Kurzgutachten
gemäß
Datenschutzgütesiegelverordnung,
Schleswig-Holstein,
für das IT-Produkt
„IzB stationär Version 1.1.6.1.“

im Auftrag des Jugendhilfe e.V. , Hamburg

Inhalt

1 Gegenstand

Mit diesem Gutachten wird die datenschutzrechtliche Auditierung des IT-Produktes IzB stationär Version 1.1.6.1. (im Folgenden auch IzB) dokumentiert. Es ist von Jugendhilfe e.V., Hamburg, erstellt worden.

Mit dem IzB wird Einrichtungen ein Instrument zur Behandlungsplanung und -dokumentation geboten, das in verschiedenen Bereichen der Rehabilitation eingesetzt werden kann.

Gegenstand der Begutachtung ist das IzB als Software selbst

2 Zeitpunkt der Prüfung

Die Prüfung, Begutachtung und Dokumentation umfasst den Zeitraum vom 21.05.2012 bis 24.12.2015 und beinhaltet eine Analyse der zur Verfügung gestellten Begleitdokumente sowie Besichtigungen des Testsystems.

3 Antragsteller

Firma	Jugendhilfe e.V.
Ansprechpartner	Frau Christine Tügel
Adresse	Repsoldstraße 4 20297 Hamburg
Telefon **E-Mail**	040 8517350 tuegel@jugendhilfe.de

4 Sachverständige

Rechtlicher Gutachter

Ansprechpartner	Rechtsanwalt Dr. Philipp Kramer
Firma	Beratungsbüro Gliss & Kramer
Adresse	Witts Park 3 22587 Hamburg

Telefon	040 39906032
E-Mail	phillip.kramer@gliss-kramer.de

Technischer Gutachter

Ansprechpartner	Frau Dipl. Ing. Doris Wolf
Firma	schernus projekte + seminare GmbH & Co. KG
Adresse	Chrysanderstraße 90 21029 Hamburg
Telefon	040 7210 4627
E-Mail	doris.wolf@schernus.com

5 Kurzbezeichnung des IT-Produktes

Das IT-Produkt „IzB stationär Version 1.1.6.1“ des Jugendhilfe e.V. (im Folgenden auch **IzB**) dient der Behandlungsplanung und -dokumentation für verschiedene Bereiche der Rehabilitation. Das Produkt erfüllt die Anforderungen an einen datenschutzkonformen Umgang mit personenbezogenen und Gesundheitsdaten.

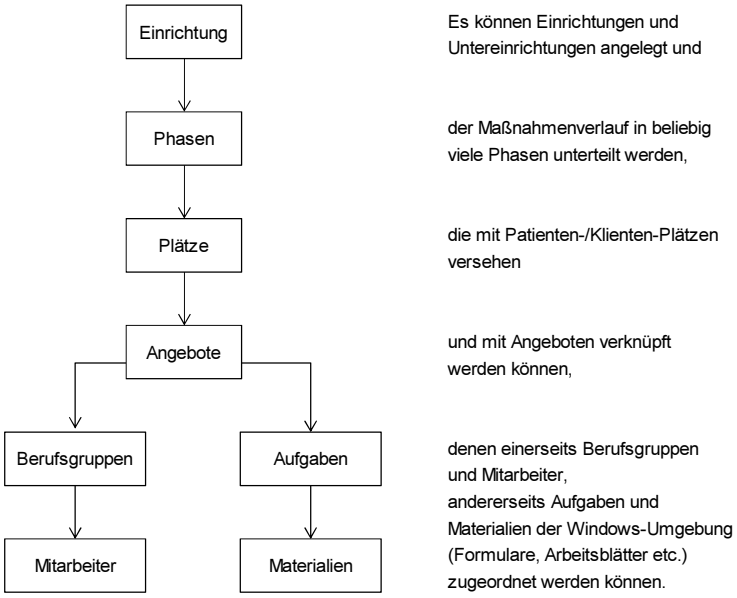
6 Detaillierte Beschreibung des IT-Produktes

Es wird das IT-Produkt IzB stationär in der Version 1.1.6.1 des Jugendhilfe e.V. begutachtet.

Das IzB ist ein Instrument zur Bedarfserfassung und Behandlungsplanung, das in verschiedenen Bereichen der Rehabilitation eingesetzt werden kann. Es wurde vom Jugendhilfe e.V., einem gemeinnützigen Hamburger Träger der Sucht- und Wohnungslosenhilfe, für seine Arbeit in der Suchthilfe entwickelt und liegt zur Begutachtung in der Version vor, die auf die inhaltlichen Vorgaben stationärer Rehabilitation zugeschnitten ist, wie sie in der Konzeption der Fachklinik Hamburg-Mitte (FKHM) des Vereins beschrieben sind.

Es gehört zur Konzeption des IzB, dass die Anpassung des Instruments an die jeweiligen Bedingungen seines Einsatzes weitestgehend systemimmanent geschehen kann, d.h. ohne Rückgriff auf den Programmierer. Hierfür werden auf der Administratoren-Ebene der Grundausstattung Listen und Werkzeuge vorgehalten, die es ermöglichen, alle Einzelbausteine und ihre Verknüpfungen so zu gestalten, dass auf der Nutzerebene ein Instrument zur

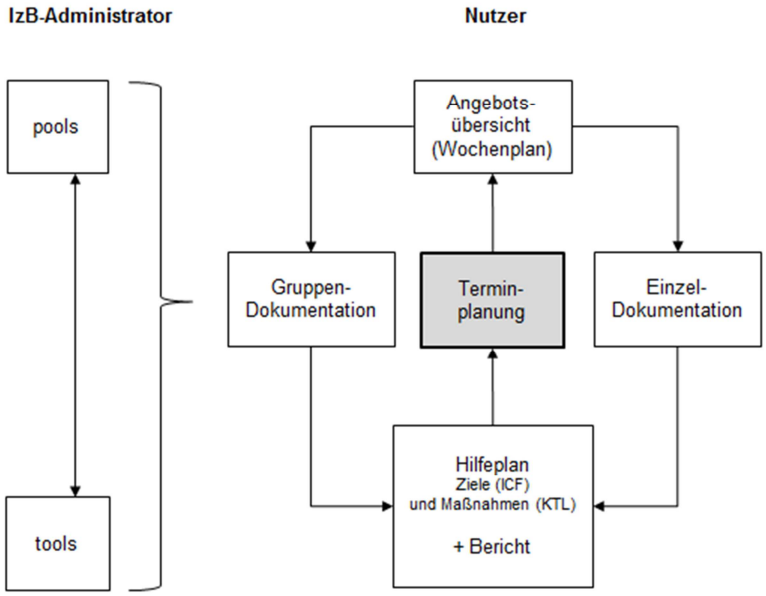
Verfügung steht, das den spezifischen Erfordernissen des jeweiligen Praxisfeldes Rechnung trägt.



Nach den vorgenommenen Einstellungen auf der Administratoren-Ebene entsteht so ein Instrument auf der Nutzerebene, das in den Grundmodulen

- Angebotsübersicht (rehabilitandenseitig und mitarbeiterseitig),
- Dokumentation (Einzel und Gruppen) sowie
- Behandlungssteuerung und Berichtswesen

den konzeptionellen Vorgaben einer Einrichtung entspricht.

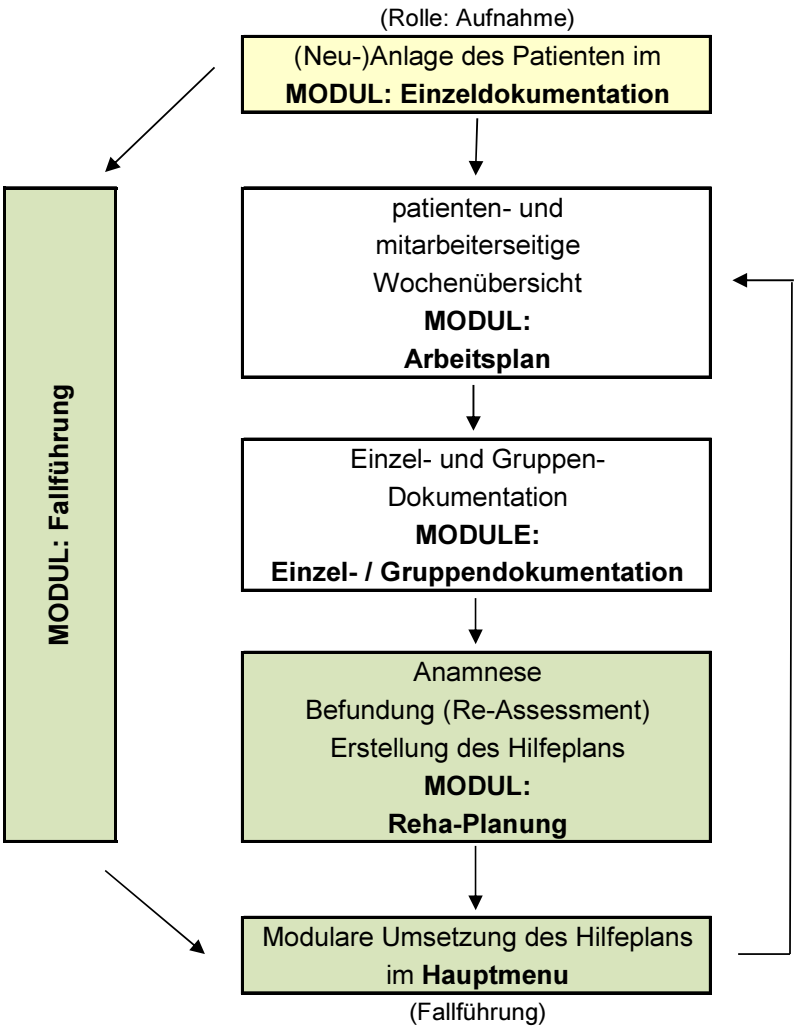


Die im Folgenden dargestellte IzB stationär Version 1.1.6.1 ist insofern die weitreichendste Fassung der IzB-Familie, als in der Ausgestaltung des Instruments hinsichtlich Anamnese, Diagnose, Hilfeplanung, Dokumentation und Berichterstattung ein komplexes, multifaktorielles Anforderungsprofil zu berücksichtigen war, das im Einzelnen folgende Parameter enthält:

- den Ärztlichen Entlassungsbericht der Deutschen Rentenversicherung (DRV),
- die Klassifikation therapeutischer Leistungen (KTL),
- die Internationale Klassifikation der Funktionsfähigkeit (ICF),
- den Peer Review der DRV,
- die Hamburger Basisdatendokumentation der Suchthilfe (BADO).

Ziel war es, mit dem IzB ein Werkzeug an die Hand zu geben, das den täglichen Anforderungen an Dokumentation, multidisziplinären Austausch und rasche Orientierung über die anstehenden Aufgaben und Arbeitsaufträge ebenso genügt wie der langfristigen Planung und Steuerung der individuellen Therapieprozesse – einschließlich des bei Therapieende zu erstellenden ärztlichen Entlassungsberichts.

Hierzu sind im Hintergrund (Administratoren-Ebene der Grundausstattung) die vier Behandlungsphasen angelegt (Aufnahme, Entwöhnung I, Entwöhnung II, Adaption), in die sich die gesamte Maßnahme maximal gliedert. Jeder dieser Phasen sind Behandlungsangebote zugeordnet, die im Rahmen der Konzeption vereinbart und gemäß den Richtlinien der Klassifikation therapeutischer Leistungen (KTL) gestaltet sind. Dabei sind Standardangebote, die für alle Rehabilitanden vorgehalten werden, unterschieden von Indikationsangeboten, die sich nach der individuellen Problemlage richten (nur in der ersten, sehr kurzen zweiwöchigen Aufnahmephase werden alle Angebote standardmäßig für alle Rehabilitanden vorgehalten). Beide Leistungsbereiche enthalten sowohl Einzel- wie Gruppenangebote.



Nach der Neuanlage des Rehabilitanden im IzB (Rolle: Aufnahme) sind für diesen und alle am Fall beteiligten Mitarbeiter alle Termine der ersten Aufnahmephase gesetzt und können in der Wochenübersicht des Arbeitsplans eingesehen werden. Sie dienen der multidisziplinären Befundung und werden in Form von Einzel- oder Gruppenangeboten durchgeführt und in den entsprechenden Modulen dokumentiert.

Den Arbeitsplan kann jeder Mitarbeiter, der eine Zugriffsberechtigung für das IzB stationär hat, einsehen. Dies ist für die Terminplanung (interner und externer Zusatztermine der Rehabilitanden) notwendig. Innerhalb des Arbeitsplans kann der Mitarbeiter nur innerhalb seiner Rollenberechtigung auf Einzel- und Gruppendokumentationen zugreifen. D. h . bspw. kann der Physiotherapeut nur auf die ihm zugewiesenen Aufgaben zugreifen.

Die Ergebnisse dieser an standardisierten Aufgaben orientierten Befundung der einzelnen Berufsgruppen sind über Hintergrundvernetzungen verknüpft mit der Ordnungsstruktur des Moduls: Reha-Planung, wo sie eingesehen und für die Erstellung des individuellen Hilfe-

plans verwendet werden können. Dieser Hilfeplan (für die nächste Phase: Entwöhnung I) enthält neben den (voreingestellten) Standard-Angeboten der Therapiephase zusätzliche Indikationsangebote, die über das Modul: Terminplanung (vom jeweils Fallführenden) in den individuellen Wochenplan des Rehabilitanden integriert werden.

Am Ende der (je aktuellen) Therapiephase entscheidet ein Re-Assessment über eine mögliche Hilfeplan-Korrektur und entsprechende Neuausgestaltung des Wochenplans.

Die Schleife: Re-Assessment – Hilfeplan-Korrektur – neuer Wochenplan wiederholt sich entsprechend der Anzahl der Therapiephasen. Dabei stehen die standardisierten Instrumente der Hamburger Basisdatendokumentation der Suchthilfe (BADO) für Anamnese / Assessment und die International Classification of Functioning, Disability and Health (ICF) für die Festlegung der individuellen Therapieziele zur Verfügung. Bei Beendigung der Therapie wird aus dem Modul Rehaplanung heraus der Entlassungsbericht generiert, einschließlich der vom Kostenträger geforderten Übersicht über die für den Rehabilitanden erbrachten therapeutischen Leistungen gemäß der Klassifikation therapeutischer Leistungen in der medizinischen Rehabilitation (KTL).

Flankiert wird diese Modulkette durch die Überblicksmodule Fallführung und Abwesenheiten. Im Fallführungsmodul werden die wichtigsten Etappen des Therapieprozesses (Fallbesprechungen, Anträge, Assessments etc.) von dem Fallführenden verwaltet, um jederzeit einen schnellen Überblick zu haben. Das Modul Abwesenheiten kann von allen Mitarbeitern eingesehen werden; es liefert ihnen Informationen darüber, wer sich zu einem gegebenen Zeitraum in der Einrichtung aufhält und wer (und aus welchem Grund) nicht. Es handelt sich in diesem Modul ausschließlich um die Abwesenheit von Rehabilitanden.

Der Fallführende ist der im Aufnahmedialog zugewiesene Bezugstherapeut und nur dieser kann auf das Modul Fallführung zugreifen. D. h. wenn die Bezugstherapeutin A den Rehabilitanden Meier zugewiesen bekommen hat, kann nur sie auf diesen zugreifen.

<u>Speichern von personenbezogenen Daten</u>

In der FKHM liegen die Rehabilitanden-Unterlagen in folgender Form vor:
a) Therapeutische Handakte (Papierform)
b) Verwaltungsakte (Papierform)
c) Digitale Rehabilitanden-Akte im IzB
d) Digitale Arbeitsmaterialien

Alle Dokumente, die das IzB im Rahmen des Rehabilitationsprozesses vorhält, können nur in der Software selbst aufgerufen und gespeichert werden.

<u>Die Ordnerstruktur des IzB stationär</u>

Die Software IzB stationär befindet sich in einem versteckten Programmordner des Zentralservers. Auf diesen Ordner kann nur der Netzwerkadministrator zugreifen, die Nutzer haben nur Leserechte. Alle Formulare, Dokumente und Arbeitsblätter sind in einem

separaten Ordner für „Quelldateien“ abgelegt. In einem weiteren Ordner werden alle ausgefüllten Dokumente gespeichert („Zieldateien“) wie z. B. der aus der Software generierte Ärztliche Entlassungsbericht, Testbögen oder Bescheinigungen. Auf den Ordner „Quelldateien“ haben neben dem Netzwerkadministrator der IzB-Administrator und die Fachklinik-Leitungen Zugriff. Die in diesem Ordner abgelegten Dokumente sind ausschließlich „Blanko-Dokumente“.

Löschen/ Entsorgen der Rehabilitanden-Akte

Der Entsorgungs- bzw. Löschungszeitpunkt wird im IzB unter dem Menüpunkt „Rehabilitanden aus dem System löschen“ angezeigt. Die Löschungstermine sind nach Fälligkeit sortiert. Eine fällige Löschung wird durch eine der fachlichen Leitungen vorgenommen. Durch den Löschungsbefehl werden alle personenbezogenen Daten in der IzB Dokumentation, im verdeckten Ordner „Zieldateien_Archiv“ sowie im Logbuch gelöscht.

6.1. Beschreibung der erhobenen und verarbeiteten Daten

Die **verarbeiteten Daten und Datenkategorien** in der IzB stationär Version 1.1.6.1 ergeben sich aus verschiedenen Vorgaben, Regelwerken und Katalogen, die im Folgenden näher beschrieben werden.

- Ärztlicher Reha-Entlassungsbericht der Deutschen Rentenversicherung (DRV)
- Klassifikation therapeutischer Leistungen (KTL)
- Internationale Klassifikation der Funktionsfähigkeit, Behinderung und Gesundheit (ICF)
- Peer Review der Deutschen Rentenversicherung (DRV)
- Hamburger Basisdatendokumentation der Suchthilfe (BADO)

Ärztlicher Reha-Entlassungsbericht der Deutschen Rentenversicherung (DRV)

Im Einzelnen erfüllt der Reha-Entlassungsbericht –jeweils unter Berücksichtigung datenschutzrechtlicher Bestimmungen- verschiedene Aufgaben.

- Informationsweitergabe
- Funktion eines sozialmedizinischen Gutachtens
- Vernetzungsfunktion
- Funktion als Qualitätsindikator
- Baustein für Rehabilitationsplanungen

Klassifikation therapeutischer Leistungen (KTL)

Die Klassifikation therapeutischer Leistungen (KTL) in der medizinischen Rehabilitation ist seit 1997 ein bewährtes Instrument zur Dokumentation der therapeutischen Leistungen in den Reha-Entlassungsberichten. Sie leistet einen wesentlichen Beitrag zur Qualitätssicherung der medizinischen Rehabilitation der Rentenversicherung sowie zur Weiterentwicklung der rehabilitativen Versorgungspraxis in Form von Reha-Leitlinien, die

Handlungsempfehlungen zur Ausgestaltung von Therapien für definierte Patientengruppen geben.

Internationale Klassifikation der Funktionsfähigkeit ICF)

Funktionsfähigkeit, Behinderung und Gesundheit sind in der Internationalen Klassifikation der Funktionsfähigkeit, Behinderung und Gesundheit (International Classification of Functioning, Disability and Health - ICF) klassifiziert. Der wesentliche Nutzen der ICF besteht in der zu Grunde liegenden bio-psycho-sozialen Betrachtungsweise der Komponenten der "Funktionsfähigkeit", deren Beeinträchtigungen im Sinne von Krankheitsauswirkungen und in der Einführung von "Kontextfaktoren".

Die Begrifflichkeiten der ICF haben bereits Eingang in das SGB V "Gesetzliche Krankenversicherung" und das SGB IX "Rehabilitation und Teilhabe behinderter Menschen" gefunden. Auch die "Rehabilitations-Richtlinie" des Gemeinsamen Bundesausschusses ist bereits auf Grundlage der ICF konzipiert worden.

Peer Review der DRV

Das Peer-Review Verfahren ist **nicht** Gegenstand der Zertifizierung, weil es außerhalb des IzB nach den Vorgaben der Deutschen Rentenversicherung durchgeführt wird.

Mit dem Peer Review-Verfahren wird die Qualität des Reha-Prozesses erfasst. Dazu werden von erfahrenen Reha-Medizinern des jeweiligen Fachgebietes (Peers) zufällig ausgewählte ***anonymisierte ärztliche Entlassungsberichte*** sowie die Therapiepläne der Rehabilitanden begutachtet. Die Bewertung basiert auf einer indikationsspezifischen Checkliste qualitätsrelevanter Merkmale der Rehabilitation und einem Handbuch. Das IzB stationär Version 1.1.6.1 informiert die Nutzer bei der Dokumentation der Reha-Leistungen über diese Qualitätsanforderungen.

Das Peer Review-Verfahren wird in circa zweijährigen Intervallen durchgeführt. Aus jeder Reha-Einrichtung werden circa 20 Entlassungsberichte von einem Gutachter einer anderen Einrichtung bewertet.

Hamburger Basisdatendokumentation der Suchthilfe (BADO)

Im Rahmen der medizinischen Rehabilitation ist keine Weitergabe von BADO-Daten vorgesehen und die Möglichkeit dazu deaktiviert.

Mit den Berichten zur Basisdatendokumentation werden die Klienten- und Betreuungsmerkmale der Hamburger Suchthilfe ausgewertet und beschrieben. Mit einer Vielzahl von Fragestellungen wird die Situation zu Betreuungsbeginn festgehalten. Ergeben sich im Laufe der Betreuungen Veränderungen in diesem Bereich, so werden diese

(prozessbegleitend) dokumentiert. Nach Auswertung werden so Entwicklungen während der Betreuung messbar.

6.2. Schnittstellen

Ärztlicher Reha-Entlassungsbericht der Deutschen Rentenversicherung (DRV)

Der Ärztliche Reha-Entlassungsbericht der Deutschen Rentenversicherung (DRV) kann mit dem vorgegebenen Formular ausgedruckt werden.

Peer Review der DRV

Das Peer-Review Verfahren ist **nicht** Gegenstand der Zertifizierung, weil es außerhalb des IzB nach den Vorgaben der Deutschen Rentenversicherung durchgeführt wird.

Hamburger Basisdatendokumentation der Suchthilfe (BADO)

Im Rahmen der medizinischen Rehabilitation ist keine Weitergabe von BADO-Daten vorgesehen.

7. Tools, die zur Herstellung des IT-Produktes verwendet wurden

Name der Datenbank: izbdaten

Die Datenbank Das IzB verwendet die aktuelle MySQL Community Version 5.7.9.

Das in dieser Version benutzte Verschlüsselungsverfahren ist Advanced Encryption Standard-256 (AES-256). Dieses Verfahren wird in der MySQL-Dokumentation als schnell und sicher eingeschätzt. Das IzB verwendet für die Verschlüsselung der Daten somit eine Schlüssellänge von 256 Bit.

Passwörter werden nach dem SHA-2-Algorithmus gehasht. Der HASH-Algorithmus SHA-2 wird als sicher betrachtet und allgemein zur Benutzung empfohlen.

8. Zweck und Einsatzbereich

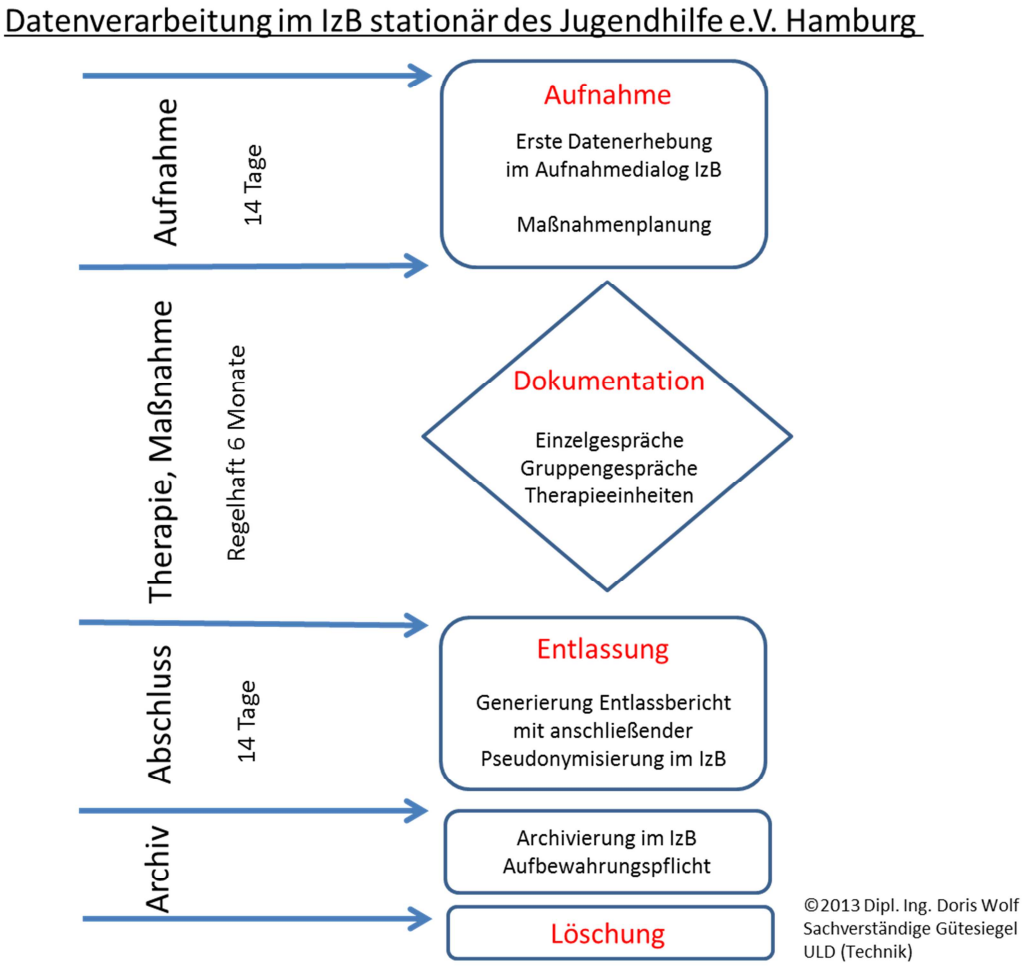
Der Zweck des IT-Produktes „IzB stationär Version 1.1.6.1“ des Jugendhilfe e.V. ist es, den Kunden ein Instrument zur Behandlungsplanung und -dokumentation, das in verschiedenen Bereichen der Rehabilitation eingesetzt werden kann, anzubieten. Mit dem IT-Produkt wird ihnen ein Werkzeug an die Hand gegeben, das den täglichen Anforderungen an Dokumentation, multidisziplinären Austausch und rasche Orientierung über die an-stehenden Aufgaben und Arbeitsaufträge ebenso genügt wie der langfristigen Planung und Steuerung der individuellen Therapieprozesse – einschließlich des bei Therapieende zu erstellenden Entlassungsberichts.

Mit dem IT-Produkt wird eine Grundausstattung zur Planung von Maßnahmen zur Bedarfserfassung und Behandlung geliefert. Die Begleitdokumente sind eine Sammlung relevanter Unterlagen als Vorschlag, die für unterschiedliche Implementierungen des IT-Produktes der einsetzenden Stelle und dessen Datenschutzbeauftragten Hilfestellung geben. Sie sind an einem Beispielfall orientiert, damit der Anwender ein besseres Verständnis der Umsetzung in seiner Einrichtung erlangt. Die Begutachtung des IT-Produktes beschränkt sich auf das IT-Produkt. Ein elektronischer Datenexport und eine elektronische Datenübermittlung werden für eine spätere Version vorgesehen.

Das IT-Produkt ist sowohl im nicht-öffentlichen als auch im öffentlichen Bereich einsetzbar.

9. Modellierung des Datenflusses

Im der folgenden Grafik wird der Datenfluss gezeigt.



10. Version des Anforderungskataloges, die der Prüfung zugrunde gelegt wurde

Prüfschemas für die Produktzertifizierung, Version 2.0 vom 17.06.2015, des ULD.

11. Beschreibung wie das Produkt den Datenschutz fördert

Mit dem geprüften IT-Produkt sind verantwortliche Stellen in der Lage, den Datenschutz Forderungen nachzukommen.

Die Software ist mit ihren Begleitdokumenten darauf ausgerichtet, nur so viele Rehabilitanden- und Beschäftigtendaten wie erforderlich zu erheben und zu verwenden.

Der Datenschutzbeauftragte der verantwortlichen Stelle wird durch dieses Produkt und den mitgelieferten Dokumentationen unterstützt und in die Lage versetzt, eine Vorabkontrolle durch Testdatenfälle durchzuführen. Eine Verfahrensdokumentation kann durch die mitgelieferten Dokumentationen leicht erstellt werden. Sowohl in der Dokumentation als auch in den internen Prozessbeschreibungen finden sich ausreichend Hinweise zum Datenschutz.

Das mitgelieferte Rollenkonzept und die voreingestellten Rollen im IzB stationär ermöglichen eine transparente und datensparsame Nutzung.

Besonders erwähnenswert im Sinne des Datenschutzes ist die Funktionsweise des Logbuchs. Einträge, Veränderungen und Manipulationen sind eindeutig erkennbar. Die originären und die veränderten Einträge sind eindeutig nachvollziehbar.

12. Prüfergebnisse nach Anforderungskatalog ULD

V	**vorbildlich**	**N**	**nicht**
A	**adäquat**	**E**	**entfällt**
U	**unzureichend**	**Ʊ**	**Verbesserung möglich**

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten	
1 Grundsätzliche technische Ausgestaltung von IT-Produkten	
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	
(Verfügbarkeit, Vertraulichkeit 3.2.1.1, 3.2.1.2, 3.2.1.3)	
Integrität	Ʊ
Intervenierbarkeit	A
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	
Datensparsamkeit	V
Nichtverkettbarkeit, Zweckbindung, Zwecktrennung	V

Verzicht auf personenbezogene Daten	V
Erforderliche Kombinationen	V
Kombination von Rehabilitandendaten	A
Kombination von Rehabilitandendaten	V
Kombination von Mitarbeiterdaten	V
Anonym oder Pseudonym	E
Löschen	V
Temporäre Datenbestände	V
Filterung auf Empfängerseite für „zu viel“ übermittelte Daten	A
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	
Transparenz für Anwender	V
Transparenz der DV für Betroffene	V
Erforderliche Vorkenntnisse	A
Leichter Zugriff auf Produktbeschreibung und andere Unterlagen	V
Aktualität der Unterlagen	A
Konzept der Datenverarbeitung	V
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	
Intervenierbarkeit	V
Sicherstellung der Erreichbarkeit	V
1.5 Anpassung des IT-Produkts	
Anpassung des IT-Produkts	Ʊ
1.6 Privacy by Default	
Privacy by Default	A
Komplex 2: Zulässigkeit der Datenverarbeitung	
2.1 Ermächtigungsgrundlage für die Verarbeitung von Daten (für jede Phase der Datenverarbeitung gesondert zu betrachten)	
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	
Abgeschlossener Katalog von Daten, die verarbeitet werden	A
Beschränkung der Erhebung und Speicherung von Daten	A
Beschränkung der erhobenen Daten auf das Erforderliche	A
Verarbeitung besonders sensibler Daten	A
Anonymisierungs- bzw. Pseudonymisierungsgebote	E
2.1.2 Einwilligung des Betroffenen	
Herbeiführung der Wirksamkeit der Einwilligung	Ʊ
Mustereinwilligungserklärung oder Hinweise zur Gestaltung der Einwilligungserklärung	V
Für die Einwilligung hat der Hersteller der Software IzB eine Einwilligungserklärung als „Datenschutz-Einwilligungserklärung“ standardisiert.	V
Hinreichend bestimmte Einwilligungserklärung	V
Verständlichkeit der Einwilligungserklärung	V
Zeitlich beschränkte Gültigkeit der Einwilligungen	A
Formerfordernisse für die Einwilligung	V
Freiwilligkeit der Einwilligung	A

Unterstützung der einzuholenden Einwilligung durch die Software IzB	V
Einwilligungsmanagement IT-gestützt	A
2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung	
2.1.3.1 Vorschriften über die Datenerhebung	
Umsetzung bestehender gesetzliche Regelungen bei der Erhebung von Daten	A
Zulässigkeitsbegründende Rechtsgrundlage der Erhebung	A
Dokumentation über die Herkunft	A
Unterrichtung des Betroffenen, gestützt durch das IT-Produkt	V
Verdeckte Erhebung von Daten	A
2.1.3.2 Vorschriften über die Übermittlung	
Einhaltung gesetzlicher Regelungen der Übermittlung	V
Protokollierung der Übermittlungen	V
Hinweis auf die Zweckbindung	V
Richtigkeit der Empfängeradresse	A
Filter für ausgehende Informationen gegen versehentliche unbefugte Weitergabe oder Offenbarung	V
Maßnahmen zur Steigerung der Sensibilität der Verarbeiter gegenüber unerlaubten Übermittlungen	V
Anonymisierung/Pseudonymisierung bei Übermittlung an Dritte	A
2.1.3.3 Löschung nach Wegfall des Erfordernisses	
Löschungsfristen, Wiedervorlagefristen, Aufbewahrungsfristen, Archivierungspflichten	V
Anonymisierung/Pseudonymisierung	A
2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten	
2.2.1 Zweckbindung und Zweckänderung	
Zweckbindung und Zweckänderung	A
Sichergestellung der Zweckbestimmung	A
Dokumentation des Zwecks der Datenverarbeitung	A
Revisionssichere Protokollierung der Verarbeitung für das Erkennen von Zweckänderungen	V
Zweckbindung durch Vermeidung von Daten und deren Trennung	A
Kennzeichnung von Datensätzen mit entsprechenden Zwecken	E
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	
Erleichterung der Umsetzung des Trennungsgebotes	A
Technische Umsetzung des Trennungsgebots	A
Automatisierten Anonymisierung/Pseudonymisierung	A
Prüfung der Rechtmäßigkeit der Weitergabe von untrennbar verbundenen Daten	A
2.3 Datenverarbeitung im Auftrag	
2.3 Datenverarbeitung im Auftrag	A
2.4 Voraussetzungen besonderer technischer Verfahren	
2.4.1 Gemeinsame Verfahren / Abrufverfahren	
Gemeinsame Verfahren / Abrufverfahren	E
2.4.2 Trennung der Verantwortlichkeiten	
Trennung der Verantwortlichkeiten	E
2.4.3 Veröffentlichungen im Internet	

Veröffentlichungen im Internet	E
2.4.4 Weitere besondere technische Verfahren	
2.4.4 Weitere besondere technische Verfahren	E
2.5 Sonstige Anforderungen	
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	
Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	E
Gebot der Pseudonymisierung von Daten	A
Komplex 3: Technisch-organisatorische Maßnahmen	
3.1 Einzelne technisch-organisatorische Maßnahmen	
3.1.1 Physikalische Sicherung	
Maßnahmen, um Unbefugten den Zutritt zu Datenträgern zu verwehren	A
Maßnahmen, um Unbefugten den Zugang zu Datenträgern zu verwehren	A
Zugangskontrollmechanismen und Protokollierung	V
Dokumentation Zugangskontrollmechanismen	V
3.1.2 Authentisierung	
Authentisierung	V
3.1.3 Autorisierung	
Vergabe detaillierter Zugriffsrechte/ Rollenkonzept	V
Detaillierungsgrad der Berechtigungen ausreichend	A
Trennung von Systemadministrationsebene und Anwendungsebene	V
Zugriffsrechte Administration	V
Vergabe der Rechte, Dokumentation	V
Dokumentation der Berechtigungen innerhalb oder außerhalb	V
Sicherstellung der Aufbewahrungsfrist von Dokumenten	A
3.1.4 Protokollierung	
Auswertung von Protokolldaten	V
Umfang der Stichprobe	Ʊ
Datenschutzrechtliche Anforderungen für die Protokolldaten	A
Löschung und Speicherfristen der Protokolldaten	Ʊ
Maßnahmen überlaufender Protokolldaten	Ʊ
Dokumentation Technische und organisatorische Maßnahmen Protokolldaten	A
Exportieren von Protokoll- und Dokumentationsdaten	V
Weitere Datenschutzrechtliche Anforderungen an die Protokolldaten	A
Überprüfung der Funktion	Ʊ
3.1.5 Verschlüsselung und Signatur	
Anerkannte Verschlüsselung	A
Dokumentation	A
3.1.6 Pseudonymisieren	
Pseudonymisieren	E
3.1.7 Anonymisieren	
Anonymisieren	E
3.2 Allgemeine Pflichten	

3.2.1 Technisch-organisatorische Maßnahmen	
3.2.1.1 Verfügbarkeit	
Dokumentation für die einsetzende Stelle	A
3.2.1.2 Integrität	
Umgang mit Integritätsverletzung	V
Schutz gespeicherter Daten	V
Unterstützung zur Aktualität von Daten	A
Dokumentation für die einsetzende Stelle	V
3.2.1.3 Vertraulichkeit	
Firewall	A
Verschlüsselungsverfahren adäquat umgesetzt	V
Maßnahmen gegen absichtliche unbefugte Weitergabe	A
Mechanismen gegen Einsichtnahme oder Abstrahlung	V
Dokumentation für die einsetzende Stelle	V
3.2.1.4 Nicht-Verkettbarkeit	
Nicht-Verkettbarkeit	V
3.2.1.5 Transparenz	
Nachvollziehbare Dokumentation	V
Nachvollziehbare Dokumentation der Prozessbeschreibung	V
3.2.1.6 Intervenierbarkeit	
Umsetzung der Rechte Betroffener	A
Auskunft, Gegendarstellung, Berichtigung, Löschung	
Dokumentation für die einsetzende Stelle	A
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	
Protokollierung von Datenverarbeitungsvorgängen	V
Aufbewahrungszeit der LogBuch Dateien	V
3.2.1.8 Test und Freigabe	
Unterstützung Test und Freigabe durch Testdatenfälle	A
3.2.2 Erleichterung der Vorabkontrolle	
Erleichterung der Vorabkontrolle	A
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	
Erleichterung bei der Erstellung des Verfahrensverzeichnisses	A
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	
Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	V
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten	
Unterstützung des behördlichen Datenschutzbeauftragten bei der Wahrnehmung seiner Pflichten	V
3.3 Spezifische Pflichten	
Verschlüsselung	A
Anonymisierung oder Pseudonymisierung	E
Mobile Datenverarbeitungssysteme	E
Video-Überwachung und –Aufzeichnung	E
Automatisierte Einzelentscheidungen	E

Veröffentlichungen im Internet	E
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	
Anleitungen zur Erstellung der geforderten Unterlagen nach DSVO	V
Unterstützung Test und Freigabe	V
Erstellung der Verfahrensdokumentation	V
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	
Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	E
Komplex 4: Rechte der Betroffenen	
4.1 Aufklärung und Benachrichtigung	
Aufklärung und Benachrichtigung	A
Aufklärung und Benachrichtigung von Betroffenen (Mitarbeiter)	V
Transparenz der Datenverarbeitung	A
Aufklärung und Benachrichtigung von Betroffenen (Rehabilitanden)	V
Transparenz der Datenverarbeitung	A
Verdeutlichung der Datenverarbeitungsschritte	V
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	
Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	V
4.3 Auskunft	
Auskunft	A
Unterstützung Auskunft von IT-Produkt	A
Automatisierte Auskunftsbearbeitung	E
Auffindbarkeit der Daten zur Auskunftserteilung	V
Vermeidung von Verknüpfungen mit Daten anderer Betroffenen	V
Protokollierung bei der Übermittlung personenbezogener Daten	E
Authentisierung des Auskunftsberechtigten	V
Umfang Auskunftsmöglichkeit	V
4.4 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	
4.4.1 Berichtigung	
Berichtigung	A
Unterstützung durch das IT Produkt bei Berichtigung	A
Weiterleitung von Berichtigungen/ Berichtigungen am Empfänger vorangegangener Datenübermittlungen	E
4.4.2 Vollständige Löschung	
4.4.3 Sperrung	
Sperrung	A
Umsetzung der Sperrung	A
Protokollierung der Sperrung und ggf. Aufhebung	A
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	
Weiterleitung von Widersprüchen an Empfänger vorangegangener Datenübermittlungen	E
4.4.5 Gegendarstellung	
Gegendarstellung	A

13. Verbesserung des IT-Produktes

Bei dem IT-Produkt IzB stationär Version 1.1.6.1. des Jugendhilfe e.V. handelt es sich um ein neues IT-Produkt, das bisher noch nicht zum Einsatz gekommen ist. In seiner jetzigen Version erfüllt es die Kriterien aus den Anforderungskatalogen des ULD. Eine Verbesserung des IT-Produktes ist in den folgenden, gelisteten Anforderungen für eine Rezertifizierung geplant.

	Stand	Verbesserungsmöglichkeit
1	Löschung Das Löschen nach Ablauf der dokumentierten Aufbewahrungsfrist wird als Auftrag an den Administrator gegeben. Der Vorgang des Löschens von Datenbeständen wird jedes Jahr auf Wiedervorlage gelegt. Der gesamte Datensatz zu einem Rehabilitanden ist händisch löschbar. Berücksichtigt werden dabei auch die Back Up-Medien.	Es könnte eine automatisierte Löschungsaufforderung oder eine automatisierte Löschung eingerichtet werden.
2	Löschung der Protokolldaten Die Protokolldaten werden genauso lange wie die eigentlichen Rehabilitandendaten aufbewahrt. Die Löschung erfolgt nach dem gleichen Ablauf, händisch.	Für die Protokolldaten könnte ebenfalls eine automatisierte Löschungsaufforderung oder eine automatisierte Löschung eingerichtet werden.
3	Anpassung des IT-Produktes Der Hersteller überwacht regelmäßig den Stand der Technik und die rechtlichen Rahmenbedingungen. Bei Veränderungen vor allem der rechtlichen Rahmenbedingungen werden die neuen Kataloge/ Vorschriften zugrunde gelegt.	Die Vorgehensweise und Realisierung der Anpassung des IT-Produktes an den Stand der Technik und an neue rechtliche Rahmenbedingungen ist noch nicht beschrieben.
4	Anleitungen zur Erstellung der geforderten Unterlagen nach DSVO (Wie wird die Erstellung des Sicherheitskonzeptes und der Risikoanalyse /nach § 6 DSVO) unterstützt?)	Eine Anleitung zur Erstellung der Unterlagen nach DSVO liegt noch nicht vor, obwohl Verfahrensdokumentation und Testfälle in der Datenbank den Datenschutzbeauftragten gut unterstützen.
5	Maßnahmen überlaufender Protokolldaten	Die Anzahl der Rehabilitanden und damit die Menge der auflaufenden Protokolldaten ist überschaubar. Zur Maßnahmeneinleitung bei überlaufenden Protokolldaten und Vorgehensweise könnte es eine spezielle Beschreibung geben.

6	Überprüfung Funktion Logbuch Integritätsprüfungen	Die Protokollierung wird regelmäßig auf Funktion überprüft. Diese Überprüfung und eine routinemäßige Integritätsprüfung zur Erkennung von veränderten Daten sollte im nächsten Update bei den Begleitdokumenten oder als technische Lösung angestrebt werden.

14. Prüfergebnisse OH-KIS

Die Orientierungshilfe konkretisiert in Teil 1 die Anforderungen, die sich aus den geltenden datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 der Orientierungshilfe werden Maßnahmen zu deren technischen Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Anforderungen der Orientierungshilfe Krankenhausinformationssysteme werden erfüllt.

Erklärung der Tabellenspalten

Anforderungen	OH-KIS
Referenz	Zuordnung OH-KIS Teil I +II
Einstufung	Soll, Muss
Erfüllt	ja/nein/entfällt

	Sicherheitskonzept			
Nr.	Anforderungen	Referenz	Ein-Stufung	Erfüllt
1.1.	Gibt es ein ausformuliertes Datenschutz- und IT-Sicherheitskonzept	II 2.18, 8.7	Soll	ja
1.2.	Können Patientendaten für Aus- und Fortbildungszwecke anonymisiert bereitgestellt werden?	I 30	Soll	ja
1.3.	Werden für besonders schutzwürdige Patientengruppen (Mitarbeiter, VIPs) Schutzmechanismen angeboten (Aliasname, Pfortensperre, enger Personenkreis mit Kenntnis; Aktenkennzeichnung, Pseudonymisierung)?	I 37 + 38, II 1.12, 1.13. 2.15	Muss	ja

1.4.	Ist der Status einer Patientenfallakte (Krankenhausaufenthalt beendet, Behandlungsfall abgeschlossen) erkennbar	II 1.9	Muss	ja
1.5.	Kann eine Auskunftssperre eingerichtet werden und ist diese ersichtlich?	II 1.11	Muss	ja
1.6.	Kann eine Kurzübersicht zurückliegender Behandlungsfälle erzeugt werden?	II 3.5	Muss	ja
1.7.	Können Widersprüche gegen Hinzuziehung der Vorbehandlungsdaten wirksam umgesetzt werden?	I 7, II. 1.10	Muss	ja
1.8.	Patientendaten für Auswertungszwecke (z. B. Controlling) müssen anonymisierbar sein.	I 29, II 1.16	Muss	entfällt
1.9.	Erfolgt ein Datenaustausch mit Externen nur mit Transportverschlüsselung?	II 2.16	Muss	entfällt
1.10.	Sind alle internen mobilen Speichermedien, die Patientendaten aufnehmen, verschlüsselt?	II 2.17	Muss	entfällt
1.11.	Sind sonstige Daten auf mobilen Speichermedien idR verschlüsselt?	II 2.17	Soll	entfällt
1.12.	Sind die Speicherorte für medizinische Daten zwingend vorgegeben?	II 3.12	Soll	ja
1.13.	Werden Fernwartungen nur im Einzelfall (!) mit Zustimmung des Krankenhauses durchgeführt?	II 8.2	Muss	entfällt
1.14.	Können Fernwartungen jederzeit durch das Krankenhaus abgebrochen werden?	II 8.3	Muss	entfällt
1.15.	Werden Fernwartungsarbeiten nur über verschlüsselte Verbindungen realisiert?	II 8.5	Muss	entfällt
1.16.	Werden die Rechte bei Fernwartungsarbeiten auf das erforderliche Maß beschränkt?	II 8.5	Muss	entfällt
1.17.	Können Fernwartungsarbeiten (Zeitpunkt, Dauer, Art des Zugriffs) protokolliert werden?	II 7.13, 7.14	Muss	entfällt
1.18.	Werden KIS und Subsysteme in ein Single-Sign-On-Verfahren einbezogen?	II 6.2	Soll	nein
1.19.	Werden Arbeitsplätze durch Autologout oder passwortgeschützte Bildschirmschoner zwingend geschützt?	II 6.3	Muss	ja
	Rollen- und Berechtigungskonzept			
Nr.	Anforderungen	Referenz	Ein-Stufung	Erfüllt
2.1.	Ist ein Rollen- und Berechtigungskonzept vorhanden?	II 4 + I 1-33	Muss	ja
2.2.	Bestehen Regeln zur Rechtevergabe?	II 1.8, 4.1, III	Muss	ja
2.3.	Sind die Regeln zur Rechtevergabe dokumentiert?	II 4.4 + 4.5	Muss	ja
2.4.	Können zeitlich beschränkte Berechtigungen gesetzt werden?	II 4.9	Muss	ja
2.5.	Differenziert das Berechtigungskonzept nach ärztlichen Beschäftigten, Verwaltungskräften, Ausbildungskräften, Externen und technischer Administration?	II 4. 2	Muss	ja
2.6.	Kann eine Übersicht der eingerichteten Berechtigungen für Personen und ihre Funktionen erstellt werden?	II 4.5 + 4.6	Muss	ja
2.7.	Ist ein aufgabenbezogener, individueller Rollenzuschnitt möglich?	II 4.12 + 4.13	Muss	ja
2.8.	Sind Gruppenlogins unmöglich	II. 4.14	Muss	ja
2.9.	Sind unberechtigte Nutzerzugriffe außerhalb des eigenen Aufgabenbereiches ausgeschlossen?	II. 3.2, 4.11	Muss	ja
2.10.	Können Zugriffsrechte auf weitere Funktionseinheiten übertragen oder erweitert werden?	II 4.7	Muss	ja
2.11.	Können Zugriffe zeitlich beschränkt werden?	II 4.9		ja

2.12.	Können situationsbedingte Aufhebungen oder Erweiterungen von Zugriffsrechten umgesetzt werden und ist dies im Berechtigungskonzept definiert? (Bereitschaft, Notfall etc.)	II 4.7 – 4.9, 4.15	Muss	ja
2.13.	Wird für Sonderzugriffe (z. B. Notfall) eine Begründung benötigt?	II 3.7 + 7.11	Muss	ja
2.14.	Wird bei der Erweiterung der Zugriffsrechte (Notfall, Qualitätssicherung) auf die Protokollierung hingewiesen?	II 4.9	Soll	ja
	Sperr- und Löschkonzept			
Nr.	Anforderungen	Referenz	Ein-Stufung	Erfüllt
3.1.	Können abgeschlossene Fallakten gesperrt werden?	I 21 + 24, II 2.10	Muss	ja
3.2.	Existiert ein schriftliches Konzept, wann Daten zu sperren und löschen sind?	II 2.9	Soll	ja
3.3.	Sind Subsysteme in ein Sperr- und Löschkonzept mit integriert?	II 2.4 + 2.7	Soll	ja
3.4.	Gibt es ein Zugriffskonzept für gesperrte Daten (Archivkonzept)?	I 24 + 25, II 2.9	Soll	ja
3.5.	Gibt es ein Verfahren Zugriffe auf gesperrte Daten gegen Offenbarung der Identität zu ermöglichen?	I 39	Soll	ja
3.6.	Bietet das KIS Daten irreversibel zu löschen (Löschflag reicht nicht!)?	II 2.11	Muss	ja
	Protokollierung und Reporting			
Nr.	Anforderungen	Referenz	Ein-Stufung	Erfüllt
4.1.	Können relevante Ereignisse zum Zwecke der Datenschutzkontrolle protokolliert werden?	II 7.1	Muss	ja
4.2.	Gibt es ein **schriftliches Protokollierungs- und Auswertungskonzept**, das Art, Umfang, Verfahrensweisen, getroffene Schutzmaßnahmen, Vorgehen bei Auswertungen und Aufbewahrungsdauer definiert?	II 7.2 – 7.4	Muss	ja
4.3.	Ist das Auswertungskonzept mit dem Datenschutzbeauftragten und der Mitarbeitervertretung abgestimmt?	II 7.2	Muss	IP
4.4.	Werden fachliche Nutzung einerseits und technisch-administrative Zugriffe andererseits protokolliert?	II 7. 5	Muss	ja
4.5.	Erfolgt eine Protokollierung der KIS-Aktivitäten?	II 7.6 + 7.5	Soll	ja
4.6.	Sind die Protokolldaten gegen Manipulation geschützt?	II 7. 8	Muss	ja
4.7.	Ist sichergestellt, dass Protokolle keine medizinischen Daten enthalten?	II 7. 9	Soll	nein
4.8.	Werden die folgenden Angaben beim Login/Log-out mit protokolliert: Zeitpunkt des Zugriffs; Kennung des jeweiligen Benutzers; Kennung der jeweiligen Arbeitsstation; aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung)?	I 40, II 7.10	Muss	ja
4.9.	Werden bei einer Suchfunktion mindestens die verwendeten Such- bzw. Abfragekriterien (z. B. Patientennummer, Fallnummer, Name, Geb.datum ,Wohnort , Diagnose etc.) protokolliert?	II 7.10	Muss	entfällt
4.10.	Werden bei Löschungen von Daten der Zeitpunkt, der Benutzer und die Datensätze protokolliert? Sind Personen zur Auswertung benannt?	II 7.15	Soll	ja

4.11.	Können die in 4.7 und 4.8 beschriebenen Protokolldaten vollständig eingesehen werden?	II.7.17	Muss	ja
4.12.	Bietet das Rollen- und Berechtigungskonzept einen separaten Zugriff auf Protokolldaten?	II 7.18	Muss	ja
4.13.	Werden Auffälligkeits- und Stichprobenauswertungen mi einer angemessenen Prüfdichte einbezogen?	II 7.20	Muss	IP
4.14.	Werden Protokolldaten mindestens zwölf Monate vorgehalten?	II 7.21	Muss	ja
4.15.	Werden Administratorentätigkeiten protokolliert?	I 35	Muss	ja
4.16.	Werden Protokolldaten aus administrativen Zugriffen deutlich länger als zwölf Monate archiviert?	II 7.22	Muss	ja
4.17.	Werden nicht abgerechnete Aufnahmen kontrolliert?	I 41	Muss	ja
4.18.	Werden Auswertungen durchgeführt, welche Benutzer über einen definierten Zeitraum sich nicht angemeldet haben?	II 4.17	Muss	entfällt

15. Bestätigung

Hiermit bestätigen wir, dass das oben genannte IT-Produkt mit seinen organisatorischen und technischen Vorgaben den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht und einen datenschutz- und datensicherheitskonformen Betrieb zulässt.

Wir versichern, dass wir an der Entwicklung des Produktes nicht beteiligt gewesen sind. Des Weiteren bestätigen wir, dass wir mit Ausnahme des Prüfauftrages für das Datenschutz-Gütesiegel über keine geschäftliche und private Beziehung zum Jugendhilfe e.V. verfügen (siehe auch Blatt 4 Antrag).

Dipl. Ing. Doris Wolf *Dr. Philipp Kramer*

Hamburg