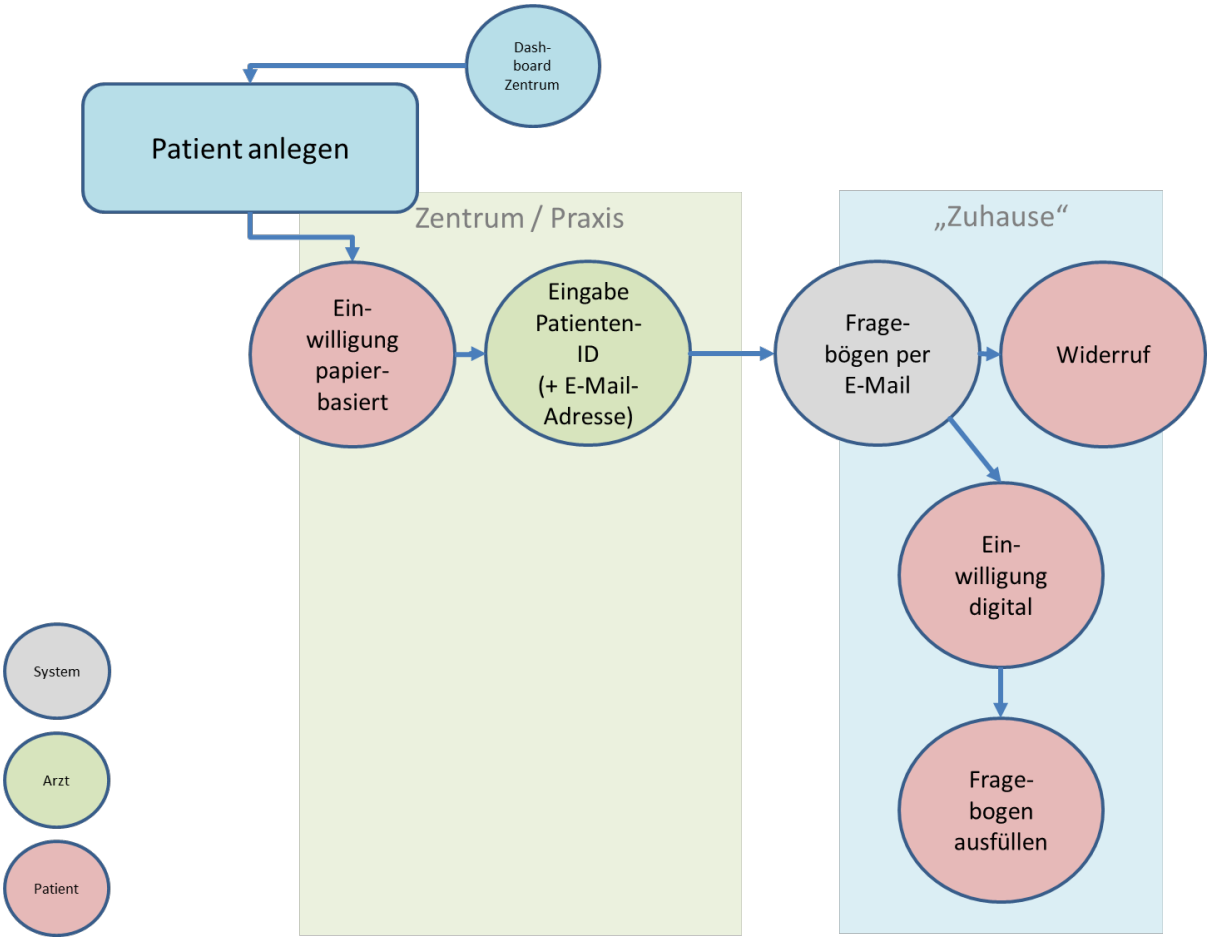
Speicherung von Patientendaten

Bei der Eingabe von personenbezogenen Daten muss in jedem Fall eine aktive Bestätigung der Patienteneinwilligung vorgenommen werden. Dabei wird unterschieden zwischen der schriftlichen und der elektronischen Einverständniserklärung. Für jede der beiden Einwilligungserklärungen wurde im System ein eigener Prozess hinterlegt.

1. Schriftliche Einwilligungserklärung (siehe Grafik 1):

Bevor im System personenbezogene Daten eines Patienten eingetragen werden, muss dem Arzt eine schriftliche Einwilligungserklärung vorliegen. Bei der Anlage des Patienten im System durch den Arzt und der damit verbundenen Eingabe von personenbezogenen Daten (E-Mail-Adresse des Patienten, Patienten-ID) muss der Arzt zusätzlich das Kontrollkästchen „Einwilligung liegt vor“ aktivieren. Ohne diese Aktivierung des Kontrollkästchens verhindert das System die Speicherung der Patientendaten – der Patient kann in diesem Fall nicht im System angelegt werden.

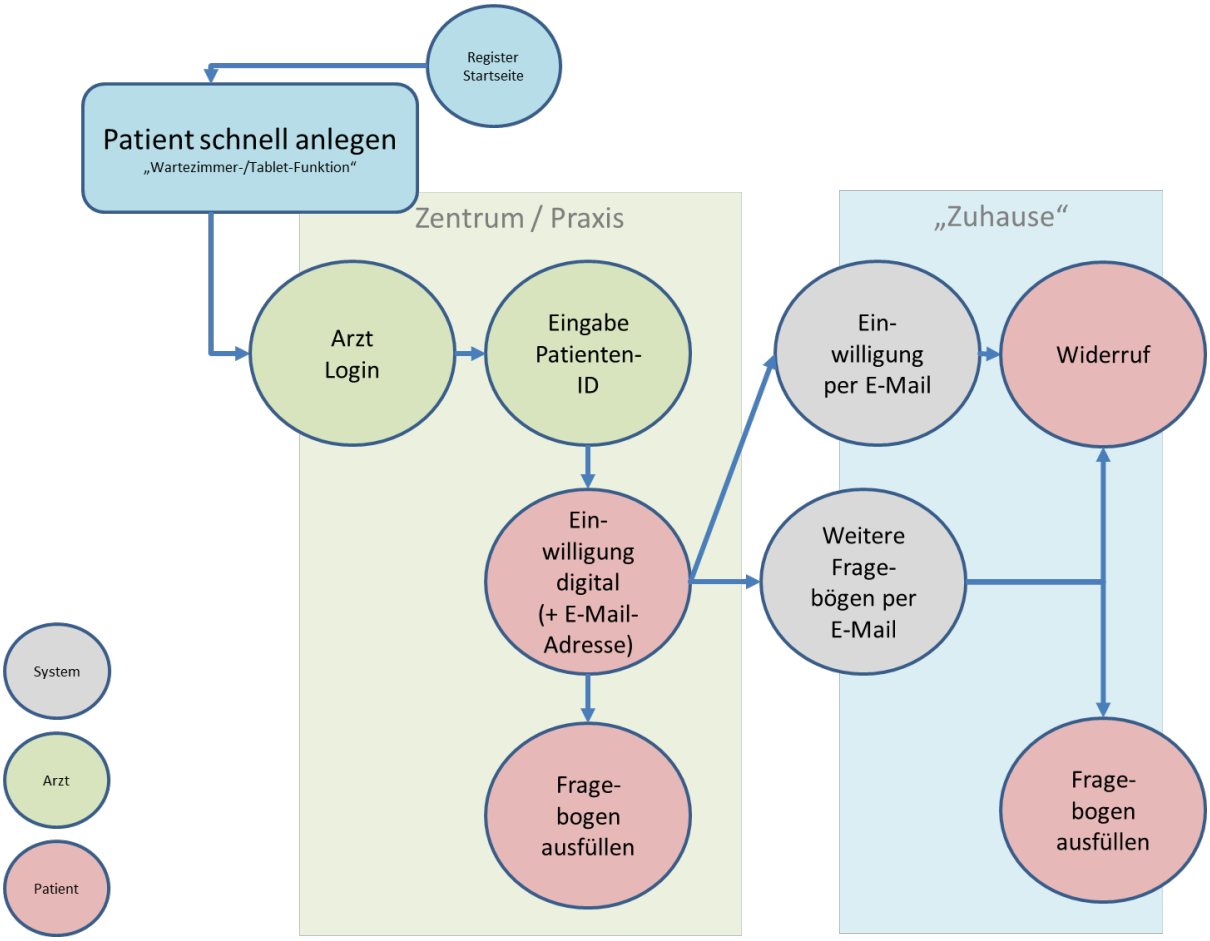
Grafik 1 Workflow Patientenanlage (schriftliche Einwilligungserklärung)



2. Elektronische Einwilligung (siehe Grafik 2):

Bevor im System personenbezogene Daten eines Patienten gespeichert werden, muss der Patient eine elektronische Einwilligungserklärung abgeben. Diese Einwilligungserklärung ist direkt im System hinterlegt und muss durch die Aktivierung eines Kontrollkästchen durch den Patienten akzeptiert werden. Ohne diese Aktivierung des Kontrollkästchens verhindert das System die Speicherung der Patientendaten – der Patient kann in diesem Fall nicht im System angelegt werden.

Grafik 2 Workflow Patientenanlage (elektronische Einwilligung)



Der Patient erhält, nachdem er im System angelegt wurde, regelmäßig E-Mails mit der Aufforderung, elektronische Fragebögen auszufüllen. Diese E-Mails enthalten personalisierte Hyperlinks, die es dem Patienten erlauben, direkt auf seine eigenen, aktuellen Fragebögen zuzugreifen, damit er diese ausfüllen kann. Bevor der Zugriff auf diese Fragebögen stattfindet, wird dem Patienten immer zuerst eine Website angezeigt, welche das bereits aktivierte Kontrollkästchen, das Datum der Einwilligung sowie einen Hyperlink zum elektronischen Aussprechen eines Widerrufs anzeigt. Das Kontrollkästchen wurde entweder zu einem früheren Zeitpunkt durch den Arzt aktiviert (in diesem Fall hat der Patient eine schriftliche Einwilligungserklärung abgegeben) oder das Kontrollkästchen wurde durch den Patienten aktiviert (in diesem Fall wurde vom Patienten selbst die Einverständniserklärung in elektronischer Form abgegeben).

Das angezeigte Datum der Einwilligung entspricht entweder dem Datum, an dem die elektronische Einwilligung durch den Patienten abgegeben wurde oder dem Datum, an dem der Arzt das Kontrollkäschen „Einwilligung liegt vor“ aktiviert wurde. Falls der Arzt das Kontrollkästchen „Einwilligung liegt vor“ aktiviert hat, kann zu diesem Zeitpunkt das eigentliche Datum der Unterzeichnung der schriftlichen Einwilligung auch in der Vergangenheit liegen.

Im Fall einer schriftlichen und elektronischen Einwilligungserklärung hat der Patient neben dem schriftlichen Widerruf auch die Möglichkeit, einen elektronischen Widerruf auszusprechen. Dazu muss er einen Hyperlink in einer der ihm zugesendeten E-Mails aufrufen und auf der dann aufgeschalteten Seite das Kontrollkäschen zur Bestätigung der Einwilligung deaktivieren. Alternativ kann er auf dieser Seite auch den Hyperlink „Einwilligung widerrufen“ anklicken.

Zertifizierung

Das Studienzentrum und das Klinikrechenzentrum des Universitätsklinikums Freiburg sind zertifiziert als „ECRIN Data Center“. Das Studienzentrum wurde vom European Clinical Research Infrastructure Network (ECRIN) als europäisches Datenzentrum zertifiziert und hat die sehr anspruchsvollen Anforderungen erfüllt. ECRIN ist ein von der Europäischen Kommission gegründetes und von den Mitgliedsländern finanziertes europäisches Infrastrukturnetzwerk für klinische Forschung (http://www.ecrin.org/, http://www.ecrin.org/activities/data-centre-certification/)

Dauer der Datenspeicherung

Personenbezogene Daten müssen gelöscht werden, wenn die Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Die Daten (Registerdaten, identifizierende Daten und Pseudonyme) werden auf unbefristete Zeit gespeichert, solange die Daten für die Erreichung der Forschungsziele der DART gGmbH wertvoll erscheinen. Die DART gGmbH entscheidet in regelmäßigen Abständen (ca. alle zwei Jahre), ob die erhobenen Registerdaten weiterhin pseudonymisiert vorliegen müssen oder ob die Daten anonymisiert werden können, wobei die DART gGmbH bestrebt ist, die Daten so früh wie möglich zu anonymisieren. Widerruft ein Teilnehmer seine Einwilligung in die Nutzung seiner Daten, werden die Registerdaten in der Datenbank zwar nicht gelöscht aber anonymisiert (Löschung von Pseudonymen und identifizierenden Daten). Nicht anonymisiert werden die Registerdaten allerdings aus bereits erstellten Auswertedatensätzen. Auswertedatensätze werden jedoch nach der Erstellung nach Möglichkeit anonymisiert.

Übergreifende technische und organisatorische Maßnahmen

Das Studienzentrum des Universitätsklinikums Freiburg hat einen Bereichsdatenschutzbeauftragten nach Vorgabe des Datenschutzhandbuchs des Universitätsklinikums Freiburg bestimmt. Das Studienzentrum arbeitet nach folgenden datenschutzrelevanten Dokumenten:

- Datenschutzhandbuch des Universitätsklinikums Freiburg
- SOP GE07 Data Protection and Security
- SOP IT01 System Set Up and Maintenance
- SOP IT02 Data Backup
- SOP IT03 IT Security
- SOP IT04 Workstation Systems
- SOP IT05 Disaster Recovery
- SOP IT06 Systemvalidierungsmasterplan
- SOP IT07 Änderungskontrolle
- SOP IT08 Risikoanalyse

Die Dokumente, Standard Operating Procedures (SOP) des Studienzentrums unterliegen einem fortlaufenden Änderungsmanagement und werden mindestens alle drei Jahre aktualisiert. Ein Datenschutzaudit des Studienzentrums durch den Datenschutzbeauftragten des Universitätsklinikums Freiburg im Jahr 2013 zeigte, dass die „Einhaltung der datenschutzrelevanten Anforderungen mit den am Studienzentrum getroffenen Maßnahmen und Verfahrensweisen angemessen realisiert“ sind.

Falls technisch bzw. organisatorisch notwendig kann dieses Datenschutzkonzept fortgeschrieben bzw. geändert werden. Ziel muss hierbei sein, ein gleichhohes oder höheres Datenschutzniveau als vorher zu erreichen.