Der Landesbeauftragte
für den Datenschutz Rheinland-Pfalz

Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Orientierungshilfe
„Krankenhausinformationssysteme“

Unterarbeitsgruppe Krankenhausinformationssysteme
Arbeitskreise Gesundheit und Soziales sowie
Technische und organisatorische Datenschutzfragen
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: März 2011

Orientierungshilfe Krankenhausinformationssysteme

Begleitpapier

Glossar

Teil I: Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus

Teil II: Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

Unterarbeitsgruppe Krankenhausinformationssysteme der
Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Begleitpapier zur Orientierungshilfe „Krankenhausinformationssysteme“

Die vorliegende Orientierungshilfe wurde von den Arbeitskreisen „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche erstellt. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern einbezogen.

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.

Für die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzaufsichts-behörden (Aufsichts- und Kontrollbehörden) wird das vorliegende Dokument den Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit bilden. Dabei sind die landesrechtlichen Bestimmungen zu berücksichtigen.

Ein Teil der am Markt angebotenen Lösungen bleibt nach den Erkenntnissen der Aufsichts- und Kontrollbehörden in technischer Hinsicht gegenwärtig noch hinter den hier dargelegten Anforderungen zurück. Mit Blick auf die Erfordernisse bei Softwareentwicklung und Qualitäts-sicherung gehen die Aufsichts- und Kontrollbehörden daher von der Notwendigkeit einer angemessenen Übergangsfrist für seitens der Hersteller erforderliche Anpassungen aus. Soweit sich die Anforderungen an die Krankenhäuser als Betreiber richten und entweder organisatorische Regelungen beim Einsatz von Krankenhausinformationssystemen betreffen oder mittels vorhandener Informationstechnik umgesetzt werden können, soll die Orientierungshilfe bereits jetzt herangezogen werden.

Stellen die Aufsichts- und Kontrollbehörden Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie unter Wahrung der Patientensicherheit mit den Krankenhäusern in einem geordneten Prozess die notwendigen Maßnahmen klären.

Die Diskussion mit Herstellern und Betreibern von Krankenhausinformationssystemen hat gezeigt, dass technische Anforderungen, Strukturen und Prozesse im Krankenhausbetrieb einem dynamischen Wandel unterworfen sind. Die Aufsichts- und Kontrollbehörden werden daher zur Fortschreibung der Orientierungshilfe weiterhin den Dialog suchen.

Glossar zur Orientierungshilfe Krankenhausinformationssysteme

Alias

Ein Alias ist ein fiktiver Name, unter dem Personen des öffentlichen Lebens oder Personen, die einem erhöhten Interesse am Datenzugriff ausgesetzt sind, mit dem Ziel aufgenommen werden, ihre Identität zu verbergen.

Anonymisierung

Anonymisierung bedeutet die Veränderung personenbezogener Daten derart, dass danach im Unterschied zur →*Pseudonymisierung* eine Zuordnung zu den Betroffenen nicht mehr oder nur mit unverhältnismäßigem Aufwand an Zeit Kosten und Arbeitskraft möglich ist. Ein bloßes Entfernen der direkt identifizierenden Angaben (z.B. Name, Anschrift, KV-Nummer) ist damit nicht ausreichend, wenn die verbleibenden (medizinischen) Daten eine Zuordnung noch ermöglichen.

Archiv (Altfälle)

Datenbestand mit Daten aus abgeschlossenen Behandlungsfällen. Das Archiv wird gebildet durch Überführung von Daten aus dem laufenden Bestand in ein Archivsystem bzw. die →*Trennung von Datenbeständen*. Archivdaten bleiben logisch Teil der →*Patientenakte*, für den Zugriff auf Archivdaten gelten besondere Berechtigungen. Diese Anforderung geht zurück auf einzelne landesgesetzliche Anforderungen. Der hier verwendete Archivbegriff meint nicht Archive im Sinne der Archivgesetze oder Archive, die aus Performancegründen gebildet werden und Daten aufnehmen, auf die über einen definierten Zeitraum nicht mehr zugegriffen wurde, die jedoch bei Bedarf direkt bereitgestellt werden können. Im letztgenannten Fall muss das Rollen- und Berechtigungskonzept greifen, welches auch für den laufenden Bestand gilt.

Behandlungsfall

In der Regel umfasst ein Behandlungsfall die Daten aller medizinisch zusammenhängenden Behandlungen eines Patienten innerhalb desselben Krankenhauses einschließlich der dortigen Weiter- oder Nachbehandlung. Für jeden Behandlungsfall wird eine →*Fallakte* angelegt.

Elektronische Patientendaten

Elektronische Patientendaten sind alle in einem →*Krankenhausinformationssystem (KIS)* erfassten und gespeicherten administrativen und klinischen Daten eines Patienten.

Fallakte

Alle Daten, die einem →*Behandlungsfall* zugeordnet sind. Alle Fallakten zusammen bilden die →*Patientenakte*.

Funktionsbezogene Organisationseinheit

Eine funktionsbezogene Organisationseinheit (OE) ist eine kleinste organisatorische Einheit innerhalb eines →*Krankenhauses*, in der Patienten von einer oder interdisziplinär von mehreren Fachrichtungen behandelt, gepflegt oder versorgt werden - z.B. eine Fachabteilung, eine Gruppe von Konsiliarärzten, eine Station, ein Labor, eine Abteilung für Medizincontrolling u.ä.. Abzugrenzen sind diese von größeren Versorgungsbereichen (z.B. Zentren). Patienten und Krankenhausmitarbeiter können mehreren funktionsbezogenen Organisationseinheiten zugeordnet sein.

Identifikationsdaten

Unter Identifikationsdaten fallen insbesondere folgende Daten: Vor- und Zuname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht, Titel, Anschrift, Krankenversichertennummer, Patienten-ID.

Krankenhaus

Ein Krankenhaus ist ein zusammengehörender Funktionskomplex im Sinne von § 107 SGB V. Welche Einrichtungen als zusammengehörig betrachtet werden, kann nach den jeweiligen Landeskrankenhausplänen, dem Auftreten unter einheitlichem Institutskennzeichen nach § 293 SGB V und der Existenz einer einheitlichen ärztlichen Leitung beurteilt werden. Die Orientierungshilfe richtet sich primär an Krankenhäuser im Sinne des § 107 Abs. 1 SGB V. Soweit die einzelnen Empfehlungen dem Sinn nach auf Vorsorge- und Rehabilitationseinrichtungen nach § 107 Abs. 2 SGB V anwendbar sind, können sie auch diesen als Orientierungshilfe dienen. Krankenhausketten oder -konzerne zählen nicht als ein zusammengehörendes Krankenhaus. Unabhängig von der Einordnung als Krankenhaus bestimmt sich die Einordnung als datenschutzrechtlich verantwortliche Stelle nach den Vorgaben des BDSG, der Landesdatenschutzgesetze und der kirchlichen Rechtsvorschriften.

Krankenhausinformationssystem (KIS)

Unter dem Begriff „Krankenhausinformationssystem (KIS)“ wird die Gesamtheit aller in einem →*Krankenhaus* eingesetzten informationstechnischen Systeme zur Verwaltung und Dokumentation →*elektronischer Patientendaten* verstanden. Dabei handelt es sich in aller Regel um einen Verbund selbständiger Systeme meist unterschiedlicher Hersteller. Auf einzelne Fachbereiche beschränkte Verfahren wie z.B. Labor-, Radiologie- oder Diagnosesysteme gehören als Subsysteme ebenfalls zum Krankenhausinformationssystem.

Löschung

Löschung bedeutet das irreversible Unkenntlichmachen von Daten. Eine Markierung von Daten als „gelöscht“, mit der Folge, dass die Daten lediglich nicht mehr angezeigt werden, ist keine Löschung. Stehen einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen, besteht Grund zu der Annahme, dass durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich, tritt an die Stelle der Löschung eine →*Sperrung.*

Mandantenfähigkeit

Mandanten im Sinne dieses Papiers sind →*Krankenhäuser* bzw. rechtlich eigenständige Stellen wie Medizinische Versorgungszentren oder Belegärzte. Mandantenfähigkeit bedeutet in diesem Zusammenhang, dass Patientendaten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können, so dass jeder Mandant nur ihm zugeordnete Daten verarbeiten kann. Mandantenfähigkeit setzt des Weiteren voraus, dass die technischen Voraussetzungen für die Einhaltung der Anforderungen aus Tz. 30, 30a und 30b des Teils 1 der Orientierungshilfe gegeben sind.

Mitbehandlung

Mitbehandlung ist jede Form der krankenhausinternen ärztlichen Mitwirkung einschließlich des Konsils zur gemeinsamen Behandlung eines bestimmten Patienten in einem zuvor durch den behandelnden Arzt begründeten Behandlungskontext.

Patientenakte

Die Gesamtheit aller zu einem Patienten bei einem Krankenhaus gespeicherten Verwaltungs- und Behandlungsdaten.

Patientenaktensystem (PAS)

Das PAS ist das Subsystem des KIS, das Krankengeschichten und Pflegedokumentationen einschließlich Anamnese- und Befunddaten, Diagnosen und Arztbriefen etc. aufnimmt. Es stellt Funktionen zur Patientenverwaltung, Behandlungsplanung und -dokumentation sowie ggf. zur Abrechnung zur Verfügung. Es ist abzugrenzen von anderen Subsystemen des KIS wie Labor- oder Radiologieinformationssystemen oder einzelnen mit dem KIS verbundenen Diagnosegeräten.

Pseudonym

Ein Pseudonym ist das Ergebnis des Ersetzens der Identitätsdaten eines Patienten zu dem Zweck, die Bestimmung des Betroffenen durch Unberechtigte auszuschließen oder wesentlich zu erschweren. Zur Abgrenzung vgl. → Alias und → temporäres Patientenkennzeichen.

Pseudonymisierung

Pseudonymisieren ist das Ersetzen von →Identitätsdaten durch ein Kennzeichen (Pseudonym) zu dem Zweck, die Bestimmung des Betroffenen durch Unberechtigte auszuschließen oder wesentlich zu erschweren. Da das Pseudonym einer bestimmten Person zugeordnet wurde, kann diese Person – anders als bei der Verwendung anonymisierter Daten – über die Zuordnungsregel identifiziert werden. Mittels der Vergabe von Pseudonymen sollen personenbezogene Daten derart verändert werden, dass sie *ohne Kenntnis der jeweiligen Zuordnungsregel* nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, für konkret definierte Ausnahmefälle aber *mittels der Zuordnungsregel* besonders hierzu Berechtigten die Identifizierung der Person möglich ist. Eine korrekte Pseudonymisierung erfordert daher, dass es nicht oder nur mit unverhältnismäßigem Aufwand möglich sein darf,

den Betroffenen unter Rückgriff auf das Pseudonym und der weiteren zu diesem Pseudonym gespeicherten Daten zu re-identifizieren.

Dies muss geprüft und sichergestellt werden, wenn ein Empfänger von Patientendaten lediglich pseudonymisierte Patientendaten zur Kenntnis erhalten darf. Der Ersatz der Identitätsdaten durch ein Pseudonym ist dabei eine notwendige, aber oft nicht hinreichende Maßnahme.

Die Verwendung von → Aliasen und → temporären Patientenkennzeichen stellt eine technisch-organisatorische Maßnahme zum Schutz der Betroffenen dar, die von einer Pseudonymisierung abzugrenzen ist.

Rolle

Zuständigkeit eines Mitarbeiters innerhalb einer Organisation (*strukturelle Rolle*) bzw. Aufgabe, die zugewiesen oder auf Grund bestehender Fachkompetenz übernommen wurde (*funktionelle Rolle*). Strukturelle Rollen sind über längere Zeiträume statisch. Funktionelle Rollen wechseln in Abhängigkeit vom Bezug der Tätigkeit zu der Behandlung der konkreten Patienten, auf deren Daten zugegriffen werden soll. Technisch wird unter einer Rolle oft ein Bündel von Zugriffsberechtigungen verstanden, die aus den Erfordernissen einer strukturellen Rolle abgeleitet sind. Funktionelle Rollen hingegen werden durch → *Verarbeitungskontexte* abgebildet, durch welche die Ausübung bestehender Zugriffsrechte auf das für die jeweilige Aufgabe erforderliche Maß beschränkt wird.

Sperrung

Sperren ist das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken. Auf gesperrte Daten kann nur noch unter eng begrenzten Voraussetzungen zugegriffen werden. Beispiele entsprechender Sperren sind die nach landes- oder bundesgesetzlichen Regelungen erforderliche Beschränkung des Zugriffs nach Abschluss der Behandlung auf den alleinigen Zugriff der jeweiligen Fachabteilung.

Temporäres Patientenkennzeichen

Ein temporäres Patientenkennzeichen ist das Ergebnis des Ersetzens der Identitätsdaten eines Patienten zu dem Zweck, diese bei der Verarbeitung zu verbergen.

Trennung von Datenbeständen

Trennung von Datenbeständen bedeutet die Organisation der Datenhaltung in einer Weise, die es erlaubt, Datenbestände funktional getrennt voneinander zu verarbeiten. Die Trennung kann durch physische Abgrenzung (z.B. Speicherung in verschiedenen Datenbankinstanzen oder auf unterschiedlichen Systemen) oder innerhalb eines Bestandes durch logische Differenzierung durch Speicherung in separaten Datenbanktabellen und Verzeichnisstrukturen oder anhand entsprechender Kennzeichnungen sichergestellt werden.

Verarbeitungskontext

Als Verarbeitungskontext wird der sachliche und technische Zusammenhang bezeichnet, in dem Nutzer des KIS in einer bestimmten funktionellen Rolle Patientendaten verarbeiten. Verarbeitungskontexte leiten sich aus den Verarbeitungszwecken ab und verfeinern diese. Beispiele für Verarbeitungskontexte sind Behandlung eines der eigenen OE zugeordneten

Patienten, Pflege eines Stationspatienten, OP-Assistenz, DRG-Controlling usw. Ein Verarbeitungskontext wird im PAS über kontextbezogene Benutzerrollen, Daten- und Funktionszugriffe und Bildschirmmasken abgebildet. So unterscheidet sich z.B. eine Suchfunktion bzw. die Präsentation von deren Ergebnissen im Verarbeitungskontext „Patientenaufnahme“ von der des Verarbeitungskontextes „Behandlung“.

Vertretung

Eine Vertretung ist die zeitlich befristete Übernahme der Aufgabe eines Mitarbeiters durch einen anderen gemäß eines Dienstplans oder einer sonstigen Regel, die von der jeweilig dafür zuständigen Leitung im Voraus festgelegt wurde.

Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus

---

Unterarbeitsgruppe Krankenhausinformationssysteme der
Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Aufnahme

Administrative Aufnahme

1. Die Aufnahmekraft darf bei Eingabe der Identifikationsdaten des neuen Patienten (Suchfunktion) vom System erfahren, ob der Patient schon einmal in demselben Krankenhaus behandelt wurde. Dies umfasst zunächst nur Identifikationsdaten (Name, Vorname, Patientennummer, etc.). Dabei kann zur klaren Identifizierung die Wild-Card-Funktion (abgekürzte Suche oder Ähnlichkeits-Suche) zugelassen werden (Ausschluss einer Doppelregistrierung derselben Person mit verschiedenen Schreibweisen). Durch nachträgliche Kontrollen muss sichergestellt werden, dass fingierte Aufnahmen von Patienten zum Zweck der Einsicht in Patientendaten aufgedeckt und sanktioniert werden.

2. Die Offenbarung einer vorbehandelnden funktionsbezogenen Organisationseinheit ist bei der administrativen Aufnahme nur dann zulässig, wenn in dem Krankenhaus noch nicht abgeschlossene Behandlungsfälle zu dem Patienten geführt werden. Eine Zugriffsmöglichkeit der administrativen Aufnahmekraft auf medizinische Daten mit Ausnahme der Einweisungsdiagnose ist mangels Erforderlichkeit nicht zulässig.

3. Die Aufnahmekraft darf auch – möglichst standardisierte – Warnhinweise im Datensatz des Patienten zur Kenntnis nehmen, die bereits vor der medizinischen Aufnahme administrative Maßnahmen erfordern. Dies gilt für frühere Betrugsversuche / Zahlungsunfähigkeit von Selbstzahlern und für Hinweise auf die Trägerschaft multiresistenter Keime, die umgehend besondere Schutzmaßnahmen erfordern.

4. Bei der Aufnahme kann der Patient der Hinzuziehung von Daten aus früheren abgeschlossenen Behandlungsfällen in demselben Krankenhaus ganz oder teilweise widersprechen. Hierauf und auf die mit einer derartigen Beschränkung verbundenen Risiken ist der Patient bereits bei der administrativen Aufnahme in allgemeiner Form (z.B. durch ein Merkblatt) hinzuweisen.

5. Die Anlage eines klinischen Basisdatensatzes ist auf Grundlage einer Einwilligung des Patienten möglich. Auf diesen darf bei neuer Vorstellung des Patienten zugegriffen werden.

6. Das Krankenhaus muss die Möglichkeit vorsehen, Auskünfte über den Patientenaufenthalt durch die Pforte, andere Auskunftsstellen und das Stationspersonal zu sperren. (Ob diese als Regel einzurichten ist und eine Aufhebung der Einwilligung bedarf, oder ob eine Widerspruchslösung genügt, hängt von den landesgesetzlichen Regelungen ab. Für psychiatrische Patienten ist generell die erste Verfahrensweise zu wählen.) Die Einrichtung einer Auskunftssperre muss zur Folge haben, dass bei der Patientensuche durch die Pforte oder eine andere Auskunftsstelle kein Treffer angezeigt wird.

Medizinische Aufnahme

6a. Die medizinische und die administrative Aufnahme können von der gleichen Person abgewickelt werden. Im Zuge der medizinischen Aufnahme ist im erforderlichen Umfang die Kenntnisnahme und Erhebung von medizinischen Daten zulässig.

7. Hat der Patient der Heranziehung von Vorbehandlungsdaten im Rahmen der administrativen Aufnahme widersprochen, ist ein Hinweis im System aufzunehmen, um dem behandelnden Arzt die Möglichkeit zu geben, den Patienten bei der medizinischen Aufnahme auf das potentiell bestehende Risiko einer Fehlbehandlung hinzuweisen und die Gelegenheit zur Rücknahme des Widerspruchs zu geben. Eventuell in begründeten Einzelfällen bestehende Möglichkeiten zur Einschränkung der Haftung des Krankenhauses oder zur Verweigerung der Behandlung ergeben sich aus dem allgemeinen und landesspezifischen Arzt- und Krankenhausrecht.

8. Ist der Patient bei der (Not-)Aufnahme nicht einsichts- oder artikulationsfähig, darf das Krankenhaus grundsätzlich von der mutmaßlichen Einwilligung in die Heranziehung von erforderlichen Vorbehandlungsdaten aus demselben Krankenhaus durch die Behandler ausgehen. Die Tatsache, dass dieser Fall eingetreten ist, muss sich aus dem KIS ergeben.

Behandlung

9. Jede an der Behandlung und Verwaltung eines Patienten direkt beteiligte Person darf auf die Identifikationsdaten des Patienten zugreifen.

10. Der Zugriff auf die medizinischen und Pflege-Daten ist nach seiner Erforderlichkeit für die persönliche Aufgabenerfüllung der Mitarbeiter auszudifferenzieren. Kriterien zur Differenzierung sind zumindest die Stellung eines Mitarbeiters im Krankenhaus und die ihm zugewiesenen fachlichen Aufgaben. Der Behandlungsort kann als Indiz für die Übernahme einer Aufgabe dienen. Beispiel sind die einem Bereitschaftsarzt zugewiesenen Stationen, die Anwesenheit eines Chirurgen im OP-Saal, in dem sich der Patient befindet, oder die Anwesenheit einer Pflegekraft auf einer Station, in der er dies tut.

Zugriffe durch Ärzte

Soweit im Folgenden auf Ärzte Bezug genommen wird, gelten die Regelungen auch für Psychotherapeuten.

11. Ein Patient ist zu jedem Zeitpunkt seiner Behandlung fachlich oder räumlich einem Arzt oder einer Gruppe von Ärzten zugeordnet. In der Regel darf diese Zuordnung alle Ärzte einer funktionsbezogenen Organisationseinheit einschließen, die sich bei der Behandlung des Patienten gegenseitig vertreten. Soweit an der Behandlung eines Patienten Ärzte mehrerer Organisationseinheiten beteiligt sind, kann auch eine entsprechende mehrfache Zuordnung erfolgen. Nach der Zuordnung bestimmen sich die Schranken für den lesenden wie schreibenden Zugriff auf die Daten dieses Patienten.

12. Die Erweiterung des Kreises der Zugriffsberechtigten erfolgt auf der Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes (z.B. Zuweisung zu einer weiteren funktionsbezogenen Organisationseinheit, Einbeziehung eines weiteren Arztes bei interdisziplinärer Behandlung, Konsilaufträge) ab dem Zeitpunkt des konkreten Behandlungsauftrags.

13. Durch Wechsel der Zuordnung des Patienten von einer funktionsbezogenen OE zu einer anderen OE innerhalb des Krankenhauses (Verlegung) erhalten die Behandler der neuen OE erstmals Zugriff auf die bisherigen Daten des Patienten. Die Ärzte der abgebenden OE behalten den Zugriff auf die bisherige Behandlungsdokumentation. Auf die „neuen“ Daten erhalten die Ärzte der abgebenden OE den Zugriff nur, soweit es zur Aufgabenerfüllung noch erforderlich ist.

14. Für nur zeitweise erweiterte Zugriffserfordernisse (Bereitschaftsdienst nachts oder am Wochenende) sollten notwendige Berechtigungen an „Diensthabende“ befristet und nur für ihren Zuständigkeitsbereich zugewiesen werden oder die Anwesenheit vor Ort voraussetzen. Mit dem schreibenden oder nur lesenden Zugriff auf Daten eines Patienten muss die dokumentierte Beteiligung des Arztes an der Behandlung dieses Patienten einhergehen. Ärzte sind darüber hinaus berechtigt, auch nach Ende des Patientenkontakts auf die Dokumentation der eigenen Leistungen und der mit ihnen zusammenhängenden medizinischen Daten zuzugreifen.

15. Konsilanforderungen (ergänzende Mitbehandlung) dürfen den Datenzugriff nur in Bezug auf den betroffenen Patienten eröffnen. Die Anforderung kann an einen einzelnen Arzt persönlich ergehen und damit nur diesen zum Zugriff berechtigen. In diesem Fall ist eine Weitergabe des Konsilauftrages zu ermöglichen. Die Anforderung kann aber auch an eine vorab definierte Gruppe von Konsiliarärzten (z.B. einen internen Konsiliardienst) gerichtet sein. Innerhalb der Konsiliardienstleistenden ist die Gruppe der im Einzelfall Zugriffsbefugten möglichst klein zu halten und nur auf sachliche Notwendigkeiten (Zweitmeinung, Vertretung) zu beschränken. Die Möglichkeit zur Stornierung der Konsilübernahme kann vorgesehen werden. Das Zugriffsrecht auf den Konsiliarbericht selbst bleibt davon unberührt. Der Umfang der zur Verfügung gestellten Daten und die Dauer der Zugriffsberechtigung ist an der Erforderlichkeit für die Konsiliarleistung auszurichten. Das Krankenhaus kann hierzu standardisierte Verfahren vorsehen. Möglichkeiten zur Befristung oder Sperrung des Zugriffs sind vorzusehen.

16. Ein darüber hinaus gehender Notzugriff auf Patientendaten außerhalb des differenzierten Berechtigungskonzepts ist in der Regel nicht erforderlich. Sollte er aus besonderen vorübergehenden Gründen doch unabweisbar sein, ist die zugreifende Person durch einen automatisch erscheinenden Hinweis darüber aufzuklären, dass sie außerhalb ihrer Berechtigung zugreift, einen Zugriffsgrund angeben muss und der Zugriff protokolliert und anschließend kontrolliert wird. Die Kontrolle ist hinsichtlich der Methode und der kontrollierenden und auswertenden Personen vorher unter Beteiligung der Beschäftigtenvertretung und der/des betrieblichen bzw. behördlichen Datenschutzbeauftragten festzulegen. Mindestens stichprobenartige Kontrollen durch das Krankenhaus sind erforderlich.

17. Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten. Für die konkret an der Behandlung beteiligten Mitarbeiter eines Beleg-Krankenhauses gelten die Ziff.10 ff.

Zugriffe durch Pflegepersonal

18. Der Zugriff des Pflegepersonals auf die erforderlichen pflegerischen und medizinischen Daten ist auf die in der eigenen funktionsbezogenen Organisationseinheit (z.B. Station) behandelten Patienten zu begrenzen.

19. Die Berechtigung ergibt sich bei wechselnder Zuordnung zu Organisationseinheiten (Springer) aus der dokumentierten Zuweisung zu einer OE durch die Pflegeleitung, ggf in Verbindung mit der Anwesenheit der Pflegekraft vor Ort.

20. Durch die Anordnung der Verlegung des Patienten in eine andere OE erhalten die Pflegekräfte der „neuen“ OE erstmals Zugriff auf die bisherigen Daten des Patienten. Die Pflegekräfte der abgebenden OE behalten ihre Zugriffsberechtigung nur für einen festzulegenden, eng begrenzten Zeitraum zum Abschluss der Dokumentation. Sie erhalten keinen Zugriff auf die „neuen“ Daten.

Fachübergreifende Zugriffe

21. Krankenhausmitarbeiter/innen mit fachrichtungsübergreifender Funktion (z.B. Anästhesie, Physiotherapie, OP-Personal, Diagnostik [z.B. MRT], Pathologie) sollten den Daten-Zugriff entweder durch individuelle Zuweisung oder mit dem/durch den Patientenkontakt erhalten. Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren. Die Differenzierung kann typisiert z.B. nach beauftragter Funktionsstelle, angeforderter Leistung oder Krankheitsbild des Patienten erfolgen. Bei bestimmten Mitarbeitern kann ein Zugriff auf sämtliche Daten zulässig sein.

22. Das (Zentral-)Labor bzw. deren diensthabende / handelnde Mitarbeiter/innen darf mit der Leistungsanforderung nur einen Zugriff auf die für die Befundung erforderlichen Daten des im Auftrag benannten betroffenen Patienten erhalten. Bei einem hauseigenen Zentrallabor, das nicht versichertenbezogen selbst abrechnen muss, ist eine Bearbeitung wünschenswert, bei der die Identitätsdaten der Patienten im Regelfall durch medizinisch-technische Assistenten und andere nichtärztliche Mitarbeiter nicht zur Kenntnis genommen werden können.

Nach der Behandlung

23. Nach Abschluss des Behandlungsfalles – d.h. nach Abwicklung der medizinischen und verwaltungsmäßigen Routinevorgänge – (oder nach Verlegung in ein anderes Krankenhaus) ist die elektronische Patientenakte im Sinne der jeweils geltenden rechtlichen Regelungen zu sperren. Dies kann auch im Zuge einer Überführung in ein Patientendokumentationsarchiv geschehen. Notwendig ist es, für die Sperrung eine feste Frist nach Entlassung des Patienten festzulegen. Diese Frist ist abhängig von den jeweiligen organisatorischen Abläufen im Krankenhaus (Fallabschluss durch medizinisches Controlling / Abrechnung / Qualitätssicherung). Von der Sperrung ausgenommen sind lediglich die zum Auffinden der gesperrten Patientendaten erforderlichen Identifikationsdaten.

24. Auf gesperrte Daten darf nur ein eingeschränkter Personenkreis Zugriff erhalten, um festgelegte Aufgaben erfüllen zu können (Zugriff durch ehemals behandelnde Ärzte; Auskünfte an MDK, externe Ärzte oder Patienten; Qualitätssicherung u.a.). Die zum Zugriff berechtigen Personen können unter Beachtung der bestehenden gesetzlichen Vorgaben die Berechtigung im Einzelfall delegieren. Der Zugriff ist auf diejenigen Daten zu beschränken, die zur jeweiligen Aufgabenerfüllung regelmäßig erforderlich sind. Die Zugriffsberechtigungen für diese Zwecke sollten nach der Erfahrung (Zeitspanne für Rückfragen) zeitlich begrenzt werden. Die Patientensuche in gesperrten Daten ist nur nach wenigen vorgegebenen Kennzeichen (z.B. Name, Entlassungsdatum) zu ermöglichen.

25. Eine Übertragung dieser Aufgaben und Zugriffsrechte auf ein zentrales Patienten-/Casemanagement bedarf zusätzlicher Sicherungsmaßnahmen (ggf. Buchstaben-Zuständigkeit, nur Leserecht, Protokollierung, Suche nur nach Fallnummern, ggf. nach vollem Patientennamen ohne Mustersuche u.a.), um einen zeitlich wie inhaltlich unbeschränkten Zugriff auf alle Patientenakten des Krankenhauses zu vermeiden.

26. Patientendaten sind in Krankenhausinformationssystemen zu löschen, wenn sie zur Durchführung des Behandlungsvertrags nicht mehr erforderlich sind, vorgeschriebene Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Zugriffe durch Funktionskräfte

27. Die Krankenhausverwaltung / Abrechnungsabteilung darf nur Zugriff auf die für sie erforderlichen Patientendaten (Stammdaten, Diagnosen, Leistungen usw.) haben, nicht aber auf nicht erforderliche, weitergehende medizinische Befunde / Dokumente bildgebender Verfahren.

28. Soweit zur internen Qualitätssicherung oder beim Controlling der Zugriff durch die an der Qualitätssicherung oder dem Controlling beteiligten Mitarbeiter auf alle Daten eines Patienten zugelassen werden muss, ist durch Zuständigkeits- und Funktionsaufteilungen und zeitliche Beschränkungen ein ständiger Vollzugriff auf alle Daten aller Krankenhauspatienten zu vermeiden. Soweit möglich ist eine Verwendung vorzusehen, bei der die Identitätsdaten des Patienten nicht zur Kenntnis genommen werden können.

Sonstige Zugriffe

29. Soweit Patientendaten zur Aus- oder Fortbildung außerhalb eines Behandlungskontexts benötigt werden, sind diese in geeigneter Weise zu anonymisieren, soweit nicht landesspezifische Bestimmungen abweichende Regelungen enthalten.

30. Patienten, die in anderen Krankenhäusern oder Unternehmen des Konzerns, dem das Krankenhaus angehört, (z.B. in GmbHs wie Medizinische Versorgungszentren) behandelt werden, werden dadurch nicht zugleich Patienten des Krankenhauses. Sie dürfen daher nur in den Patientenbestand des jeweiligen Krankenhauses bzw. Unternehmens aufgenommen werden. Ein gemeinsames (Krankenhaus und andere Stelle bzw. anderes Krankenhaus umfassendes) KIS ist wenn überhaupt, dann nur bei Trennung der Datenbestände in verschiedene Mandanten möglich.

Einrichtungs- und insbesondere mandantenübergreifende Zugriffe stellen datenschutzrechtlich Übermittlungen dar, deren Zulässigkeit sich nach Arzt- und Datenschutzrecht richtet.

30a. Eine Person kann mehreren Mandanten als Mitarbeiter zugeordnet werden. Greift eine solche Person im Zuge ihrer Tätigkeit für einen Mandanten auf Daten zu, die diesem Mandanten bereits zugeordnet sind, dann liegt keine Übermittlung vor, so dass die Mandantenzuordnung der Daten unverändert zu bleiben hat, gleich von wo der Zugriff erfolgte.

Neben mandantenbezogenen Datenbeständen kann ein KIS einzelne nicht personenbezogene Datenbestände vorhalten, auf die von allen Mandanten aus zugegriffen werden kann.

30b. Übermittelte Daten sind in die Primärdokumentation des empfangenden Krankenhauses zu übernehmen. Benutzen übermittelndes und empfangendes Krankenhaus unterschiedliche Mandanten des gleichen KIS, so müssen die übermittelten Daten von dem empfangenden Mandanten in seinen Datenbestand übernommen werden.

Technische Administration

31. Durch technische und administrative Rollenteilung (z.B. Systemadministration und Administration der einzelnen Anwendungen) ist ein missbräuchlicher Datenzugriff zu erschweren. Die Zugriffsrechte und Eingriffsebenen der Administratoren sind entsprechend ihren spezifischen Aufgaben zu begrenzen.

32. Die Aktivitäten der Administratoren sind revisionsfest zu protokollieren. Dies gilt auch für eine eventuell notwendige Möglichkeit, Patientendaten auf Datenträger zu kopieren. Für die Nutzung der Protokolldaten zu Kontrollzwecken ist ein Auswertungskonzept zu erstellen. Bei Remote-Zugriffen auf Arbeitsplatzrechner ist sicherzustellen, dass sie ausschließlich mit Kenntnis und Einwilligung des Nutzers erfolgen (können) und automatisch dokumentiert werden.

33. Bei einer (Fern-)Wartung durch Dritte/Externe sind besondere Maßnahmen erforderlich, damit die Wartung nur mit Wissen und Wollen des Krankenhauses im zugelassenen Umfang stattfinden kann.

Besonders schutzwürdige Patientengruppen

34. Krankenhaus-Mitarbeiter/innen als Patienten müssen davor geschützt werden, dass Kolleginnen und Kollegen von ihrem Aufenthalt erfahren (können), die nicht unmittelbar an der Behandlung beteiligt sind. Soweit dies nicht bereits durch die oben beschriebenen Maßnahmen erreicht wird, kommt (zusätzlich) u.U. eine Aufnahme unter fiktivem Namen in Betracht. Die Zuordnung von fiktivem zu tatsächlichem Namen ist geschützt und nur einem eng begrenzten Personenkreis zugänglich aufzubewahren.

35. Für Patienten, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, gilt grundsätzlich dasselbe. Die Festlegung trifft die Klinikleitung.

36. Ambulant in Nebentätigkeit behandelte Privatpatienten sind grundsätzlich nicht Patienten des Krankenhauses, sondern der insoweit berechtigten Ärzte. Ihre Behandlungsdaten dürfen anderen Mitarbeiter/innen des Krankenhauses nicht standardmäßig, sondern nur insoweit und nur so lange zugänglich sein, als sie in die Behandlung einbezogen werden (z.B. Labor). Soweit die Daten dieser Patienten im KIS verarbeitet werden sollen, sind sie getrennt von den übrigen Daten zu halten. Die Zugriffsberechtigungen für diesen Datenbestand sind getrennt von den anderen Zugriffsberechtigungen im KIS zu verwalten.

Zugriffsprotokollierung und Datenschutzkontrolle

37. Aufgrund von Art und Umfang der in einem Klinikinformationssystem verarbeiteten medizinischen und administrativen Daten bedarf es für eine datenschutzgerechte Gestaltung einer angemessenen Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Grundlage hierfür ist eine aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe sowie geeignete Auswertungsmöglichkeiten.

Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat. Dies betrifft sowohl Zugriffe aus der fachlichen Verfahrensnutzung (einschließlich des Zugriffs auf sog. Patientenübersichten mit Angaben zu der behandelnden Abteilung, Diagnosen etc.) als auch aus der administrativen Betreuung. Dabei gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.

38. Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle ist ebenso Aufgabe des Krankenhauses wie eine Kontrolle aus konkretem Anlass (s.Ziff.39).

Auskunftsrechte des Patienten

39. Der Patient muss die Möglichkeit erhalten, Auskunft über und Einsicht in alle zu seiner Person gespeicherten Daten zu bekommen. Hierzu gehören auch die nach einer Behandlung archivierten Daten sowie die Empfänger von übermittelten Daten. Auch psychiatrische und psychotherapeutische Patienten haben grundsätzlich einen gesetzlichen Auskunftsanspruch. Die Auskunft und Einsicht kann auch durch einen Ausdruck oder die Übergabe eines Datenträgers (CD, USB-Stick) erfolgen.

40. Das Auskunftsrecht umfasst auch die Information darüber, wer zu welchem Zeitpunkt welche Daten zur Kenntnis genommen hat. Werden unter Voraussetzung der Einhaltung der in Ziff. 1 bis 33 niedergelegten Grundsätze die lesenden Zugriffe nicht vollständig protokolliert, genügt es, den Kreis der Personen zu benennen, welche die Daten auf Grund ihrer Zugriffsrechte hätten zur Kenntnis nehmen können (z.B. Pflegepersonal der Station XY, Ärzte der Fachabteilung XY).

41. Da bei der Auskunft gegebenenfalls Dritte (z.B. Informationsgeber; Angehörige) vor einer Offenbarung zu schützen sind, kommt ein automatisches Kopieren und Aushändigen nicht in Betracht. Es bedarf vielmehr der Überprüfung und ggf. einer teilweisen Unkenntlichmachung durch hierzu besonders beauftragte und geschulte Mitarbeiter. Die Berechtigung zur Auskunftserteilung mit Zugriff auf die gesamte Patientenakte muss auf einen möglichst engen Personenkreis beschränkt werden.

Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

Version 1.0

Unterarbeitsgruppe Krankenhausinformationssysteme der
Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Vorbemerkung

Das vorliegende Papier ist der zweite Teil der Orientierungshilfe „Krankenhausinformationssysteme (KIS) datenschutzgerecht gestalten und betreiben“ der Arbeitskreise „Technik“ sowie „Gesundheit und Soziales“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Es beschreibt Maßnahmen zur technischen Umsetzung der bestehenden datenschutzrechtlichen Regelungen und der Vorgaben zur ärztlichen Schweigepflicht beim Einsatz von Krankenhausinformationssystemen. Sie nehmen auf die in Teil I der Orientierungshilfe dargestellten normativen Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus Bezug und geben Hinweise zu einer datenschutzkonformen Gestaltung und einem datenschutzgerechten Betrieb von Krankenhausinformationssystemen.

Unter dem Begriff „Krankenhausinformationssystem (KIS)“ wird im Folgenden die Gesamtheit aller zur Verwaltung und Dokumentation von elektronischen Patientendaten eingesetzten informationstechnischen Systeme verstanden. Dieses Papier nimmt dabei in erster Linie die zentralen, elektronische Patientenakten führenden Systeme in den Blick, hier Patientenaktensystem (PAS) genannt.[1] Dabei kann es sich sowohl um eine integrierte Gesamtlösung als auch einen Verbund selbständiger Systeme, gegebenenfalls von unterschiedlichen Herstellern, handeln. Die Anforderungen an das PAS sind jedoch grundsätzlich auf die anderen Subsysteme eines KIS übertragbar. Das PAS wie das Krankenhausinformationssystem als Ganzes müssen letztlich so gestaltet sein und so betrieben werden, dass im Gesamtkontext ein datenschutzkonformer Einsatz gewährleistet ist. Soweit die Subsysteme selbst nicht über eigene Mechanismen verfügen, die es erlauben vergleichbare Anforderungen wie im führenden System umzusetzen, kann dies auch über Schnittstellen erfolgen, um ein datenschutzkonformes Zusammenwirken der einzelnen Komponenten zu ermöglichen.

Bei den einzelnen Anforderungen wird, soweit diesen eine entsprechende Textziffer der normativen Eckpunkte (Teil I) zu Grunde liegt, auf diese Bezug genommen. Im Übrigen gehen die Anforderungen auf die rechtlichen Vorgaben zum technisch-organisatorischen Datenschutz in §§ 3a, 9 Bundesdatenschutzgesetz bzw. den entsprechenden Regelungen in den Landesdatenschutzgesetzen und kirchlichen Rechtsgrundlagen zurück. Hinsichtlich der Protokollierung (Kapitel 7) wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Protokollierung in zentralen Verfahren der Gesetzlichen Krankenversicherung[2] übernommen, soweit sie inhaltlich auf den Einsatz von Krankenhaussystemen übertragbar waren. Diese Protokollierungsanforderungen behandeln die aus Datenschutzsicht relevanten Aspekte; Protokollierungen, die im Rahmen des technischen Verfahrensbetriebs erfolgen und z.B. Betriebsparameter erfassen, werden nicht betrachtet.

Soweit konkrete Vorgaben zur Gestaltung oder Konfiguration gemacht werden, sind diese als musterhafte Umsetzungen zu verstehen, die aus der Kontroll- und Beratungspraxis der Datenschutzbeauftragten erwachsen sind. Anstelle der dargestellten Mechanismen kommen jedoch auch andere Lösungen in Betracht, wenn mit ihnen im Ergebnis das gleiche Schutzniveau bzw. die gleiche Funktionalität erreicht wird.

---

[1] Gebräuchlich ist die Bezeichnung einrichtungsinterne elektronische Patientenakte, der Begriff Patientenakte wird in diesem Text jedoch für die Akte eines einzelnen Patienten verwendet

[2] http://www.datenschutz.rlp.de/downloads/oh/dsb_oh_protokollierung_gkv.pdf

Der datenschutzkonforme Einsatz eines Krankenhausinformationssystems erfordert im ersten Schritt bestimmte Funktionalitäten in den eingesetzten Produkten. In diesem Zusammenhang sind vor allem die Hersteller entsprechender Produkte angesprochen. Deren Verantwortung erstreckt sich darauf, dass ein KIS bzw. einzelne KIS-Komponenten so gestaltet sind, dass zur Umsetzung datenschutzrechtlicher Vorgaben geeignete Funktionen und Mechanismen zur Verfügung stehen.

Im zweiten Schritt bedarf es einer Konfiguration des Systems, die im Betrieb die datenschutzrechtlichen Anforderungen berücksichtigt. Dies liegt in der Verantwortung der Betreiber der Systeme als die datenschutzrechtlich verantwortlichen Stellen.

Die Anforderungen werden daher nach drei Kategorien unterschieden:

- Anforderungen, die Konzeption und Gestaltung der Produkte durch die Hersteller betreffen (H),
- Anforderungen, die den Einsatz der Produkte im Krankenhaus betreffen und auf die Konfiguration und Nutzung durch den Anwender/Betreiber zielen (B) und
- Anforderungen, die sich an Hersteller und Betreiber gemeinsam richten, da eingeschätzt wird, dass sie eine krankenhausindividuelle Anpassung in Zusammenarbeit des Herstellers und des Betreibers erfordern (HB).

Weiterhin wird differenziert zwischen zwingenden Anforderungen („muss“), Anforderungen, ohne deren Einhaltung ein datenschutzgerechter Betrieb eines KIS wesentlich erschwert wird („soll“) und Anforderungen die allgemein einen datenschutzfreundlichen Einsatz unterstützen („sollte“). Bei nicht erfüllten Muss-Anforderungen ist ein datenschutzkonformer Betrieb eines KIS nicht gegeben.

Die Orientierungshilfe wurde erstellt von einer gemeinsamen Arbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Zusammenarbeit mit dem Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und dem Datenschutzbeauftragten der norddeutschen Bistümer der Katholischen Kirche. In die vorliegende Fassung sind weiterhin Anregungen und Kritik von Hersteller- und Betreiberseite eingeflossen.

II. Technische Anforderungen

1 Datenmodell

Die Datenbasis eines PAS besteht aus Datenobjekten. Jedes Datenobjekt ist einem Datensubjekt, dem Patienten, und einem Behandlungsfall zugeordnet. Es enthält Attribute, die sich nach ihrer Semantik in folgende Kategorien einteilen lassen:

- Patientenstammdaten,
- Verwaltungsdaten
- medizinische und
- pflegerische Daten.

Darüber hinaus enthalten die Datenobjekte Metadaten, welche z.B. den Status des Falls, die verantwortliche Stelle bzw. den verantwortlichen Arzt oder den Ersteller des Datenobjekts festhalten, sowie auf weitere Datenobjekte verweisen.

Alle Daten, die einem Behandlungsfall zugeordnet sind, bilden die (einrichtungsinterne) Fallakte des Patienten. Alle Fallakten zu einem Patienten bei ein und demselben Krankenhaus bilden dessen (einrichtungsinterne) Patientenakte.

1.1	Jedes PAS muss mandantenfähig sein (Teil I Tz. 17,30,36).	H	muss
	Verwenden verschiedene Krankenhäuser dieselbe Installation eines PAS, sind darin separate Mandanten einzurichten. Gleiches gilt für die gemeinsame Nutzung derselben Installation eines PAS durch ein Krankenhaus gemeinsam mit einer rechtlich selbständigen Stelle, insbesondere einem Medizinischen Versorgungszentrum (Teil I Tz. 17,30,36).	B	muss
	Datenbestände verschiedener Mandanten sind logisch oder physisch so zu trennen, dass Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können (Teil I Tz. 17,30,36). Für weitere Komponenten eines KIS gelten, soweit abbildbar, die Anforderungen analog.	B	muss
1.2	Jedes Datenobjekt, das sich auf einen einzelnen Patienten bezieht, ist genau einer Fallakte, jede Fallakte genau einem Mandanten zuzuordnen. Aus der Fallakte muss sich ergeben, welcher Arzt für die Behandlung zu gegebenem Zeitpunkt die Verantwortung trägt. Einzelne Datenobjekte müssen einer funktionsbezogenen Organisationseinheit bzw. einem verantwortlichen Arzt zuzuordnen sein (Teil I Tz. 11).	HB	muss

1.3	Für Datenobjekte, welche Patienten betreffen, die ambulant in Nebentätigkeit eines privat liquidierenden Arztes oder stationär durch einen privat liquidierenden Chefarzt bzw. durch einen Belegarzt behandelt werden, muss die entsprechende Zuordnung in einem Statuskennzeichen ausgewiesen werden, sofern für den behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 30).	B	muss
1.4	Die Fallakte eines Patienten muss Angaben aufnehmen können, welchen funktionsbezogenen Organisationseinheiten ein Patient derzeit zugeordnet ist. Hierbei soll zwischen Behandlung und Mitbehandlung (auch Konsil) unterschieden werden können. Es muss eine flexible Mehrfachzuordnung von Patienten zu Ärzten oder pflegerischen und medizinischen Organisationseinheiten möglich sein. Ziel ist es, umfassende generelle Zugriffsrechte zu vermeiden und stattdessen die im Rahmen der Behandlung erforderlichen Zugriffe abzubilden (Teil I Tz. 10,11,12,13,18).	H	muss
1.5	Für jedes patientenbezogene Datum mus sich unabhängig vom Inhaltstyp bestimmen lassen, wer es wann erstellt und wer es wann wie modifiziert hat. Werden z.B aus Haftungsgründen Vidierungen (Freigabenachweise; Teil I, Tz. 10; vgl. auch Tz. 3.9) verwendet, muss sich für jedes hierfür vorgesehene Datum bzw. sachlich zusammenhängenden und gemeinsam zur Anzeige gebrachten Datensatz (Befund, Diagnose) erkennen lassen, ob er vidiert wurde und ggf. durch wen.	H	muss
1.6	PAS müssen eine Trennung von Daten in Datenobjekte erlauben, welche den unter Tz. 1 genannten Kategorien zugeordnet sind. Diese Trennung muss in den Bildschirmmasken zur Abfrage/Recherche, zur Datenpräsentation, beim Datenexport, im Rollen und Berechtigungskonzept sowie bei der Protokollierung berücksichtigt werden können (Teil I Tz. 4,9,10,17,30). Beispiele für solche Datenobjekte sind Einzelbefunde, Einträge in die Pflegedokumentation, Einträge in die Liste der abrechenbaren Leistungen. PAS sollen eine Trennung von Patientenstammdaten und Datender anderen Kategorien ermöglichen.	HB	muss
1.7	Das Datenmodell eines PAS sollte die Anlage eines klinischen Basisdatensatzes (vgl. Teil 1, Tz. 5) ermöglichen. Das PAS sollte es dem Betreiber ermöglichen, Datenobjekte zu kennzeichnen, die standardmäßig oder patientenindividuell in den Basisdatensatz eingehen sollen. (Teil I Tz. 5/Teil II Tz. 3.13)).	H	sollte
	Welche Inhalte in einen Basisdatensatz übernommen werden, liegt in der Verantwortung des Betreibers.	B	
1.8	Für Behandlungsfälle und deren Datenobjekte muss erkennbar sein, ob in dem Fall, dem es zugeordnet ist, die Behandlung fortdauert, die Behandlung beendet, die Abrechnung jedoch noch nicht vollzogen ist, oder der Fall abgeschlossen ist. Ebenso muss erkennbar sein, wenn ein Datenobjekt einem gesperrten oder archivierten Fall zugeordnet ist (vgl. Tz. 2.11). Entsprechende Kennzeichnungen müssen in der Fallakte festgehalten werden können. Das Rollen- und	HB	muss

	Berechtigungskonzept muss es ermöglichen, dass an diese Kennzeichnungen besondere Zugriffsregelungen geknüpft werden. (Teil I Tz. 2,4,23,24).		
1.9	Für Datenobjekte innerhalb einer Fallakte soll die Möglichkeit bestehen, Kennzeichen zu setzen, das festhält, dass der Patient der Hinzuziehung dieser Vorbehandlungsdaten ganz oder teilweise widersprochen hat. Das Kennzeichen muss jederzeit wieder gelöscht werden können. Vergabe/Rücknahme des Kennzeichens sollen durch das Rollen- und Berechtigungskonzept geregelt werden (Teil I Tz. 4, 7).	H H B	soll muss soll
	Das PAS soll die Möglichkeit bieten, das Widerspruchskennzeichen in Abhängigkeit vom Verarbeitungskontext bei nachfolgenden Zugriffen anzuzeigen oder zu unterdrücken.	HB	soll
1.10	Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob und ab wann für den Patienten eine Auskunftssperre gilt (Teil I Tz. 6).	H	muss
1.11	Fallakten müssen bei Bedarf dahingehend gekennzeichnet werden können dass der Patient Mitarbeiter des behandelnden Krankenhauses ist, bzw. dass für die Fallakte ein besonderes Schutzniveau gilt. Das Rollen- und Berechtigungskonzept muss es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können (Teil I Tz. 34).	HB	muss
	Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden.	B	muss
1.12	Fallakten müssen bei Bedarf dahingehend gekennzeichnet werden können, dass sie bekannte Personen des öffentlichen Lebens, Personen, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, betreffen, oder dass für die Fallakte ein besonderes Schutzniveau gilt. Das Rollen- und Berechtigungskonzept muss es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können (Teil I Tz. 34).	H	muss
1.13	Die unter Tz. 1.10 und 1.11 genannten Kennzeichen sollen nicht dazu verwendet werden können, gezielt nach solchen Patienten zu suchen. Soweit eine solche Funktion unverzichtbar ist, ist sie an eine gesonderte funktionelle Rolle zu binden, die nur einem sehr eng begrenzten Personenkreis zugewiesen wird (Teil I, Tz. 10).	HB	soll
1.14	Warnhinweise administrativer oder medizinischer Natur sollen nur mit einem (konfigurierbaren) Wertevorrat belegt werden können und nicht als Freitextfelder gestaltet sein (Teil I Tz. 3).	H	soll
1.15	Wenn Patientendaten für allgemeine Auswertungszwecke, die keinen Patientenbezug erfordern, in eine separate Architekturkomponente übernommen werden (z.B. Data Warehouse), muss eine Anonymisierung erfolgen (Teil I, Tz. 29). Externe Komponenten für Auswertungen, die keinen Patientenbezug erfordern, dürfen nur dann auf den Datenbestand des PAS zugreifen, wenn eine Identifizierung von Patienten anhand der im Zugriff stehenden Daten ausgeschlossen ist.	HB	muss

2 Systemfunktionen

2.1	Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren.	HB	soll
2.2	Ein PAS sollte es ermöglichen, bei der Übertragung von Daten von einer Komponente in eine andere Referenzen auf Datenobjekte statt der Datenobjekte selbst zu übertragen (Vermeidung der Datenduplizierung). Soweit eine redundante Datenhaltung unvermeidbar ist, müssen Sperrungen, Auslagerungen oder Löschungen in allen betroffenen Datenbeständen berücksichtigt werden.	H HB	Sollte muss
2.3	In das KIS sollte ein Single-Sign-On-Dienst integrierbar sein.	H	sollte
2.4	Bei einem KIS mit eigenständigen Subsystemen muss eine Parallelführung von Mandanten möglich sein. Dies bedeutet, dass Datenübernahmen mandantenbezogen vorgenommen werden können. So müssen z.B. Daten des Mandanten A auf dem Laborsystem in die Komponente Behandlungsdokumentation des Mandanten A und Daten des Mandanten B im Laborsystem in die Behandlungsdokumentation des Mandanten B übernommen werden können (Teil I Tz. 17,30,36).	HB	muss
2.5	Werden im Zuge des Datenaustauschs zwischen verschiedenen Komponenten des KIS Dienstleistungen externer Provider in Anspruch genommen, muss für eine Transportverschlüsselung gesorgt werden. Die Schlüssel dürfen sich nur in alleiniger Kontrolle des Krankenhauses befinden.	HB	muss
2.6	Kennzeichen nach 1.2 bis 1.4 und 1.7 bis 1.11 sollen in den verschiedenen Komponenten des KIS abgebildet werden können, sofern sie für deren Nutzung nicht offensichtlich irrelevant sind. (Bsp: Eine Tumordokumentation muss keine Angaben über eine Auskunftssperre i.S.v. Teil I Nr. 6 enthalten.) Für die Kennzeichen nach 1.3 und 1.7 ist dies zwingend erforderlich (Teil I, Tz. 10).	HB	soll
2.7	Berechtigungen auf Datenobjekte und ggf. Funktionen sollten in den verschiedenen Komponenten des KIS in gleicher Weise abgebildet werden können, jedenfalls insoweit als die Nutzermengen sich überschneiden (Teil I, Tz. 10,13,18,21,27).	H	soll
2.8	Speichermedien, welche Daten des KIS aufnehmen, müssen eine Verschlüsselung ermöglichen (Datenträger- / Datenbank- / Dateisystem-verschlüsselung). Dies gilt insbesondere für Datensicherungen und Daten, welche sich auf mobilen Systemen befinden. Das Informationssicherheits-konzept des Krankenhauses hat den besonders hohen Schutzbedarf des verwendeten Schlüsselmaterials zu berücksichtigen. Die verwendeten Schlüssel dürfen für externe Dienstleister und im Rahmen der technischen Administration grundsätzlich nicht im Zugriff stehen.	HB B	muss muss

2.9	Das KIS muss über eine Funktion verfügen, die es ermöglicht, eine Übersicht der zu einem Patienten im KIS gespeicherten Daten zu erzeugen (Teil I Tz. 39, 41). Diese Funktion dient der Datenschutzkontrolle sowie der Beantwortung von Auskunftsersuchen nach § 34 BDSG bzw. landesrechtlichen Regelungen.	H	muss
2.10	Es muss möglich sein, zeit- und ereignisgesteuert abgeschlossene (→1.8) Fallakten oder Teile davon zu sperren oder sie in ein Archiv auszulagern, und sie dem operativen Zugriff zu entziehen. Das PAS muss es erlauben, einzelne Angaben zur zweifelsfreien Identifikation des Patienten festzulegen und diese für eine Suche vorzuhalten. Über Abfragefunktionen, die gesperrte/ausgelagerte Datensätze betreffen, dürfen zunächst nur diese Daten angezeigt werden. Soweit für bestimmte Aufgaben ein Zugriff auf gesperrte/ausgelagerte Behandlungsfälle erforderlich ist, dürfen die darüber hinausgehenden Daten erst nach dem unter Tz. 4.9 beschriebenen Verfahren bereitgestellt werden (Teil I Tz. 23,24).	H	muss
	Das Krankenhaus muss einen Zeitraum von unter einem Jahr festlegen, nach dem abgeschlossene Fallakten gesperrt oder ausgelagert werden.	B	muss
2.11	Das PAS muss über eine Funktion verfügen, die sicherstellt, dass nach Ablauf festgelegter Speicherfristen Behandlungsfälle gelöscht werden. Löschung bedeutet in diesem Zusammenhang eine physikalische Löschung. Eine Markierung als „gelöscht“, mit der Folge, dass die Daten lediglich nicht mehr angezeigt werden, ist nicht ausreichend (Teil I Tz. 26).	H	muss
2.12	Lösch- und Auslagerungsaufträge müssen zwischen den Komponenten eines KIS propagiert werden können. Einzelne Datenbestände (für die womöglich gesonderte Aufbewahrungsfristen gelten) müssen vom Löschvorgang ausgenommen werden können (Teil I Tz. 26).	H	muss
2.13	Das PAS muss über eine Funktion verfügen, die es ermöglicht, einzelne Datenfelder oder Behandlungsfälle zu löschen oder zu sperren (Teil I, Tz. 26).	H	muss
	Sperr- und Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Mitarbeitern eingesetzt werden.	B	muss
2.14	Jede Komponente eines PAS soll eine effiziente Replikation des Datenbestandes in ein Testsystem ermöglichen, das zur Fehlersuche und zum Test von Maßnahmen der Fehlerbehebung dient. Im Zuge der Replikation des Datenbestandes soll es möglich sein, eine Pseudonymisierung etwa durch Ersatz der Identifikationsdaten mit Dummy-Daten durchzuführen.	H	soll
2.15	In das KIS muss ein Pseudonymisierungsdienst eingebunden werden, der verwendungszweckspezifisch temporäre Patientenkennzeichen oder Pseudonyme auf der Basis der gespeicherten Identitätsdaten generiert und verwaltet (Teil I, Tz. 28)[3].	HB	muss

[3] Dieser Pseudonymisierungsdienst ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf ein Empfänger nur pseudonymisierte Daten erhalten, muss zusätzlich geprüft und sichergestellt werden, dass ein Re-Identifizierung durch den Inhalt des Datensatzes mit verhältnismäßigem Aufwand nicht möglich ist.

3 Anwendungsfunktionen

3.1 Anwender interagieren mit dem PAS innerhalb der ihnen zur Verfügung stehenden Verarbeitungskontexte durch Ausführung von Transaktionen[4] zur Dateneingabe, Datenpräsentation, Datenimport oder Datenexport. Hierbei beeinflusst der jeweils aktive Verarbeitungskontext ggf. die Ergebnisse der Transaktion, etwa durch Eingrenzung der in einen Suchlauf einbezogenen Patienten und durch Auswahl der im Ergebnis angezeigten Datenfelder (→3.4). Die Verarbeitungskontexte müssen derart konfigurierbar sein, dass ein Verarbeitungskontext lediglich die Transaktionen zur Verfügung stellt, die zur Ausübung der funktionellen Rolle erforderlich ist, denen er zugeordnet ist.
Mindestens folgende Verarbeitungskontexte soll ein PAS unterscheiden (soweit die entsprechenden funktionellen Rollen durch das PAS unterstützt werden): H soll

- Administrative Patientenaufnahme
- Behandlung
  - Behandlung nach fachlicher Zuordnung
  - Mitbehandlung auf Anfrage oder Anordnung eines Arztes mit bestehendem Behandlungszusammenhang
  - Konsil
  - Behandlung im Bereitschaftsdienst außerhalb der fachlichen Zuordnung
  - Notbehandlung außerhalb eines Bereitschaftsdienstes und ohne fachliche Zuordnung des Patienten zu einer OE des Behandlers
  - OP
  - Physiotherapie
- Pflege
- Diagnostik (je unterstützter Leistungsstelle, z.B. Labor)
- Therapeutische Leistungsstellen (je unterstützter Leistungsstelle, z.B. Strahlentherapie)
- Kodierung und Freigabe der diagnosebezogenen Fallgruppen (DRG)
- Sozialarbeit
- Qualitätssicherung
- Abrechnung

[4] Dieses Papier verwendet den Begriff Transaktion unabhängig von seiner softwaretechnischen Realisierung und nicht notwendig im datenbanktechnischen Sinn

- Controlling (differenziert nach unternehmenssteuerndem und abrechnungsorientiertem Controlling)
- Ausbildung (differenziert nach Ausbildungsziel und Vorgängen innerhalb und außerhalb eines Behandlungskontextes)
- Verwaltung (verwaltungsmäßige Abwicklung des Behandlungsvertrages, insbesondere Abrechnung)
- Dokumentation für Zwecke der GKV (über die Regelabrechnungsvorgänge hinaus) oder auf der Grundlage anderer gesetzlicher Anordnung
- Revision
- Datenschutzkontrolle

	Für die Erfüllung der Aufgaben auf verschiedenen Funktionsebenen des Krankenhauses sollten verschiedene Verarbeitungskontexte abgebildet werden können	H B	soll
3.2	Bei Beginn der Sitzung und vor jeder Transaktion, deren Ausführung vom Verarbeitungskontext abhängt, muss es möglich sein einen Benutzerwechsel oder einen Wechsel des Verarbeitungskontexts zu vorzunehmen. Beachte jedoch 4.4. Ein Benutzerwechsel/Wechsel des Verarbeitungskontexts muss eine an den neuen Benutzer und dessen Zugriffsrechte angepasste Datenpräsentation und Anwendungsfunktionen zur Folge haben (Teil I, Tz. 10,18,21,24,27). Bei einem Wechsel der Verarbeitungskontexte kann ein Bezug der im alten Verarbeitungskontext geöffneten Fallakte (Fall-ID) an den neuen Verarbeitungskontext übergeben werden, sofern und soweit gewährleistet ist, dass diese Fallakte im neuen Verarbeitungskontext nur geöffnet wird, falls sie im Ergebnis einer im neuen Verarbeitungskontext zulässigen Suche oder Abfrage gefunden werden kann.	H	muss
3.3	Ein PAS muss es ärztlichen Mitarbeitern ermöglichen, einen Behandlungsfall für den Zweck der Mitbehandlung durch Dokumentation einer ärztlichen Entscheidung zu delegieren. Es muss die Möglichkeit vorsehen, diese Delegierung zeitlich zu befristen und hierfür eine Standardfrist vorzukonfigurieren (Teil I, Tz. 12,15).	H	muss
3.4	Ein PAS muss es ermöglichen, die Bearbeitungs- und Recherchefunktionen einschließlich der angebotenen Suchattribute und im Ergebnis anzuzeigenden Datenfelder in Abhängigkeit von Verarbeitungskontext und Zugriffsberechtigungen anzupassen. Menüpunkte und Bildschirmmasken müssen in dieser Hinsicht flexibel gestaltet werden können (Teil I Tz. 4,10,30).	H B	muss
	Das Krankenhaus muss in seinem Berechtigungskonzept für jeden Verarbeitungskontext festlegen, welche Funktionen für die Ausübung der mit ihm verbundenen funktionellen Rolle erforderlich sind und bereitgestellt werden. Insbesondere muss es in seinem Berechtigungskonzept die für den	B	muss

	jeweiligen Verarbeitungskontext für eine Suche erforderlichen Attribute nach ihrer Erforderlichkeit festlegen (Teil I, Tz. 10,18,21,24,27).		
3.5	Das PAS muss über eine Funktion verfügen, mit der im Rahmen der Aufnahme eines Patienten eine Kurzübersicht mit den zugelassenen (→ Tz. 1-2, Teil 1) Daten zurückliegender Behandlungsfälle erzeugt werden kann (Teil I Tz. 1 - 5, 23,24).	H	muss
3.6	Das Ergebnis der Suchfunktionen muss in Abhängigkeit vom Verarbeitungskontext konfigurierbar sein hinsichtlich der dargestellten Attribute und der in die Suche einbezogenen Patienten, insbesondere unter Berücksichtigung der Kennzeichen nach 1.2 bis 1.4 und 1.7 bis 1.11.	H	muss
3.7	Übersichtslisten mit Patientendaten (etwa Stationslisten) müssen in Abhängigkeit vom Verarbeitungskontext konfigurierbar sein (Teil I, Tz. 10,18,21,24,27).	H	muss
3.8	Ein PAS muss im Zuge eines Datenzugriffs im Notfall-Verarbeitungskontext den Zugreifenden zu einer ärztlichen Dokumentation der Erforderlichkeit dieses Notfallzugriffs solange auffordern, bis diese, ggf. auch im Nachhinein, erbracht wird. (vgl. Tz. 4.9).	H	muss
3.9	Ein PAS muss eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein.	H	muss
3.10	Ein PAS muss es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9).	H	muss
3.11	Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden.	H B	soll
3.12	Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 28)[5].	H B	soll
3.13	Das PAS sollte über eine Funktion verfügen, mit der ein klinischer Basisdatensatz erzeugt werden kann (Teil I Tz. 5 / Teil II 1.7).	H	sollte
3.14	Das PAS muss über eine Funktion verfügen, mit der eine Übersicht erstellt werden kann, welche Personen während der Dauer der Speicherung eines Behandlungsfalles auf diesen zugegriffen haben (vgl. Tz. 7). Soweit unter Berücksichtigung der unter Tz. 7.2/7.8 genannten Anforderungen lesende Zugriffe nicht protokolliert werden, muss die Übersicht erkennen lassen, welche Stellen grundsätzlich zugriffsberechtigt waren (Teil I Tz. 40).	H	muss
3.15	Das PAS sollte die Möglichkeit unterstützen, in den nach TZ. 1.10, 1.11 gekennzeichneten Fällen einzelne Datenbereiche (z.B. Diagnosen, Laborwerte, Pflegedaten) verschlüsseln zu können. Die Möglichkeit zur (automatischen) Entschlüsselung sollte als Zusatzrolle den jeweiligen Beschäftigten zugewiesen	H	sollte

[5] Dies ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf eine Empfänger nur pseudonymisierte Daten erhalten, muss zusätzlich geprüft und sichergestellt werden, dass eine Re-Identifizierung durch den Inhalt des Datensatzes mit verhältnismäßigem Aufwand nicht möglich ist.

werden können.

3.16	Die Speicherorte medizinischer Daten sowie die Möglichkeit zum Export von Daten sollten durch Konfiguration beschränkbar sein, z.B. sollte die Datenspeicherung lokal auf den Arbeitsplatzrechnern unterbunden werden können.	H	sollte

4 Rollen- und Berechtigungskonzept

4.1 Das Berechtigungskonzept des PAS muss es ermöglichen, Berechtigungen anknüpfend an folgende Attribute eines Datenobjekts bzw. der Patientenakte zu erteilen: H muss

- Zuordnung des Patienten zu Organisationseinheiten
- Dokumentierte ärztliche Anweisungen (u.a. Leistungsanforderungen) und explizite Delegierungen
- Datenkategorie
- Kennzeichen nach 1.2 – 1.4, 1.7 – 1.11
- Ersteller des Datenobjekts / eines Datenobjekts in der Patientenakte
- Impliziter oder explizit erklärter Verarbeitungskontext

Das Berechtigungskonzept muss es ferner erlauben, Rechte zeitabhängig zu vergeben, und sollte es ermöglichen, Rechte in Abhängigkeit von

- dem Ort des Zugreifenden, insbesondere im Verhältnis zum Patienten,
- einem Dienst- oder Bereitschaftsplan, und
- dem hinterlegten Behandlungspfad des Patienten

zu erteilen (Teil II 4.8)

4.2 Das Rollen- und Berechtigungskonzept muss grundsätzlich folgende Benutzerkategorien unterscheiden: H muss

- Ärztliche Mitarbeiter
- Nicht-ärztliches medizinisches Fachpersonal (z.B. Pflegekräfte)
- Verwaltungskräfte
- Ausbildungskräfte
- Externe Kräfte
- Administration

4.3 Das Rollenmodell muss zumindest nach folgenden strukturellen Rollen differenzieren: H muss

- Administrative Aufnahmekraft
- Medizinische Aufnahmekraft
- QS-Management
- Pflegekraft/Leitende Pflegekraft
- Funktionskraft

- Konsiliar
- Bereitschaftsdienst
- Belegarzt
- Behandelnder Arzt
- Honorar-Arzt
- Honorar-Pflegekraft
- Verwaltungsmitarbeiter
- Mitarbeiter Forschung
- Controlling
- Datenschutzbeauftragter
- Revision
- Sekretariat / Hilfskraft
- Ausbildungskraft
- Wartung
- Anwendungsadministration
- Berechtigungsadministration
- Seelsorge

4.4	Zur Definition von Rechten muss es möglich sein, Organisationseinheiten flexibel und überlappend zu definieren (Teil I, Tz. 11,12). Beispielsweise überlappen sich die OE „psychiatrischer Konsiliardienst“ und „psychiatrische Fachabteilung“, wo beide bestehen, so dass es möglich sein muss, einen Facharzt beiden OE zuzuordnen.	H	muss
	Der Verarbeitungskontext (oder die Menge der verfügbaren Verarbeitungskontexte) sollte für alle Mitglieder einer Organisationseinheit gleich sein.	B	sollte
4.5	Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann.	B	muss
4.6	Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen.	H	muss
4.7	Das PAS muss über eine Funktion verfügen, die es erlaubt, für bestimmte Berechtigungen in einer Übersicht die Benutzer darzustellen, die über diese Berechtigung verfügen.	H	muss
4.8	Das PAS muss über eine Funktion verfügen, mit der ein Behandlungsfall einer weiteren funktionsbezogenen Organisationseinheit oder einzelnen Behandlern dauerhaft oder befristet zur Mitbehandlung oder zum Konsil zugewiesen werden kann (Teil I Tz. 11,14,15,20,21,24 / Teil II Tz. 4.1).	H	muss

	Die notwendigen Zugriffsberechtigungen auf alte bzw. neue Daten (vgl. Teil I Tz. 13) sollten automatisiert angepasst werden können. Alternativ hierzu kommt ein bedarfsweises Aneignen der notwendigen Berechtigungen nach dem unter Tz. 4.9 beschriebenen Verfahren in Betracht.	B	sollte
4.9	Das Berechtigungskonzept muss die Möglichkeit bieten, Zugriffsbeschränkungen situationsbezogen aufzuheben bzw. Zugriffsrechte zu erweitern. Dies gilt insbesondere für Notfallzugriffe, Zugriffe im Rahmen retrospektiver Prüfungen oder Zugriffe im Rahmen der Qualitätssicherung. Dabei ist ein zweistufiges Verfahren vorzusehen, bei dem vor der Ausführung einer Transaktion in einem ersten Schritt • ein Hinweis auf die Erweiterung der Zugriffsrechte und die Protokollierung des Vorgangs erfolgt, oder • eine Begründung für die Erforderlichkeit der Transaktion eingegeben werden muss (vgl. Tz. 3.9), oder • die Bestätigung durch einen zweiten berechtigten Mitarbeiter erfolgen muss (4-Augen-Prinzip)	HB	muss
	und im zweiten Schritt der Zugriff eröffnet wird. Dabei soll die Möglichkeit bestehen, den Zugriff zeitlich zu beschränken (z.B. 24 Std.)	HB	soll
	Der Vorgang ist revisionssicher zu protokollieren. Die Protokollierung muss den anfordernden Benutzer, die Fall-/Patientennummer, den Zeitpunkt des Zugriffs und gegebenenfalls den Zugriffsgrund erkennen lassen. Eine Protokollierung muss auch erfolgen, wenn der Zugriffsversuch abgebrochen wurde (Teil I Tz. 16,24). Die Protokolle eines nach dieser Tz. Eingerichteten zweistufigen Verfahrens zur Zugriffsrechteerweiterung müssen in die vorbeugende Datenschutzkontrolle (→7.22) mit einer Prüfdichte einbezogen werden, welche die diesem Verfahren eigenen Risiken besonders berücksichtigt. Hierzu hat das Krankenhaus sein Berechtigungskonzept derart einzurichten, dass die Zahl der Einsätze des zweistufigen Verfahrens, die nicht im Nachhinein mit einem automatisierten Verfahren auf Legitimität überprüft werden können, hinreichend klein bleibt.	HB	muss
4.10	Rollen und Berechtigungen z.B. für Bereitschaftsdienste oder Vertretungen müssen einer Benutzerkennung einfach und flexibel zugeordnet werden können, um etwaigen wechselnden Aufgabenstellungen Rechnung zu tragen. Hierbei sollen auch zeitliche Muster und Dienstpläne abgebildet werden können (z.B. Rolle Bereitschaftsdienst am Wochenende oder für einen bestimmten Zeitraum; Teil I, Tz. 14).	H	muss sollte
4.11	Zur Authentisierung von Mitarbeitern gegenüber dem KIS sollte ein Zwei-Faktor-Verfahren eingesetzt werden. Das KIS sollte es ermöglichen, Datenzugriffe an die Anwesenheit eines bestimmten Benutzers, nachgewiesen	H	sollte

	durch z.B. einen maschinenlesbaren Mitarbeiterausweis, ein RFID-Tag oder ein vergleichbares Token zu knüpfen (Teil I Tz. 12,15,16,19).		
4.12	Es muss sichergestellt sein, dass es keinem Nutzer möglich ist, durch die Verknüpfung von Rechten und den Wechsel des Verarbeitungskontexts sich über die Summe der ihm erteilten Rechte hinaus zusätzliche Rechte anzueignen. Insbesondere müssen die Zugriffsbeschränkungen auch bei dem Zugriff auf Daten über Patientenlisten und die Suchfunktion beachtet werden (Teil I, Tz. 10,18,21,24,27).	H	muss
4.13	Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben.	H	muss
4.14	Das Krankenhaus muss strukturelle Rollen so zuschneiden, dass sie sich unabhängig von der konkreten Person an der Stellung in der Krankenhausorganisation, es muss funktionelle Rollen so zuschneiden, dass sie sich unabhängig von einer konkreten Person an einer abgrenzbaren fachlichen Aufgabe und den hiermit in Zusammenhang stehenden Tätigkeiten orientieren (Teil I, Tz. 10,18,21,24,27).	B	muss
4.15	Die Einrichtung von gemeinsam zu nutzenden Benutzerkennungen muss grundsätzlich vermieden werden. In Betracht kommen solche Benutzerkennungen ausnahmsweise z.B. für den Verarbeitungskontext „Pflegekräfte in Stationszimmern“ oder im OP-Bereich. Für den Bereich der Administration sind sie unzulässig.	B	muss
4.16	Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Teil I, Tz. 10,18,21,24,27).	H	muss
4.17	Die Benutzerverwaltung sollte über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Mitarbeitern automatisiert zu deaktivieren (Teil I, Tz. 10,18,21,24,27).	HB	sollte
4.18	Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer für einen festgelegten Zeitraum keine Anmeldung mehr erfolgt ist.	H	sollte
	Diese Funktion dient der Datenschutzkontrolle durch die Aufsichtsbehörden und die betrieblichen/behördlichen Datenschutzbeauftragten der Krankenhäuser. Einer missbräuchlichen Nutzung durch den Arbeitgeber muss durch das Berechtigungskonzept bzw. geeignete organisatorische Maßnahmen begegnet werden.	B	
4.19	Das PAS muss es ermöglichen, dass für die Verfahrensbetreuung und die Berechtigungsverwaltung unterschiedliche Personen mit separaten Benutzerkennungen festgelegt werden können (vgl. Tz. 8.1). Die Berechtigungsverwaltung muss bei Bedarf auf mehrere Personen verteilt werden können.	H	muss
4.20	Für ein gegebenes Datenobjekt muss effizient bestimmt werden können, welche Mitarbeiter darauf schreibend oder lesend zugreifen können.	H	muss

5 Datenpräsentation

5.1	Das PAS muss es ermöglichen, in Abhängigkeit vom Verarbeitungskontext in den Bildschirmmasken die Anzeige von Teilen der Patientenakte mit oder ohne Darstellung der Identitätsdaten des Patienten zu konfigurieren, z.b. für Schulungszwecke. Das PAS muss es ermöglichen, die Darstellung der Patientenidentifikationsdaten nach dem in Tz. 4.9 beschriebenen Verfahren hinzuzuschalten (Teil I, Tz. 10,18,21,24,27).	H	muss
5.2	Das PAS soll es ermöglichen, in Abhängigkeit vom Verarbeitungskontext Teile der Patientenakte mit Pseudonymen, die die Identitätsdaten des Patienten ersetzen, darzustellen (Teil I Tz. 28)[6].	HB	soll
5.3	Das PAS sollte die Oberflächen verschiedener Verarbeitungskontexte klar voneinander optisch (z.B. farblich) unterscheiden. Dies gilt insbesondere für die Oberfläche des Notfallzugriffs.	H	sollte
5.4	Es muss die Möglichkeit bestehen Kennzeichen nach 1.2 bis 1.4 und 1.7 bis 1.12 in Bildschirmmasken zu integrieren.	H	muss

[6] Dies ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf eine Empfänger nur pseudonymisierte Daten erhalten, muss zusätzlich geprüft und sichergestellt werden, dass eine Re-Identifizierung durch den Inhalt des Datensatzes mit verhältnismäßigem Aufwand nicht möglich ist

6 Nutzungsergonomie

6.1	Ein PAS muss einen schnellen Benutzerwechsel ermöglichen (vgl. Tz. 3.2).	H	muss
6.2	Ein PAS und zugehörige Subsysteme sollten unter Voraussetzung der Verwendung einer Zwei-Faktor-Authentisierung in ein Single-Sign-On-Verfahren einbezogen werden können.	HB	sollte
6.3	Im PAS muss eine (arbeitsplatzabhängige) automatische Arbeitsplatzsperre eingerichtet werden.	HB	muss
6.4	Wird beim Login (als einer der beiden einzusetzenden Faktoren) ein Token eingesetzt, so sollte nach Login eines Nutzers das Entfernen des Tokens zur Sperrung, das Einführen des Tokens zur Freischaltung der Arbeitsstation, insbesondere nach einem Auto-Logout genutzt werden können.	HB	sollte
6.5	Jedem Nutzer muss ein Standard-Verarbeitungskontext zugeordnet werden können (Teil I, Tz. 10,18,21,24,27).	H	muss
6.6	Ein PAS sollte die Speicherung und Wiederaufnahme einer Sitzung an einem anderen Arbeitsplatz innerhalb des Krankenhauses ermöglichen. Zur Wiederaufnahme einer Sitzung an einem anderen Arbeitsplatz muss die gleiche Authentisierung wie bei der Initialisierung der Sitzung vorgesehen werden.	H H	sollte muss
6.7	Es muss mit geringem Aufwand möglich sein, Transaktionen zur Dokumentation von ärztlichen Anweisungen, welche Rechteänderungen nach sich ziehen, (etwa eine Konsilanforderung) auszuführen (Teil I, Tz. 15).	H	muss
6.8	Ein PAS sollte die Hinterlegung von Behandlungspfaden und Geschäftsprozessen (etwa für die Abrechnung) in der Fallakte ermöglichen, mit Hilfe derer rechterelevante Änderungen der Zuordnung des Patienten zu Organisationseinheiten (Behandlung und Pflege) und einzelnen Mitarbeitern (Verwaltung und Qualitätssicherung) vorgeplant und diese Änderungen (etwa Verlegungen) einfach aktiviert werden können (Teil I, Tz. 10,18,21,24,27).	H	sollte
6.9	Die Arbeitsoberfläche zur Rechte- und Rollenverwaltung muss übersichtlich gestaltet sein, die Auswirkung der Erteilung von Rechten und Rollen klar zu erkennen geben, und ein einfaches Backup und Restore (von Teilen) der Rechtekonfiguration ermöglichen. Die für die Rechteverwaltung einzusetzenden Transaktionen müssen hinreichend performant ausgeführt werden können, so dass geänderte Zugriffsrechte unmittelbar wirksam werden.	H	muss
6.10	Zur Interpretation und Zulässigkeitsprüfung von Datenzugriffen sollte das PAS eine transparente Verknüpfung von Protokolldaten, Inhaltsdaten und ggf. Dienstplänen ermöglichen.	H	sollte

6.11	Die Gestaltung des KIS soll den Anforderungen an die Ergonomie der eingesetzten Software, wie sie in den Normen ISO 9241 und DIN EN ISO 14915 beschrieben sind, entsprechen. Insbesondere ist zu ermöglichen, dass für die datenschutzrelevanten Funktionen bei Bedarf erläuternde Informationen oder Hilfestellungen aufgerufen werden können.	H	soll
6.12	Technische Schutzmaßnahmen müssen so implementiert werden, dass sie vom Nutzer kontrolliert werden können. Ein versehentliches Abschalten muss möglichst verhindert werden. Jede Freigabe muss als bewusster Akt erfolgen.	HB	muss
6.13	Durch Schulungen müssen die Beschäftigten regelmäßig für Datenschutzfragen sensibilisiert werden um sicher zu stellen, dass die Sicherheitsfunktionen des KIS ordnungsgemäß genutzt werden.	B	muss

7 Protokollierung

7.1	Für Zwecke der Datenschutzkontrolle muss eine Protokollierung relevanter Ereignisse vorhanden sein. Die Protokollierung muss darüber Auskunft geben können, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat. Neben der erstmaligen Speicherung personenbezogener Daten, deren Änderung und gegebenenfalls Löschung/Sperrung müssen auch lesende Zugriffe auf personenbezogene Daten nachvollzogen werden können (Teil I Tz. 16,25,32,37).	H	muss
7.2	Die Art und der Umfang der Protokollierung müssen sich an der Art und Weise der Verarbeitung und am Schutzbedarf der jeweiligen Daten orientieren. Die Protokollierung ist auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken. Eine detaillierte Protokollierung ist entbehrlich bei Zugriffen im Rahmen technisch festgelegter Prozesse, bei denen in wiederkehrender Weise bestimmte Verarbeitungsschritte aufeinander folgen (Workflow) soweit diese anhand der Dokumentation des Verfahrens nachvollziehbar sind. In diesem Fall ist es ausreichend, den Start des Workflows zu dokumentieren. Art und Umfang der Protokollierung, die Verfahrensweisen zur Speicherung und Auswertung, die getroffenen Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen sowie die Aufbewahrungsdauer der Protokolldaten sind in einem Protokollierungskonzept festzulegen.	HB B	muss muss
7.3	Die Protokollierung muss hinsichtlich des zu protokollierenden Sachverhalts vollständig sein. Eine stichprobenweise Protokollierung oder die Protokollierung lediglich eines bestimmten Anteils von Zugriffen ist für eine effektive Datenschutzkontrolle untauglich (Teil I Tz. 37).	B	muss
7.4	Die Auswertung der Protokollierung muss sowohl anlassbezogen als auch in Stichproben erfolgen können. Hierzu muss eine Vorgehensweise unter Einbeziehung des behördlichen/betrieblichen Datenschutzbeauftragten und der Mitarbeitervertretung festgelegt werden (Teil I, Tz. 38).	B	muss
7.5	Es müssen Mechanismen vorhanden sein, mit denen Zugriffe orientiert an der Kategorie der Daten bzw. anhand der genutzten Funktionen differenziert protokolliert werden können. Der Umfang der Protokollierung korrespondiert dabei mit den bestehenden Zugriffsregelungen. Bei hinreichend fein differenziertem Zugriffsschutz kann eine Protokollierung reduziert werden; umgekehrt steigt ihre Bedeutung in den Bereichen mit weit gefassten (Abfrage-) Berechtigungen (Teil I, Tz. 37).	HB	muss
7.6	Die Protokollierung sollte auf der Ebene der Anwendungsfunktionen erfolgen, um eine an der fachlichen Verfahrenslogik bzw. den jeweiligen Geschäftsprozessen orientierte Nachvollziehbarkeit zu ermöglichen. Eine Protokollierung auf Datenbankebene oder eine technische Protokollierung ohne Bezug zum sachlichen Zusammenhang eines Zugriffs trägt dem nicht	H	sollte

Rechnung.

7.7	Protokollfunktionen müssen revisionssicher ausgestaltet sein, d.h., vorgesehene Protokollierungen dürfen nicht umgangen werden können und eine nachträgliche Veränderung von Protokolldaten darf nicht möglich sein, z.B. durch Speicherung der Daten auf WORM-Medien, ein Vier-Augen-Prinzip beim Zugriff auf Protokolldaten oder deren kryptografische Absicherung (Teil I, Tz. 32,37).	H	muss
7.8	Die Protokollierung eines Anwenderzugriffs muss mindestens folgende Angaben umfassen: - Zeitpunkt eines Zugriffs, - Kennung des jeweiligen Benutzers, - Kennung der jeweiligen Arbeitsstation, - aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung), - betroffener Patient/Behandlungsfall Bei Aufruf einer Suchfunktion muss das Protokoll mindestens die folgenden Angaben enthalten - verwendete Such- bzw. Abfragekriterien (z.B. Patientennummer, Fallnummer, Name, Geburtsdatum, Wohnort, Diagnose etc.), - Ergebnis der Abfrage (z.B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske), - etwaige Folgeaktionen bzw. Navigationsschritte (z.B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport); (Teil I Tz. 25, 37)	H	muss
7.9	Bei der Protokollierung muss zwischen Zugriffen, die aus der fachlichen Nutzung des Verfahrens resultieren (Zugriffe durch ärztliche Mitarbeiter, Pflege-, Verwaltungs-, Ausbildungs- oder externe Kräfte) und administrativen Zugriffen im Rahmen des System- und Verfahrensbetriebs (Zugriffe durch administrative Mitarbeiter) differenziert werden (Teil I Tz. 32, 37).	H	muss
7.10	Ist für die Ausführung einer Transaktion die Eingabe einer besonderen Begründung vorgesehen (vgl. 4.9), muss diese Transaktion und ein (vorzugsweise automatisiert nachverfolgbarer) Verweis auf die eingegebene Begründung von der Protokollierung erfasst werden Teil I, Tz. 16, 37).	H	muss
7.11	Protokolle sollen so konfigurierbar sein, dass sie keine medizinischen Daten enthalten,. Nachweise über Datenwerte vor bzw. nach einer Änderung sollen in der Anwendung selbst, nicht in den Datenschutzprotokollen vorgehalten werden.	HB	soll
7.12	Das Rollen- und Berechtigungskonzept muss es erlauben, den Zugriff auf	H	muss

	Protokolldaten zu beschränken. Zur Wahrung der Vertraulichkeit, Integrität und Authentizität der Protokolldaten sollen geeignete kryptografische Verfahren nach dem Stand der Technik eingesetzt werden können. Beispiele hierfür sind hybride Verschlüsselungsverfahren, bei denen der Entschlüsselungsschlüssel in einer geschützten Hardware gespeichert wird, und die Nutzung eines Zeitstempeldienstes.		soll
7.13	Der Zugriff auf Protokolle muss separat berechtigt werden können. Es sollte möglich sein, das Vier-Augen-Prinzip durchzusetzen. „Zugriffe der IT-Administration auf Protokolldaten sind nur zweckgebunden für einer nachträgliche Kontrolle und ausschließlich als lesende Zugriffe zulässig. Sie sollen im Wege des Privileged Account Managements nach dem Vier-Augen-Prinzip nur mit einem Datenschutzverantwortlichen erfolgen.	B	muss sollte
7.14	Notfallzugriffe müssen mit der Angabe zu Benutzer, Fall-/Patientenummer, Zeitpunkt des Notzugriffs und Zugriffsgrund revisionssicher protokolliert werden, auch wenn der Zugriff in diesem Kontext abgebrochen wurde. Auf die Erweiterung der Zugriffsrechte und die Protokollierung ist vor der Gewährung des Zugriffs hinzuweisen (Teil I Tz. 16).	B	muss
7.15	Zugriffe auf gesperrte Daten müssen protokolliert werden. Dies gilt insbesondere für Zugriffe im Zuge der administrativen Aufnahme, welche nicht zur Entsperrung der Patientenakte der aufgerufenen Person durch Neuaufnahme geführt haben. Ein Entsperren der Daten darf nur nach einem festgelegten Verfahren erfolgen.	B	muss
7.16	Der konkrete Umfang der Protokollierung muss im Rahmen der Grundkonfiguration des Verfahrens mit dem behördlichen/betrieblichen Datenschutzbeauftragten des Krankenhauses abgestimmt werden.	B	muss
7.17	Neben der Anmeldung am Verfahren (Login/Logout) müssen insbesondere Aufrufe von Transaktionen bzw. Reports zu folgenden Datenkategorien protokolliert werden : - Datensätze besonderer Personengruppen (z.B. Mitarbeiterdaten, VIPs), soweit besonders gekennzeichnet, - Daten außerhalb des primären Zuständigkeitsbereichs des Benutzers, - abgeschlossene Fälle, - Rückweisungen aufgrund fehlender Berechtigungen, - Datenexporte; (Teil I Tz. 25, 37).	B	muss
7.18	Die Löschung von Daten ist Teil ändernder Zugriffe. Sie sollte lediglich insoweit protokolliert werden, als für einzelne Daten der Zeitpunkt der Löschung und der jeweilige Benutzer, für Datensätze zusätzlich die jeweilige Fallnummer oder vergleichbare Identifikationsmerkmale festgehalten werden.	B	sollte
7.19	Es müssen geeignete Mechanismen zur Verfügung stehen, um die	H	muss

Protokolldaten auswerten zu können.

Hierzu sollten bereits im Verfahren selbst Auswertungsmöglichkeiten vorgesehen werden, die eine schnelle Selektion prüfungsrelevanter Datensätze nach folgenden Gesichtspunkten erlauben: sollte

- Verarbeitungskontext
- Begründungspflicht für die Transaktion (vgl. 4.9)
- Benutzerkennung,
- Arbeitsstation,
- Funktionen/Transaktionen,
- Suchkriterien,
- Patientennummer / Fallnummer,
- Zeitraum.

(Teil I Tz. 38).

.

7.20 Es muss eine Auswertung möglich sein, welche Benutzer wann mit welchen Rechten eingerichtet worden sind. H muss

7.21 Struktur und Format der Protokolldaten müssen es ermöglichen, dass bei Bedarf auch flexible Auswertungen erfolgen können. Die Protokolldaten sollten daher in ein durch gängige Analysewerkzeuge oder Datenbankfunktionen auswertbaren Format überführt werden können (z.B. CSV-Format mit geeigneten Trennzeichen, je Protokolleintrag eine Zeile). Eine solche Umwandlung muss den Zugriffsbegrenzungen nach Tz. 7.12 unterliegen. Nach Abschluss der Auswertung sind die umgewandelten Protokolldaten zu löschen. Im Interesse der zeitlichen Eingrenzbarkeit und der leichteren Steuerung von Aufbewahrungsfristen sollte möglichst eine tages- oder monatsbezogene Speicherung erfolgen. H muss

7.22 Für eine vorbeugende Datenschutzkontrolle sollen die Protokolle auf bestimmte Auffälligkeiten hin, wie die Häufung von Abfragen bestimmter Benutzerkennungen, eine Häufung von Abfragen außerhalb der Dienstzeiten, unübliche Suchkriterien oder kritische Transaktionen (Zugriffe auf Akten behandelter Kollegen, VIPs) ausgewertet werden können (Teil I Tz. 38). Hierfür sind geeignete Auswertungsfunktionen vorzusehen.
Krankenhäuser müssen die vorbeugende Datenschutzkontrolle in ihrem Protokollierungskonzept berücksichtigen, und datenschutzrechtliche Auffälligkeits- und Stichprobenauswertungen vorsehen, zumindest insoweit, wie das Berechtigungskonzept unberechtigte Zugriffe nicht ausschließt. Eine (teil-)automatisierte Protokollauswertung mit Benachrichtigungsfunktion sollte ermöglicht werden. HB soll

7.23	Im Rahmen der Zugriffskontrolle muss gewährleistet sein, dass eine Einsichtnahme nur den Personen möglich ist, in deren Aufgabenbereich Auswertungen von Protokolldaten fallen.	B	muss
7.24	Die Aufbewahrungsdauer für Protokolldaten aus der Verfahrensnutzung muss so bemessen sein, dass Zugriffe die im Zeitraum der Behandlung erfolgt sind, nachvollzogen werden können. Sie soll im Regelfall bei zwölf Monaten liegen.	B	muss
7.25	Für Protokolldaten, die nicht im unmittelbaren Zugriff stehen müssen, sollte über ein Archivierungskonzept eine Auslagerung vorgesehen werden.	HB	sollte

8 Technischer Betrieb, Administration

8.1	Die Administration eines KIS muss in die Bereiche - technische Administration der genutzten IT-Komponenten, - Anwendungsadministration / Verfahrensbetreuung und - Berechtigungsverwaltung	B	muss
	Getrennt werden. Die jeweiligen Rollen sollen unterschiedlichen Personen zugewiesen werden(Teil I TZ. 2).	B	soll
8.2	Das Krankenhaus muss sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann (Teil I, Tz. 33).	B	muss
	Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 33).	H	soll
8.3	Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können (Teil I, Tz. 33).	H	muss
8.4	Fernwartungsarbeiten müssen über verschlüsselte Verbindungen und unter separaten, über Identifikations- und Authentisierungsmechanismen geschützten Benutzerkennungen durchgeführt werden. Deren Zugriffsmöglichkeiten müssen auf das für die Durchführung der Wartungsarbeiten erforderliche Maß beschränkt sein; erforderlichenfalls sind mehrere Wartungskennungen einzurichten (Teil I, Tz. 33).	B	muss
8.5	Es muss nachvollziehbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt wurden, insbesondere welche Zugriffe auf personenbezogene Daten erfolgt sind (Teil I, Tz., 33,37).	H	muss
	Hierzu müssen die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festgehalten und für die Dauer eines Jahres aufbewahrt werden.	B	muss
8.6	Die Übernahme neuer Softwareversionen sollte grundsätzlich nicht im Rahmen der Fernwartung erfolgen. Soweit im Einzelfall unvermeidlich, ist dies zu dokumentieren und die Integrität der übernommenen Software durch geeignete Maßnahmen sicherzustellen (Teil I, Tz.33).	B	sollte
8.7	Das Krankenhaus soll eine transparent kryptografisch verschlüsselte Datenhaltung einsetzen, um um die Kenntnisnahme der Identität von Patienten und ihrer medizinischen Daten im Zuge der Systemadministration oder des technischen Betriebs zu erschweren und eine Offenbarung bei einem Datenträgeraustausch auszuschließen.	HB	soll

8.8	Die im Rahmen des Betriebs des KIS notwendigen technischen und organisatorischen Maßnahmen des Datenschutzes sollen auf der Grundlage einer Schutzbedarfs- und Risikoanalyse in einem Datenschutzkonzept, soweit sie die Informationssicherheit betreffen, auf der Grundlage der IT-Grundschutzstandards 100-1 bis 100-4 des BSI im Informationssicherheitskonzept, festgelegt werden.	B	soll
8.9	Aufgrund der Reichweite administrativer Funktionen bedarf ihre Nutzung einer besonderen Kontrolle. Die Protokollierung von Zugriffen im Rahmen der technischen und fachlichen Verfahrensbetreuung muss alle Zugriffe erfassen, die Auswirkungen auf Art oder Umfang der Verarbeitung personenbezogener Daten haben, insbesondere: - Maßnahmen der Installation / Deinstallation von Software, - Änderungen der Anwendungskonfiguration (z.B. Festlegen von Residenzzeiten / Löschfristen, Login-Parametern, Anzeigeparametern, usw.), - Zugriffe im Rahmen einer etwaigen Mandantenverwaltung, - die Anlage, Änderung und Löschung von Rollen, - die Vergabe, Änderung und Löschung von Berechtigungen, - die Administration von Benutzern (Anlage, Sperre, Löschung, Rollenzuweisung), - die Einrichtung / Änderung standardmäßig vorgegebener Auswertungs-möglichkeiten (Reports), - der Import / Export von Datenbeständen, - Datenübermittlungen, - Prozesse zur Aggregierung, Pseudonymisierung / Anonymisierung von Datenbeständen (Date Warehouse), - Archivierungen / Datensicherungen; (Teil I Tz. 32, 37)	HB	muss
8.10	Daten aus der Protokollierung administrativer Zugriffe sind, soweit sie Konfigurationsänderungen und Datenübermittlungen betreffen als Teil der Verfahrensdokumentation anzusehen. Hier müssen längere Aufbewahrungs-fristen als unter Tz. 7.24 genannt, orientiert an der Dauer des Einsatzes eines Verfahrens vorgesehen werden.	B	muss