

**Kerndokumentation und Qualitätssicherung
in der Schmerztherapie
KEDOQ-Schmerz**

**Datenmanagement für die
Deutsche Schmerzgesellschaft (DGSS) e.V.**

**Datenschutz- und Datensicherheits-
Konzept**

**Fassung 3
14. Oktober 2014**

1. Einleitung und Ziel

Die Deutsche Schmerzgesellschaft hat eine externe Qualitätssicherung initiiert, ein Institut zur Umsetzung beauftragt und einen KEDOQ Kommission einberufen.

Sie hat einen Datensatz beschlossen, mit dem folgende Ziele verfolgt werden:

- Patienten, die heute in schmerztherapeutischen Einrichtungen in Deutschland behandelt werden, mit ihren wesentlichen demographischen und klinischen Daten zu erfassen und zu beschreiben
- die Möglichkeit zu schaffen, dass diese Einrichtungen ihr Leistungsspektrum und ihre Ergebnisse bestimmen können
- einen vom jeweils genutzten Computerprogramm (Primärprogramm) unabhängigen Datensatz zu schaffen, der von allen Programmen als Austauschdatensatz verwendet werden kann
- die Grundlage für eine externe Qualitätssicherung (EQS) durch multizentrische Daten zur Prozess- und Ergebnisqualität zu schaffen.

Die Datensammlung soll online geschehen, die Primärprogramme sorgen für die Pseudonymisierung der Daten, die zum Patienten zusammengeführt werden, sowie die Datendefinition für das Hochladen.

2. Datenlieferung und Datenhaltung, verantwortliche Strukturen

Schmerztherapeutische Einrichtungen erklären der Deutschen Schmerzgesellschaft ihre Teilnahme an dem Qualitätssicherungsprojekt.

Bei der Deutschen Schmerzgesellschaft ist eine KEDOQ Kommission als ad-hoc-Kommission eingerichtet, die die Bedingungen der Teilnahme, die Vereinbarungen mit den am Datenaustausch teilnehmenden Einrichtungen und die Funktion der Datensammlung überwacht.

CLARA richtet die Datensammlung und -haltung sowie Verfügbarkeit der Daten ein und übernimmt die unmittelbare Gestaltung. Die Datenhoheit liegt bei der Deutschen Schmerzgesellschaft.

3. Daten

Die Datensammlung soll Daten zur Einrichtung (Adresse, Ansprechpartner, Struktur und Zuordnung zu einer Teilnehmergruppe) und zum Patienten enthalten (DSF, Diagnosen, Chronifizierungsstadium, eingeleitete Therapie und -verlauf nach 3-6 Monaten) s. Kerndatensatz. Die Daten sollen aus den vorhandenen Datenerfassungssystemen ausgelesen und in eine online-Datenbank eingepflegt werden.

Die Daten werden pseudonymisiert mit einer systembezogenen ID des Patienten vom liefernden Zentrum übernommen und werden unter dieser ID zusammen mit der Identität des Zentrums eindeutig zugeordnet. Die systembezogene ID eines Patienten soll sich aus dessen Daten eindeutig generieren (hash), um Übergaben von Patienten zwischen teilnehmenden Einrichtungen zu erfassen.

4. Datenschutz

Es ist eine Einverständniserklärung durch die Patienten erforderlich, die eine verschlüsselte Verwertung der Daten in KEDOQ-Schmerz erlaubt. Die Daten werden ausschließlich pseudonymisiert hochgeladen. Um Patientenwege zu erfassen, müssen die Patientenidentifizierungsdaten unabhängig vom Daten liefernden Programm eindeutig einem Patienten (Name, Vorname, Geburtsdatum, PLZ des Wohnortes als hash-Wert) zugeordnet werden. Es werden keine Klarnamen verwendet.

Die übrigen Daten sind Informationen, die während der Therapie in schmerztherapeutischen Einrichtungen üblicherweise erhoben werden (sollten). Diese Daten werden nach Einrichtungsgruppen zusammengefasst. Nur als solche stehen sie zur Auswertung zur Verfügung. Ggf. werden weitere Maßnahmen getroffen, um die Zuordnung von Daten zu einzelnen Einrichtungen zu verbünden.

5. online-Datenbank

Die online-Datenbank liegt auf einem geschützten Server.

Die online-Programmierung erfolgt über php plattformunabhängig.

Zur Datenübermittlung nutzen die Eingabestationen einen gängigen Browser (Internet-Explorer o.ä.) und ihren Zugang über eine gesicherte Internetverbindung (https-Protokoll).

Es werden jeweils die aktuellsten Datensätze eines Patienten gespeichert. Falls eine Datenlieferung doppelt erfolgt, werden die neuesten Datensätze gespeichert.

6. Datenzugriffsrechte

Die interessierten Einrichtungen melden sich bei CLARA an und erhalten nach vertraglicher Verpflichtung Benutzername und Kennwort für jeweils ein Jahr. Wiederholte Fehlversuche beim Login führen zur Sperrung. Nach einer Zeit an Inaktivität erfolgt ein automatischer Logout.

Bei einer Kündigung bleiben die bis zum Kündigungsdatum erhobenen und eingegebenen Daten in der Datenbank verfügbar.

Auf die Daten darf nur zugreifen, wer zu diesem Zeitpunkt Zugriffsrechte besitzt. Die Zugriffsrechte auf Patienten werden je teilnehmende Einrichtung verwaltet und beim Aufruf jeder Seite geprüft. Ein Hochladen von Daten wird nur von autorisierten Einrichtungen akzeptiert.

Für Auswertungen online (ad hoc-Tabellen) können die Daten aller Einrichtungen als Gruppen ausgewählt werden – ohne Information über die einzelne Einrichtung als Datenquelle.

Die eigenen Daten stehen der teilnehmenden Einrichtung in Tabellen, alle anderen im Prinzip allen Teilnehmern als Vergleichswerte zur Verfügung. Sie können für Fragestellungen ohne Bezug zur Datenquelle ausgewertet werden. Dazu muss die Fragestellung bei dem KEDOQ Ethikbeirat beantragt werden. Dieser entscheidet auf Basis der Teilnahme der Einrichtung, der Fragestellung und der Vereinbarkeit mit den Pflichten und Interessen der Deutsche Schmerzgesellschaft gegenüber ihren Mitgliedern.

Alle zentralen Datenauslesemaßnahmen werden bei CLARA zur Vorlage bei der KEDOQ Kommission protokolliert.

7. Datensicherheit

Der Zugang funktioniert mit Benutzernamen und Kennwort unter einer gesicherten verschlüsselten Verbindung (SSL), jedes Zentrum greift nur auf die eigenen Patientendaten bzw. deren Auswertung zu. Eine Verknüpfung zwischen den übermittelten Daten und der Daten liefernden Einrichtung ist ausschließlich dem zentralen Datenmanager bei CLARA vorbehalten, der sich einer entsprechenden Schweigepflicht unterwirft.

Die Daten liefernden Einrichtungen erhalten eine Übersicht der gelieferten, geprüften und akzeptierten Datensätze. Sie können fehlerhafte Datensätze nacharbeiten und bei der nächsten Datenlieferung hoch laden.

Für jede Einrichtung bzw. bei Einrichtungen mit mehreren Teilbereichen muss eine getrennte Anmeldung erfolgen. Dort sollte möglichst jeweils eine andere Person für die Datenlieferung zuständig sein. Plausibilitätskontrollen sollen Verwechslungen vermeiden.

8. Bericht

Die Deutsche Schmerzgesellschaft hat mit dem beauftragten Institut CLARA einen jährlichen Bericht erstmalig zum Oktober 2012 vereinbart. Teil dieses Berichts ist der Datenschutz.

9. Fehler und Risiken

Nicht übereinstimmende Anmeldung und Hochladeversuche

A. Verstoß gegen Gesetze und Verträge

Fehler und Risiken können in dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten bestehen.

Bekanntgabe von Zugangsdaten: Beispiel: Eine Einrichtung gibt ihre Zugangsdaten versehentlich oder absichtlich weiter.

Folge: Ein Unbefugter erhält Zugang zu der zentralen Datenbank. Er kann dort die einrichtungsbezogenen Strukturdaten einsehen (und ändern), er könnte die hochgeladenen Daten herunterladen, hat dort aber keine Personen-identifizierenden Angaben.

Vermeidung: Vertraglich wird die Weitergabe der Zugangsdaten verboten. Das Risiko ist durch die Verschlüsselung der Daten und die mangelnde Zuordnung zu bestimmten Personen minimiert.

Vergessen der Zugangsdaten: Beispiel und Folge: Tatsächliches Vergessen führt zu nicht möglichem Zugang zu den eigenen Daten.

Vermeidung bzw. Maßnahmen: erneute Freischaltung durch Vergabe eines neuen Kennworts beim Datenmanager von CLARA.

Falsche Anmeldung: Beispiel und Folge: 3maliges Eingeben einer falschen Zugangskennung führt zur Sperrung des Zugangs, der Zugang zu den eigenen Daten ist nicht mehr möglich.

Vermeidung bzw. Maßnahmen: erneute Freischaltung durch Vergabe eines neuen Kennworts beim Datenmanager von CLARA.

Verwechslung der Zugangsdaten z.B. in Teilbereichen einer Einrichtung: Dann können die Daten falsch zugeordnet werden. Folge: Falsche Einschätzung von Zielen (falsche Benchmarks).

Vermeidung: Plausibilitätskontrolle bei der Frage nach dem Setting, in dem die Patienten behandelt wurden (muss mit der Zuordnung zur Gruppe des Teilnehmers übereinstimmen). Eindeutige Zuordnung von verantwortlichen Personen zu Teilbereichen in teilnehmenden Einrichtungen.

Doppelung einer Patientenennung: 1. Unterschiedliche Patienten haben trotz unterschiedlichen Namens u.a. Daten dieselbe Hash-Kennung, eine solche sogenannte Kollision ist in extrem seltenen Fällen möglich.

Vermeidung: Das zeitgleiche Auftreten in dieser Weise ist in einer Einrichtung extrem unwahrscheinlich. Daher können die Daten nicht falsch zugeordnet werden. Daten könnten bei der zentrumsübergreifenden Auswertung falsche Rückschlüsse über die betreffenden Patienten im Sinne einer Mehrfachbehandlung an unterschiedlichen schmerztherapeutischen Einrichtungen ziehen lassen.

2. Patientenennung wird wegen unterschiedlicher Schreibweise unterschiedlich ausgegeben. Dem Patienten werden die ihn betreffenden Datensätze nicht korrekt zugeordnet, der Datensatz erscheint als unvollständig.

Vermeidung: Den Nutzern werden Vereinbarungen zur Schreibweise bei der hash-Kennung übermittelt.

Ausfall des Servers, Datenverlust: Beispiel: Der Server ist blockiert oder ganz ausgefallen.

Folge: Der Datenzugriff und die Datenintegrität können beeinträchtigt sein. Ggf. kommt es zu einem Datenverlust.

Vermeidung bzw. Abhilfemaßnahmen: Es werden regelhaft Sicherheitskopien und Serverspiegelungen erstellt, die auf den Server rückgeladen werden können.

Störung der Kommunikation bei der Dateneingabe: Beispiel: Abbruch der Dateneingabe

Folge: unvollständiges upload

Vermeidung bzw. Abhilfe: wenn das Hochladen abgebrochen wird, gibt es im Register keine Datensätze. Das Protokoll weist diesen Fehler aus und die Einrichtung kann jederzeit erneut hochladen.

B. Beeinträchtigung des informationellen Selbstbestimmungsrechts

Unzulässige Erhebung personenbezogener Daten ohne Einwilligung.

Vermeidung: Die Einrichtungen müssen in ihrer Primärsoftware vor der Dateneingabe bestätigen, dass eine Einwilligung vorliegt. Nur solche Daten werden hochgeladen. Personen-identifizierende Daten werden nicht übermittelt, verändert, weitergegeben oder zweckentfremdet.

C. Negative Innen- oder Außenwirkung

Die teilnehmenden Einrichtungen wollen eine individualisierte qualitätsbewertende Rückmeldung ohne oder nur mit gezielter freigegebener Veröffentlichung ihrer Einrichtung als Datenquelle. Schlussfolgerungen aus den Daten und Berichten obliegen ausschließlich der teilnehmenden Einrichtung.

Vermeidung: Daten werden nur auf Antrag an den Beirat herausgegeben und die Hinweise auf die Einrichtung als Datenquelle wird vor Weitergabe von Daten entfernt.