GMDS - Deutsche Gesellschaft für Medizinische Informatik,
Biometrie und Epidemiologie e.V.
Industriestraße 154
D-**50996** Köln

Tel.: +49 (2236) 3319958
Fax: +49 (2236) 3319959
Email: info@gmds.de
http://www.gmds.de

Vereinsregister: VR 16225 Amtsgericht Köln

Umsatzsteuer-Identifikationsnummer:
27.07.02 DE 182645846

Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“ (DGI) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)

Synopse

„Orientierungshilfe Krankenhausinformationssysteme“[1]

Vergleich 2. Fassung, Stand März 2014, mit der 1. Fassung (Stand März 2011)

Autor: Dr. Bernd Schütze

[1] herausgegeben von den Arbeitskreisen „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Das Originaldokument der OH KIS steht zum Download bei den Datenschutzaufsichtsbehörden des Bundes, der Länder und der Kirchen zur Verfügung, z. B. unter der URL http://www.datenschutz-berlin.de/attachments/771/Orientierungshilfe_Krankenhausinformationssysteme.pdf
Der Text der OH kann unter den gleichen Bedingungen (textlich unveränderte Übernahme, Angabe zu Urheberschaft und Fundstelle des Originaldokuments) verwendet werden.

Haftungsausschluss / Copyright

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde vom Autor mit größter Sorgfalt zusammengestellt. Der Autor ist kein Jurist. Insofern kann und darf er keine rechtsverbindlichen Auskünfte geben. Daher ist diese Ausarbeitung nur als Standpunkt des Autors aufzufassen. Eine Haftung für die Angaben übernimmt der Autor nicht. In diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen von der Organisation/Institution/Firma an Hand der jeweiligen Situation und der für sie geltenden Normen und Vorschriften geprüft und angepasst werden.

Der Autor ist bestrebt, in allen Publikationen die Urheberrechte der verwendeten Grafiken, Tondokumente, Videosequenzen und Texte zu beachten, von ihm selbst erstellte Grafiken, Tondokumente, Videosequenzen und Texte zu nutzen oder auf lizenzfreie Grafiken, Tondokumente, Videosequenzen und Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt:

Dieses Werk ist unter einer Creative Commons-Lizenz (3.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:

- das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen
- Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anfertigen

Zu den folgenden Bedingungen:

- **Namensnennung**. Sie müssen den Namen des Autors/Rechteinhabers nennen, wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt
- **Keine kommerzielle Nutzung**. Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.
- **Weitergabe unter gleichen Bedingungen**. Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die daraufhin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

Im Weiteren gilt:

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

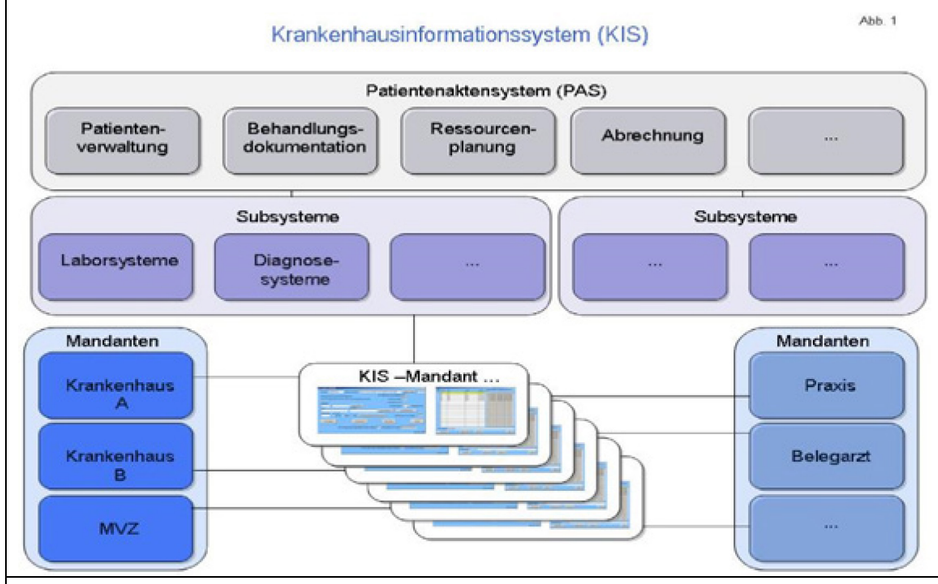
Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

http://creativecommons.org/licenses/by-nc-sa/3.0/de/

Düsseldorf, 05. April 2014

Glossar

OH Kis Version 1.0	OH Kis Version 2.0
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.	**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.	**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.	**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.~~	**Behandlungsfall** Eine *medizinische Behandlung* umfasst alle Anamnese-, Diagnose-, Therapie- und Nachbehandlungsmaßnahmen zu derselben Krankheit, Verdachtsdiagnose oder Symptomatik, wegen der der Patient stationär aufgenommen wurde. Medizinisch kann eine Behandlung aus mehreren ambulanten und stationären Behandlungsfällen bestehen und über Jahrzehnte andauern (chronische Krankheiten). Unter *Behandlungsfall* ist bei einer stationären Behandlung die gesamte Behandlung derselben Erkrankung zu verstehen, die ein Patient in einem Krankenhaus von der stationären Aufnahme bis zur Entlassung aus der stationären Behandlung erhält. Eingeschlossen sind die dem Behandlungsfall zuzuordnenden vor- und nachstationären Behandlungen I. S. v. § 115 a SGB V, sowie Wiederaufnahmen innerhalb der oberen Grenzverweildauer i. S. v. § 8 Abs. 5 Krankenhaus-Entgeltgesetz (KHEntG).
Elektronische Patientendaten Elektronische Patientendaten sind alle in einem →*Krankenhausinformationssystem (KIS)* erfassten und gespeicherten administrativen und klinischen Daten eines Patienten.	**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*.	**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	**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

OH Kis Version 1.0	OH Kis Version 2.0
Krankenhausmitarbeiter können mehreren funktionsbezogenen Organisationseinheiten zugeordnet sein.	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.	## Identifikationsdaten Unter Identifikationsdaten fallen insbesondere folgende Daten: Vor- und Zuname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht, Titel, Anschrift, Krankenversichertennummer, Patienten-ID.
	## Konsil/Konsiliardienst Konsil ist die patientenbezogene Beratung des behandelnden Arztes durch einen anderen Arzt. Konsiliardienst ist das in einem Krankenhaus bestehende Angebot zur Beurteilung und Mitbetreuung von Patienten, das von den behandelnden Ärzten für deren Patienten angefordert werden kann.
## 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.	## 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. Abb. 1 Krankenhausinformationssystem (KIS)  	## 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

OH Kis Version 1.0	OH Kis Version 2.0
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*.	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.~~	## Mandantenfähigkeit Der abgeschlossene Datenhaltungs- und Verarbeitungszusammenhang einer im datenschutzrechtlichen Sinne verantwortlichen Stelle wird in diesem Papier nachfolgend als "Mandant" bezeichnet, die getrennte Speicherung und Verarbeitung als "Mandantentrennung". Ein Verfahren ist "mandantenfähig", wenn Patientendaten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. (s. Orientierungshilfe Mandantenfähigkeit des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2012).
## 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~~.	## Mitbehandlung Als Mitbehandlung stellen sich alle vom behandelnden Arzt veranlassten Leistungen Dritter zur medizinischen Versorgung des Patienten dar.
## Patientenakte Die Gesamtheit aller zu einem Patienten bei einem Krankenhaus gespeicherten Verwaltungs- und Behandlungsdaten.	## 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.	## 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*.	## 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.	## 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.

OH Kis Version 1.0	OH Kis Version 2.0
Die Verwendung von →*Aliasen* und →temporären Patientenkennzeichen stellt eine technisch-organisatorische Maßnahme zum Schutz der Betroffenen dar, die von einer Pseudonymisierung abzugrenzen ist.	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.	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.
	Sonderzugriff Sonderzugriffsrechte sollen dringende, zum sofortigen medizinischen Eingreifen erforderliche, jedoch anders nicht erfüllbare Informationsbedarfe befriedigen. Sie gehen über die beschränkte Rollen- und Aufgaben-bezogene Berechtigung zum Zugriff auf Patientendaten hinaus.
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.	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.	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.	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“.	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.	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.

Teil 1

OH Kis Version 1.0	OH Kis Version 2.0
~~Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientenakten im Krankenhaus~~	**Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen** Bei der Aufnahme eines Patienten in das Krankenhaus spielen sowohl administrative als auch medizinische Belange eine Rolle. Abfolge und handelnde Beschäftigten unterscheiden sich von Krankenhaus zu Krankenhaus und je nachdem, ob es sich um eine geplante oder eine Notfallaufnahme handelt. In jedem Fall gilt: Der Umfang der Daten, welche die Beschäftigten jeweils aufnehmen dürfen, richtet sich nach den ihnen zugewiesenen Aufgaben. Der folgende Abschnitt verdeutlicht diese Einschränkung auf das Erforderliche für Beschäftigte, deren Wirkungskreis sich auf die administrativen Belange beschränkt.
Aufnahme	**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.~~	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) und in der Trefferliste neben Identifikationsdaten auch der Zeitraum des letzten stationären Aufenthalts angezeigt 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.	2. Die Offenbarung einer vorbehandelnden funktionsbezogenen Organisationseinheit ist bei der administrativen Aufnahme nur dann zulässig, wenn die Behandlung durch Ärzte dieser Organisationseinheit medizinisch noch nicht abgeschlossen ist. 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.	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.	4. 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 Auskunftsstellen kein Treffer angezeigt wird. Bei anderen Stellen — insbesondere auf der jeweiligen Station — muss der Umstand der Auskunftssperre erkennbar werden.

OH Kis Version 1.0	OH Kis Version 2.0
~~**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.	5. 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	**Behandlung**
9. Jede an der Behandlung und Verwaltung eines Patienten direkt beteiligte Person darf auf die Identifikationsdaten des Patienten zugreifen.	6. 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.	7. Der Zugriff auf die medizinischen und Pflege-Daten ist nach seiner Erforderlichkeit für die persönliche Aufgabenerfüllung der Beschäftigten auszudifferenzieren. Kriterien zur Differenzierung sind zumindest die Stellung der Beschäftigten im Krankenhaus und die ihnen 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.
	8. Der Zugriff auf Vorbehandlungsdaten ist nur soweit zulässig, wie das Landeskrankenhausrecht dies gestattet. Ein Widerspruch des Patienten gegen diesen Zugriff ist zu berücksichtigen.
Zugriffe durch Ärzte Soweit im Folgenden auf Ärzte Bezug genommen wird, gelten die Regelungen auch für Psychotherapeuten.	**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.	9. 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 (ggf. interdisziplinär besetzten) 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.	10. 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.	11. 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 Daten des Patienten. Die Ärzte der abgebenden OE können die Zugriffsmöglichkeit auf die Fallakte behalten. Sie dürfen diese Möglichkeit nutzen, soweit dies zur Aufgabenerfüllung (einschließlich der Sicherung der Qualität der

OH Kis Version 1.0	OH Kis Version 2.0
	eigenen Behandlung) 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.	12. 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 soweit zur Aufgabenerfüllung (einschließlich der Sicherung der Qualität der eigenen Behandlung) erforderlich 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~~.	13. Konsilanforderungen dürfen den Datenzugriff nur in Bezug auf den betroffenen Patienten eröffnen. Die Anforderung kann einzelne Ärzte oder eine Gruppe von spezialisierten Konsiliarärzten berechtigen. Sie ist auf die Daten zu beschränken, die für die Festlegung der Konsiliarleistung erforderlich ist. Der durch die Konsilanforderung eröffnete Datenzugriff ist zu befristen. Konsilärzte sind darüber hinaus berechtigt, auch nach Ende des Patientenkontakts soweit zur Aufgabenerfüllung (einschließlich der Sicherung der Qualität der eigenen Behandlung) erforderlich auf die Dokumentation der eigenen Leistungen und der mit ihnen zusammenhängenden medizinischen Daten zuzugreifen.
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.	14. Ein darüber hinaus gehender Sonderzugriff 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.	15. Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten. Für die konkret an der Behandlung beteiligten Beschäftigten eines Beleg-Krankenhauses gelten die Tz. 6 ff.
Zugriffe durch ~~Pflegepersonal~~	**Zugriffe durch den pflegerischen Stationsdienst**
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.	16. 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.	17. Die Berechtigung ergibt sich bei wechselnder Zuordnung zu Organisationseinheiten (Springer) aus der dokumentierten Zuweisung zu einer OE durch die zuständige Stelle, 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.~~	18. 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.
~~Fachübergreifende~~ Zugriffe	**Zugriffe außerhalb der bettenführenden Fachabteilungen**
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	19. Beschäftigte des Krankenhauses 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

OH Kis Version 1.0	OH Kis Version 2.0
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.	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 Beschäftigten kann ein Zugriff auf sämtliche Daten der jeweiligen Patienten zulässig sein.
	20. Der Schreibdienst sollte so organisiert sein, dass der Zugriff durch individuelle Zuweisung zeitlich beschränkt erfolgt. Sofern dies nicht möglich ist, muss zumindest sichergestellt sein, dass die einzelnen Schreibkräfte jeweils nur einer bestimmten Funktionseinheit mit entsprechenden Zugriffsrechten zugeordnet sind.
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.~~	21. Das (Zentral-)Labor bzw. deren diensthabende / handelnde Beschäftigte dürfen mit der Leistungsanforderung nur einen Zugriff auf die für die Befundung erforderlichen Daten des im Auftrag benannten betroffenen Patienten erhalten.
~~Nach der Behandlung~~	Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls
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.~~	22. Nach Abschluss des Behandlungsfalles und Abwicklung der ihn betreffenden medizinischen und verwaltungsmäßigen Routinevorgänge sind die für Zwecke der unmittelbaren Behandlung und deren Abrechnung eingerichteten Zugriffsmöglichkeiten nicht mehr erforderlich und daher einzuschränken. Zur Erfüllung anderer, festgelegter Aufgaben kann der Zugriff für einen organisatorisch festgelegten Personenkreis bestehen bleiben.
~~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.	23. 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.
	24. Diese Zugriffsbeschränkung hat als technisch-organisatorische Maßnahme unabhängig davon zu erfolgen, ob und wann nach datenschutzrechtlichen Vorschriften eine Sperrung der Daten vorzunehmen ist.
	25. Das Krankenhaus hat eine angemessene Frist (nicht länger als ein Jahr) nach Abschluss des Behandlungsfalls entsprechend den jeweiligen organisatorischen Abläufen im Krankenhaus festzulegen, innerhalb derer die Einschränkung der Zugriffsmöglichkeiten spätestens zu erfolgen hat.
	26. Wird ein Patient nach Wirksamwerden der Zugriffsbeschränkung erneut behandelt, darf die Beschränkung des Zugriffs auf Daten aus früheren Behandlungsfällen aufgehoben werden. Der Zugriff auf Vorbehandlungsdaten ist nur soweit zulässig, wie das Landeskrankenhausrecht dies gestattet.
	Löschung
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.	27. 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~~	Zugriffe für Abrechnung' Controlling' Qualitätssicherung und Ausbildung

OH Kis Version 1.0	OH Kis Version 2.0
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. Die Krankenhausverwaltung / Abrechnungsabteilung darf nur Zugriff auf die für sie erforderlichen Patientendaten (Stammdaten, Diagnosen, Leistungen usw.) haben.
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.	29. Soweit zur internen Qualitätssicherung oder beim Controlling der Zugriff durch die an der Qualitätssicherung oder dem Controlling beteiligten Beschäftigten auf alle Daten eines Patienten zugelassen werden muss, ist durch Zuständigkeits- und Funktionsaufteilungen, zeitliche Beschränkungen oder sonstige geeignete technisch-organisatorische Maßnahmen ein ständiger Vollzugriff auf alle Daten aller Krankenhauspatienten zu vermeiden.
	30. Soweit nicht erforderlich (z. B. für das Geschäftsprozessmanagement, das strategische Controlling und die betriebswirtschaftliche Steuerung des Krankenhauses) 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.	31. 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.
	Verarbeitung durch verschiedene Leistungserbringer
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.	32. Patienten, die in anderen Krankenhäusern oder Einrichtungen des Trägers des Krankenhauses (z.B. in Medizinische Versorgungszentren gleich welcher Rechtsform) behandelt werden, werden dadurch nicht zugleich Patienten des Krankenhauses. Sie dürfen daher nur in den Patientenbestand der tatsächlich behandelnden Einrichtung aufgenommen werden. Ein gemeinsames (Krankenhaus und andere Einrichtung 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.	33. Einrichtungs- und insbesondere mandantenübergreifende Zugriffe stellen datenschutzrechtlich Übermittlungen dar, deren Zulässigkeit sich nach Arzt- und Datenschutzrecht richtet. Beispiele für die zulässige Ausgestaltung derartiger Übermittlungen sind in einem Szenarienkatalog ausgeführt, der ergänzend zu der vorliegenden Orientierungshilfe von der federführenden Unterarbeitsgruppe bereitgestellt wird.
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.	34. Eine Person kann mehreren Mandanten als Beschäftigter 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.	35. 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.	36. 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.
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.~~	37. Ambulant in Nebentätigkeit behandelte Privatpatienten sind grundsätzlich nicht Patienten des Krankenhauses, sondern der insoweit berechtigten Ärzte. Für Behandlungsakten von ambulant in Nebentätigkeit behandelten Privatpatienten hat der Arzt die alleinige datenschutzrechtliche Verantwortung.

OH Kis Version 1.0	OH Kis Version 2.0
Technische Administration	**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.	38. 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.	39. Die Aktivitäten der Administratoren sind 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.	40. 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	**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.	41. Beschäftigte des Krankenhauses 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.	42. Für Patienten, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, gilt grundsätzlich dasselbe. Die Festlegung trifft die Klinikleitung auf Antrag des Patienten.
Zugriffsprotokollierung und Datenschutzkontrolle	**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.	43. Aufgrund von Art und Umfang der in einem Krankenhausinformationssystem 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.	44. 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~~).	45. Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle ist ebenso Aufgabe des Krankenhauses wie eine Kontrolle aus konkretem Anlass (s.Tz. 40). Aufnahmevorgänge, die nicht mit einer abrechnungsfähigen Behandlung in Verbindung stehen, müssen kontrolliert werden.
Auskunftsrechte des Patienten	**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.	46. Der Patient muss die Möglichkeit erhalten, Auskunft über und Einsicht in alle zu seiner Person gespeicherten Daten zu bekommen, soweit keine erheblichen therapeutischen Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. 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 je nach Wunsch des Patienten auch durch einen Ausdruck oder in elektronischer Form erfolgen.

OH Kis Version 1.0	OH Kis Version 2.0
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 X~~Y~~, Ärzte der Fachabteilung ~~XY~~).	47. Bei einem besonderen berechtigten Interesse, z.B. bei einem Datenmissbrauchsverdacht, umfasst das Auskunftsrecht auch die Information, wer zu welchem Zeitpunkt welche Daten zur Kenntnis genommen hat. Werden die lesenden Zugriffe zulässigerweise (vgl- Teil II, Tz. 7.5) 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 X, Ärzte der Fachabteilung A).
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.	48. 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 Beschäftigte. Die Berechtigung zur Auskunftserteilung mit Zugriff auf die gesamte Patientenakte muss auf einen möglichst engen Personenkreis beschränkt werden.

Teil 2

OH Kis Version 1.0	OH Kis Version 2.0
Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen	**Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen**
I. Vorbemerkung II. Technische Anforderungen ~~an Gestaltung und Betrieb von Krankenhausinformationssysteme~~ 1. Datenmodell 2. Systemfunktionen 3. Anwendungsfunktionen 4. Rollen- und Berechtigungskonzept 5. Datenpräsentation 6. ~~Nutzungsergonomie~~ 7. Protokollierung 8. Technischer Betrieb, Administration	**I.** Vorbemerkung **II.** Technische Anforderungen **1.** Datenmodell **2.** Systemfunktionen **3.** Anwendungsfunktionen **4.** Rollen- und Berechtigungskonzept **5.** Datenpräsentation **6.** Systemzugang **7.** Protokollierung **8.** Technischer Betrieb, Administration
I. Vorbemerkung	**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~~.	Das vorliegende Papier ist der zweite Teil der „Orientierungshilfe Krankenhausinformationssysteme" der Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen 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 „Rechtlichen Rahmenbedingungen" für den Einsatz von Krankenhausinformationssystemen Bezug und geben Hinweise zu einer datenschutzkonformen Gestaltung und einem datenschutzgerechten Betrieb dieser Systeme.
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.[2] Dabei kann es sich sowohl um eine integrierte Gesamtlösung als auch einen Verbund selbstständiger 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.	Unter dem Begriff „Krankenhausinformationssystem (KIS)" wird im Folgenden die Gesamtheit aller zur Verwaltung und Dokumentation von elektronischen Patientendaten eingesetzten informationstechnischen Systeme eines Krankenhauses verstanden. Dieses Papier nimmt dabei in erster Linie die zentralen, elektronische Patientenakten führenden Systeme in den Blick, hier Patientenaktensystem (PAS) genannt.[31] Dabei kann es sich sowohl um eine integrierte Gesamtlösung als auch einen Verbund selbstständiger 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[4] übernommen, soweit	Bei den Anforderungen wird soweit möglich auf die entsprechenden Textziffern des Teils I 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; auf die jeweils relevanten Kontrollen bzw. Schutzziele wird in diesem Fall verwiesen. Hinsichtlich der Protokollierung (Kapitel 7) wurden die Empfehlungen der Konferenz der

[2] Gebräuchlich ist die Bezeichnung einrichtungsinterne elektronische Patientenakte, der Begriff Patientenakte wird in diesem Text jedoch für die Akte eines einzelnen Patienten verwendet
[3] Gebräuchlich ist die Bezeichnung einrichtungsinterne elektronische Patientenakte, der Begriff Patientenakte wird in diesem Text jedoch für die Akte eines einzelnen Patienten verwendet
[4] http://www.datenschutz.rlp.de/downloads/oh/dsb_oh_protokollierung_gkv.pdf

OH Kis Version 1.0	OH Kis Version 2.0
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.	Datenschutzbeauftragten des Bundes und der Länder zur Protokollierung in zentralen Verfahren der Gesetzlichen Krankenversicherung[5] 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.	Soweit konkrete Vorgaben zur Gestaltung oder Konfiguration gemacht werden, sind diese als musterhafte Umsetzungen zu verstehen, die aus den Erfahrungen der Kontroll- und Beratungspraxis der Datenschutzbeauftragten abgeleitet wurden. Anstelle der dargestellten Mechanismen kommen jedoch auch andere Lösungen in Betracht, wenn mit ihnen im Ergebnis das gleiche Schutzziel erreicht wird.
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.	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.	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).	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.	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 zwingenden Anforderungen an Konfiguration und Nutzung des KIS durch den Betreiber ist ein datenschutzkonformer Betrieb des 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.~~	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.
	Der Erstellung der ersten wie auch der hier vorgelegten, überarbeiteten Fassung ist ein konstruktiver Dialog mit Krankenhausbetreibern, Anbietern von KIS-Lösungen und Krankenhausgesellschaften vorausgegangen. Stets wurde dabei betont, dass die in der Orientierungshilfe beschriebenen Anforderungen nicht Ausdruck eines Misstrauens sind oder einem Generalverdacht gegenüber den im Krankenhaus Tätigen entspringen, sondern auf den Krankenhausbereich bezogene Konkretisierungen bestehender datenschutzrechtlicher Regelungen für den Einsatz der Informationstechnik darstellen, die zu einem vertrauensvollen Verhältnis zwischen Patienten und

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

OH Kis Version 1.0		OH Kis Version 2.0	
		Krankenhausbeschäftigten beitragen.	
		Anregungen und Kritik seitens der Hersteller und Betreiber von Krankenhausinformationssystemen sind in die vorliegende Fassung der Orientierungshilfe eingeflossen. Auf die ergänzenden „Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme", welche von der Deutschen Krankenhausgesellschaft herausgegeben wurden, wird in diesem Zusammenhang ausdrücklich hingewiesen.	
II. Technische Anforderungen		**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 Struktur der Daten im PAS** Der folgende Abschnitt enthält Anforderungen an die Datengrundlage eines PAS. Eine geeignete Struktur dieser Daten ist erforderlich, um zum einen eine Trennung der Daten nach Verarbeitungszwecken zu ermöglichen und zum anderen Anknüpfungspunkte für ein angemessenes Konzept für die Regelung der Zugriffe auf die Daten zu bieten. Die Datenbasis eines PAS besteht aus Datenobjekten, die inhaltlich zusammengehörige Daten je nach der softwaretechnischen Gestaltung der Anwendung aufnehmen. Beispiele für solche Datenobjekte sind Einzelbefunde, Einträge in die Pflegedokumentation, Einträge in die Liste der abrechenbaren Leistungen. 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 sind die Datenobjekte mit Metadaten verknüpft, 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, das in einem Umfeld eingesetzt wird, in dem es von mehreren rechtlich selbstständigen Leistungserbringern genutzt werden soll, muss mandantenfähig sein. (Teil I, Tz. 32).	H Muss
1.1 ~~Jedes PAS muss mandantenfähig sein (Teil I Tz. 17,30,36).~~ 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). ~~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.~~	~~H muss~~ B muss ~~B muss~~	1.2 Verwenden verschiedene Krankenhäuser dieselbe Installation eines PAS, sind darin separate Mandanten einzurichten. Gleiches gilt für die Nutzung derselben Installation eines PAS durch ein Krankenhaus gemeinsam mit einer weiteren rechtlich selbständigen Stelle, insbesondere einem Medizinischen Versorgungszentrum (Teil I, Tz. 32).	B Muss
		1.3 1.3 Datenbestände verschiedener Mandanten sind logisch oder physisch so zu trennen, dass Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Für weitere Komponenten eines KIS gilt, soweit relevant, diese Anforderung analog. (Teil I, Tz. 32) Anforderungen an die Ausgestaltung mandantenfähiger Systeme sind im Übrigen in der Orientierungshilfe zur Mandantenfähigkeit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2012 in der jeweils aktuellen Fassung niedergelegt.	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	1.4 1.4 Jedes Datenobjekt, das sich auf einen einzelnen Patienten bezieht, ist genau einer Fallakte, in Systemen mit mehreren Mandanten jede Fallakte genau einem Mandanten zuzuordnen (Teil I, Tz. 26, 32). Aus der Fallakte muss sich ergeben, welcher leitende Arzt oder welche Ärzte für die Behandlung zu gegebenem Zeitpunkt die Verantwortung tragen (Teil I, Tz. 9).	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~~	~~B~~ muss	1.5 Für Datenobjekte, welche Patienten betreffen, die ambulant in Nebentätigkeit eines privat liquidierenden Arztes oder durch einen Belegarzt behandelt werden, muss das PAS die Möglichkeit bieten, Berechtigungen an diesen Status anknüpfen zu lassen, sofern für den	H Muss

OH Kis Version 1.0			OH Kis Version 2.0	
	~~Statuskennzeichen ausgewiesen werden~~, sofern für den behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. ~~30~~).		behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 15, 37)	
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	1.6 Die Fallakte eines Patienten muss Angaben aufnehmen können, welchen funktionsbezogenen Organisationseinheiten ein Patient derzeit zugeordnet ist. Flexible Mehrfachzuordnungen von Patienten zu Ärzten bzw. medizinischen Organisationseinheiten müssen möglich sein (Teil I, Tz. 9). Hierbei soll zwischen Behandlung und Konsil unterschieden werden können (Teil I, Tz. 10 und 13). Ziel ist es, umfassende generelle Zugriffsrechte zu vermeiden und stattdessen die im Rahmen der Behandlung erforderlichen Zugriffe abzubilden (Teil I, Tz. 7).	H Muss
1.5	Für jedes patientenbezogene ~~Datum~~ muss 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	1.7 Für jedes patientenbezogene Datenobjekt muss sich unabhängig vom Inhaltstyp bestimmen lassen, wer es wann erstellt und wer es wann wie modifiziert hat (Eingabekontrolle / Revisionsfähigkeit). 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 (Eingabekontrolle / Authentizität).	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~~.	H~~B~~ muss	1.8 PAS müssen eine Trennung von Daten in Datenobjekte erlauben, welche den in der Einleitung zu diesem Kapitel 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. Die Betreiber sollen die Einteilung der Daten nach Kategorien nutzen, um den Zugriff von Beschäftigten auf die von ihnen benötigte Datengrundlage zu begrenzen. (Teil I, Tz. 1, 6, 7, 28)	H Muss B Soll
~~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)). Welche Inhalte in einen Basisdatensatz übernommen werden, liegt in der Verantwortung des Betreibers.~~	~~H sollte 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 Berechtigungskonzept muss es ermöglichen, dass an diese Kennzeichnungen besondere Zugriffsregelungen geknüpft werden. (Teil I Tz. 2,4,23,24).~~	~~HB muss~~		
~~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. ergabe/Rücknahme des Kennzeichens sollen durch das Rollen- und Berechtigungskonzept geregelt werden (Teil I Tz. 4, 7). Das PAS soll die Möglichkeit bieten, das Widerspruchskennzeichen in Abhängigkeit vom Verarbeitungskontext bei nachfolgenden Zugriffen anzuzeigen oder zu unterdrücken.~~	~~H soll H muss B soll HB soll~~		
			1.9 Für jede Fallakte muss erkennbar sein, ob der Krankenhausaufenthalt beendet und ob der Behandlungsfall administrativ abgeschlossen ist (Teil I, Tz. 22). Fallakten müssen ein Sperrkennzeichen aufnehmen können oder das PAS eine Methode bereitstellen, mit welcher festgestellt werden kann, ob die Fallakte gesperrt ist. (Teil I, Tz. 24).	HB Muss
			1.10 Das PAS muss die Möglichkeit bieten, einen Widerspruch des Patienten gegen die Hinzuziehung von Daten aus einer Vorbehandlung wirksam umzusetzen. (Teil I, Tz. 26).	H Muss

OH Kis Version 1.0		OH Kis Version 2.0	
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 Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob für den Patienten eine Auskunftssperre gilt (Teil I, Tz. 4).	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)~~. Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden.	HB muss B muss	1.12 Fallakten sollen bei Bedarf dahingehend gekennzeichnet werden können, dass der Patient Mitarbeiter des behandelnden Krankenhauses ist bzw. dass für die Fallakte ein besonderer Schutzbedarf besteht. Die Struktur des Rollen- und Berechtigungskonzepts soll es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können. Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden. (Teil I, Tz. 41)	H Soll 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 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 besonderer Schutzbedarf besteht. Die Struktur des Rollen- und Berechtigungskonzepts muss es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können (Teil I, Tz. 42). Die Kennzeichen nach dieser Tz. und Tz. 1.12 können in einem Kennzeichen zusammengefasst werden.	HB Muss Sollte
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 Die unter Tz. 1.11 bis 1.13 genannten Merkmale 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. 7, 41, 42).	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 Warnhinweise an nichtmedizinisches Personal sollen nur aus einer abschließend festgelegten Liste ausgewählt werden können und nicht als Freitextfelder gestaltet sein (Teil I, Tz. 3, 7).	H Soll B 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	1.16 Wenn Patientendaten für allgemeine Auswertungszwecke, die keinen Patientenbezug erfordern, in eine separate Architekturkomponente übernommen werden (z. B. in ein Data Warehouse), muss eine Anonymisierung erfolgen (Teil I, Tz. 30). 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 (Teil I, Tz. 30, 31, Datensparsamkeit, Zweckbindung).	HB Muss
2 Systemfunktionen		**2 Systemfunktionen**	
2.1 Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren.	HB soll	2.1 Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren (Transparenz).	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 sollte HB muss	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 (Datensparsamkeit). Soweit eine redundante Datenhaltung unvermeidbar ist, müssen Zugriffsbeschränkungen und Löschungen in allen betroffenen Datenbeständen berücksichtigt werden (Teil I, Tz. 22, 27).	H Sollte HB Muss
2.3 In das KIS sollte ein Single-Sign-On-Dienst integrierbar sein.	H sollte	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	2.4 In einem KIS, in dem Daten für mehrere Mandanten verarbeitet werden, muss auch beim Einsatz eigenständiger Subsysteme eine Parallelführung der Mandanten möglich sein. Dies bedeutet, dass Datenübermittlungen zwischen diesen Subsystemen mandantenbezogen vorgenommen werden. (Teil I, Tz. 32, 33).	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~~	~~HB muss~~		

OH Kis Version 1.0			OH Kis Version 2.0	
	~~des Krankenhauses befinden.~~			
2.6	~~Kennzeichen~~ nach 1.~~2~~ bis 1.4 und 1.~~7~~ bis 1.1~~1~~ 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	2.6 Merkmale nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 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, Tz. 4, enthalten.) Für die Merkmale nach Tz. 1.5 und 1.9 ist dies zwingend erforderlich (Teil I, Tz. 7, 37).	H Sollte
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	2.7 Berechtigungen auf Datenobjekte und ggf. Funktionen sollten in den verschiedenen Komponenten des KIS in gleicher Weise abgebildet werden können, jedenfalls insoweit sich die Nutzermengen überschneiden.	H Sollte
~~2.8~~	~~Speichermedien, welche Daten des KIS aufnehmen, müssen eine Verschlüsselung ermöglichen (Datenträger- / Datenbank- / Dateisystemverschlüsselung). Dies gilt insbesondere für Datensicherungen und Daten, welche sich auf mobilen Systemen befinden. Das Informationssicherheitskonzept 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 muss~~ ~~B 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	2.8 Das KIS muss über Funktionen verfügen, die es ermöglichen, insgesamt eine Übersicht der zu einem Patienten im KIS gespeicherten Daten zu erzeugen (Teil I, Tz. 43 bis 45 und 47). Diese Funktionen dienen der Datenschutzkontrolle sowie der Beantwortung von Auskunftsersuchen nach § 34 BDSG bzw. den entsprechenden 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	2.9 Es muss möglich sein, zeit- und ereignisgesteuert die Zugriffsberechtigungen für abgeschlossene (1.9) Fallakten oder Teile davon einzuschränken 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 ausschließlich diese für eine Suche unter den der Zugriffsbeschränkung unterliegenden Daten vorzuhalten. In den Ergebnissen einer derartigen Suche sollen zunächst ebenfalls nur die identifizierenden Angaben erscheinen. Soweit für bestimmte Aufgaben ein Zugriff auf einen derart identifizierten Behandlungsfall erforderlich ist, sollen die darüber hinausgehenden Daten erst nach dem unter Tz. 4.9 beschriebenen Verfahren bereitgestellt werden (Teil I, Tz. 22, 23).	H Muss Soll
	Das Krankenhaus muss einen Zeitraum von unter einem Jahr festlegen, nach dem abgeschlossene Fallakten ~~gesperrt oder ausgelagert werden~~.	B muss	2.10 Das Krankenhaus muss einen Zeitraum von unter einem Jahr festlegen, nach dem der Zugriff auf abgeschlossene Fallakten gemäß Tz. 2.9 spätestens eingeschränkt wird (Teil I, Tz. 25).	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	2.11 Das PAS muss über Funktionen verfügen, die zusammengenommen sicherstellen, 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. 27).	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	2.12 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. 27).	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). Sperr- und Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Mitarbeitern eingesetzt werden.	H muss B 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). Sperr- und Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Mitarbeitern eingesetzt werden.	H Muss 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	H soll	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	H Soll

OH Kis Version 1.0		OH Kis Version 2.0	
durchzuführen.		durchzuführen. (Datensparsamkeit; Zugriffskontrolle / Vertraulichkeit)	
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~~)[6].	HB muss	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. 30, 31).[7]	HB Muss
		Verschlüsselung Eine Verschlüsselung von Daten dient dem Schutz ihrer Vertraulichkeit. Sie ist das wirksamste und oft das einzige Mittel zum Schutz von Patientendaten gegen Offenbarung an Dritte außerhalb des Krankenhauses, soweit dieses nicht die ausschließliche Kontrolle über die Daten besitzt (Tz. 2.16 und 2.17). Sie kann ferner dazu eingesetzt werden, um organisatorische Rollentrennungen, die unbefugte Offenbarungen innerhalb des Krankenhauses unterbinden sollen, wirksam zu unterstützen (Tz. 2.18 bis 2.19).	
		2.16 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
		2.17 Speichermedien, welche Daten des KIS aufnehmen und nicht fest installiert sind, müssen verschlüsselt werden (durch Datenträger- oder Dateisystemverschlüsselung). Gleiches gilt für Speichermedien, die sich nicht im alleinigen Zugriff des Krankenhauses befinden. Andere Speichermedien sollen verschlüsselt werden. Die Verschlüsselung mobiler Datenmedien dient dem Schutz der Daten bei Verlust des Mediums, die Verschlüsselung fest installierter Medien dient der Minderung des Risikos unberechtigten Zugriffs auf den Datenträger, auch nach seiner Aussonderung.	B Muss B Soll
		2.18 Das Informationssicherheitskonzept 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.	B Muss
7.12 ~~Das Rollen- und Berechtigungskonzept muss es erlauben, den Zugriff auf 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.	~~H muss~~ ~~soll~~	2.19 Zur Wahrung der Vertraulichkeit, Integrität und Authentizität der Daten in Protokollen, die zu Zwecken der Datenschutzkontrolle geführt werden, sollten 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.	Sollte
3 Anwendungsfunktionen		**3 Anwendungsfunktionen**	
		Anwender interagieren mit dem PAS innerhalb der ihnen zur Verfügung stehenden Verarbeitungskontexte, in dem sie eine Funktion des PAS zur Anwendung bringen. Der jeweils aktive Verarbeitungskontext bestimmt die Auswahl der zur Verfügung stehenden Funktionen und modifiziert ggf. deren Ergebnis.	
3.1 ~~Anwender interagieren mit dem PAS innerhalb der ihnen zur Verfügung stehenden Verarbeitungskontexte durch Ausführung von Transaktionen[8] 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		3.1 Die Verarbeitungskontexte sollen derart konfigurierbar sein, dass ein Verarbeitungskontext lediglich die Transaktionen zur Verfügung stellt, die zur Ausübung der funktionellen Rollen erforderlich ist, denen er zugeordnet ist. (Teil I, Tz. 7)	H Soll

[6] 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.

[7] 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.

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

OH Kis Version 1.0		OH Kis Version 2.0	

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):~~
• ~~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~~
• ~~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 soll
	
	~~H soll~~
	~~B~~		

		3.2 Das Krankenhaus muss in seinem Berechtigungskonzept für jeden Verarbeitungskontext festlegen, welche Funktionen für die Ausübung der mit ihm verbundenen funktionellen Rollen erforderlich sind und bereitgestellt werden. (Teil I, Tz. 1, 7, 28).	
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	H muss	3.3 Die Nutzer müssen jederzeit im Rahmen ihrer Aufgaben die Möglichkeit haben, den der anstehenden Arbeitsaufgabe zugeordneten Verarbeitungskontext auszuwählen. Bei einem Wechsel der Verarbeitungskontexte kann ein Bezug der im alten Verarbeitungskontext geöffneten Fallakte (Fall-ID) an den neuen Verarbeitungskontext übergeben werden, sofern gewährleistet ist, dass diese Fallakte im neuen Verarbeitungskontext nur geöffnet wird, soweit sie im Ergebnis einer im neuen Verarbeitungskontext zulässigen Suche oder Abfrage gefunden werden kann.	H Muss

OH Kis Version 1.0		OH Kis Version 2.0	
Verarbeitungskontext nur geöffnet wird, ~~falls~~ sie im Ergebnis einer im neuen Verarbeitungskontext zulässigen Suche oder Abfrage gefunden werden kann.			
~~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). ~~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 jeweiligen Verarbeitungskontext für eine Suche erforderlichen Attribute nach ihrer Erforderlichkeit festlegen (Teil I, Tz. 10,18,21,24,27).~~	H muss ~~B~~ ~~B muss~~	3.4 Ein PAS muss es ermöglichen, die Bearbeitungs- und Recherchefunktionen einschließlich der angebotenen Suchattribute und im Ergebnis anzuzeigenden Datenfelder sowie die in eine Suche einzubeziehenden Patienten in Abhängigkeit von Verarbeitungskontext und Zugriffsberechtigungen nach dem Prinzip der Erforderlichkeit anzupassen. Menüpunkte und Bildschirmmasken, sowie Ergebnislisten müssen in dieser Hinsicht flexibel gestaltet werden können. Das gleiche gilt für allgemeine Übersichtslisten (wie z. B. Stationslisten). (Teil I, Tz. 1, 7, 28)	H Muss
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	3.5 Das PAS muss über eine Funktion verfügen, mit der im Rahmen der Aufnahme eines Patienten eine Kurzübersicht mit den zugelassenen Daten zurückliegender Behandlungsfälle erzeugt werden kann (Teil I, Tz. 1 - 3).	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~~		
		3.6 Das PAS soll über eine Funktion verfügen, mit der Akten abgeschlossener Behandlungsfälle eines Patienten (oder Teile hiervon) der aktuellen Fallakte mit der Auswirkung zugeordnet werden können, dass die Aufbewahrungsfrist der aktuellen Fallakte sich auf die zugeordneten Daten erstreckt. (Teil I, Tz. 27)	
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	3.7 Für Sonderzugriffe muss systemseitig die Eingabe einer Begründung gefordert werden können, ggf. auch im Nachhinein. (vgl. Tz. 4.9). (Teil I, Tz. 14)	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~~	3.8 Ein PAS soll eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein. (Authentizität)	H Soll
3.10 Ein PAS ~~muss~~ es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9).	H ~~muss~~	3.9 Ein PAS soll es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9). (Authentizität)	H Soll
3.11 Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden.	H soll B	3.10 Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden. (Teil I, Tz. 30, 31)	HB Soll
3.12 Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. ~~28~~)[9].	H soll B	3.11 Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 30, 31)[10].	HB 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~~	~~H muss~~		

[9] 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.

[10] Dies ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf ein 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.

OH Kis Version 1.0		OH Kis Version 2.0	
~~Anforderungen lesende Zugriffe nicht protokolliert werden, muss die Übersicht erkennen lassen, welche Stellen grundsätzlich zugriffsberechtigt waren (Teil I Tz. 40).~~			
~~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 werden können.~~	~~H sollte~~		
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	3.12 Die Speicherorte medizinischer Daten sowie die Möglichkeit zum Export von Daten sollen durch Konfiguration beschränkbar sein, z. B. soll die lokale Datenspeicherung auf Arbeitsplatzrechnern unterbunden werden können. (Zugriffs- und Weitergabekontrolle / Vertraulichkeit)	HB Soll
4 Rollen- und Berechtigungskonzept		**4 Rollen- und Berechtigungskonzept**	
		Berechtigungen regeln, wer auf welche Daten welcher Patienten wann lesenden oder schreibenden Zugriff nehmen darf. Sie können den Beschäftigten entsprechend der von ihnen ausgefüllten Rollen statisch zugewiesen werden. Wichtiger Parameter ist hierbei die Zuordnung der Beschäftigten zu Organisationseinheiten, in denen sie tätig und die Patienten behandelt werden. Andere Berechtigungen ergeben sich über diese Zuordnung hinaus dynamisch, insbesondere aus Leistungsanforderungen und anderen ärztlichen Entscheidungen heraus. Damit diese Entscheidungen berechtigungswirksam werden, bedürfen sie der elektronischen Dokumentation und der Fähigkeit des Systems auf das Vorliegen der Anordnung zu reagieren. Schließlich können sich Berechtigungen auch situationsbezogen ergeben, insbesondere dann, wenn die Beschäftigten auf unvorhergesehene Umstände reagieren müssen. Diese Umstände können sowohl in einem medizinischen Ereignis begründet sein, als auch in ungeplanten organisatorischen Lagen. Eine gängige und zulässige Möglichkeit für den Umgang mit diesen speziellen Situationen ist unten in Tz. 4.9 beschrieben.	
4.1 Das Berechtigungskonzept des PAS muss es ermöglichen, Berechtigungen anknüpfend an folgende Attribute eines Datenobjekts bzw. der Patientenakte zu erteilen: • 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)	H muss	4.1 Das Berechtigungskonzept des PAS muss es ermöglichen, Berechtigungen anknüpfend an folgende Attribute eines Datenobjekts bzw. der Patientenakte zu erteilen: • Zuordnung des Patienten zu Organisationseinheiten (Teil I, Tz. 9) • Dokumentierte ärztliche Anweisungen (u.a. Leistungsanforderungen) und explizite Delegierungen (Teil I, Tz. 10, 13) • Datenkategorie (Teil I, Tz. 1, 7, 28) • Kennzeichen nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 (s. dort) • Ersteller des Datenobjekts / eines Datenobjekts in der Patientenakte (Teil I, Tz. 12, 15, 22) • Impliziter oder explizit erklärter Verarbeitungskontext (Teil I, Tz. 1, 7, 28) 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 (Teil I, Tz. 7, 12), • einem Dienst- oder Bereitschaftsplan (Teil I, Tz. 12 und 17), und • dem hinterlegten Behandlungspfad des Patienten (Teil I, Tz. 10) zu erteilen (4.8)	H Muss Sollte
4.2 Das Rollen- und Berechtigungskonzept muss grundsätzlich folgende Benutzerkategorien unterscheiden: • Ärztliche ~~Mitarbeiter~~ • Nicht-ärztliches medizinisches Fachpersonal (z.B. Pflegekräfte) • Verwaltungskräfte • Ausbildungskräfte • Externe Kräfte Administration	H muss	4.2 Das Rollen- und Berechtigungskonzept muss grundsätzlich folgende Benutzerkategorien unterscheiden: • Ärztliche Beschäftigte (Teil I, Tz. 7, 9ff.) • Nicht-ärztliches medizinisches Fachpersonal (z. B. Pflegekräfte) (Teil I, Tz. 16ff., 19ff.) • Verwaltungskräfte (Teil I, Tz. 28 bis 30) • Ausbildungskräfte (Teil I, Tz. 31) • Externe Kräfte (Teil I, Tz. 15, 32) Technische Administration (Teil I, Tz. 38ff.)	H Muss

OH Kis Version 1.0		OH Kis Version 2.0	
~~4.3 Das Rollenmodell muss zumindest nach folgenden strukturellen Rollen differenzieren:~~ ~~• 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~~	~~H muss~~		
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. ~~Der Verarbeitungskontext (oder die Menge der verfügbaren Verarbeitungskontexte) sollte für alle Mitglieder einer Organisationseinheit gleich sein.~~	H muss ~~B sollte~~	4.3 Zur Definition von Rechten muss es möglich sein, Organisationseinheiten flexibel und überlappend zu definieren (Teil I, Tz. 9, 10). 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
4.5 Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann.	B muss	4.4 Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann. (Transparenz, Datenschutzkontrolle)	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	4.5 Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen. (Transparenz, Datenschutzkontrolle)	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	4.6 Das PAS muss über eine Funktion verfügen, die es erlaubt, für bestimmte Berechtigungen in einer Übersicht die Benutzer darzustellen, die über diese Berechtigung verfügen. Insbesondere muss es für ein gegebenes Datenobjekt effizient bestimmt werden können, welche Mitarbeiter darauf schreibend oder lesend zugreifen können. (Transparenz, Datenschutzkontrolle)	H Muss B 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~~). ~~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.~~	H muss B sollte	4.7 Das PAS muss über Funktionen verfügen, mit denen ein Behandlungsfall a) zur Mitbehandlung einer weiteren funktionsbezogenen Organisationseinheit oder einzelnen Behandlern dauerhaft, befristet oder auftragsbezogen zugewiesen werden kann (Teil I, Tz. 10, 12, 13) und b) im Rahmen einer Verlegung einer anderen funktionsbezogenen Organisationseinheit dauerhaft zugewiesen werden kann. Das Rollen- und Berechtigungskonzept muss anknüpfend an die Zuweisung den Zugriff der anderen Organisationseinheit ermöglichen. (Teil I, Tz. 11 und 18)	H Muss
		4.8 Rollen und Berechtigungen z. B. für Bereitschaftsdienste oder Vertretungen müssen einer Benutzerkennung einfach und flexibel zugeordnet werden können, um etwaigen	H Muss

OH Kis Version 1.0		OH Kis Version 2.0	
		wechselnden Aufgabenstellungen Rechnung zu tragen. Hierbei sollten auch zeitliche Muster und Dienstpläne abgebildet werden können (z. B. Rolle Bereitschaftsdienst am Wochenende oder für einen bestimmten Zeitraum; Teil I, Tz. 12 und 17).	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) und im zweiten Schritt der Zugriff eröffnet wird. Dabei soll die Möglichkeit bestehen, den Zugriff zeitlich zu beschränken (z.B. 24 Std.) ~~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 ~~HB soll~~ ~~HB muss~~	4.9 Das Berechtigungskonzept muss die Möglichkeit bieten, Zugriffsbeschränkungen situationsbezogen aufzuheben bzw. Zugriffsrechte zu erweitern. Dies gilt insbesondere für Sonderzugriffe (Teil I, Tz. 14), Zugriffe im Rahmen retrospektiver Prüfungen oder Zugriffe im Rahmen der Qualitätssicherung (Teil I, Tz. 22 und 29). Dabei ist ein zweistufiges Verfahren vorzusehen, bei dem vor der Ausführung einer Transaktion in einem ersten Schritt • eine Begründung für die Erforderlichkeit der Transaktion eingegeben wird (vgl. Tz. 3.9) oder • die Bestätigung durch einen zweiten berechtigten Mitarbeiter erfolgen muss (4-Augen-Prinzip) und erst im zweiten Schritt der Zugriff eröffnet wird. Dabei soll die Möglichkeit bestehen, den Zugriff zeitlich zu beschränken (z. B. auf 24 Std.) Auf die Erweiterung der Zugriffsrechte und die Protokollierung des Zugriffs (vgl. 7.11) soll zuvor hingewiesen werden.	HB Muss H Muss B Soll H Muss B Soll
~~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 durch z.B. ~~einen~~ maschinenlesbaren ~~Mitarbeiterausweis~~, ~~ein~~ RFID-~~Tag~~ oder ~~ein vergleichbares Token~~ zu knüpfen ~~(Teil I Tz. 12,15,16,19)~~.	H sollte	4.10 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 z. B. durch Präsenz eines maschinenlesbaren Mitarbeiterausweises, eines RFID-Tags oder eines vergleichbaren Tokens zu knüpfen (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit).	H Sollte
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	4.11 Es muss sichergestellt sein, dass es keinem Nutzer möglich ist, durch eine Verknüpfung von Rechten oder einen 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 (Zugriffskontrolle / Vertraulichkeit).	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	4.12 Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben. (Zugriffskontrolle / Vertraulichkeit)	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	4.13 Das Krankenhaus muss strukturelle Rollen so zuschneiden, dass sie sich unabhängig von der konkreten Person an der Stellung in der Krankenhausorganisation ausrichten. 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 (Transparenz).	B Muss

OH Kis Version 1.0		OH Kis Version 2.0	
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	4.14 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. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)	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	4.15 Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Zugriffskontrolle / Vertraulichkeit).	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	4.16 Die Benutzerverwaltung sollte über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Mitarbeitern automatisiert zu deaktivieren.	HB Sollte
4.18 Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer für einen festgelegten Zeitraum keine Anmeldung mehr erfolgt ist. 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.	H sollte B	4.17 Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer für einen festgelegten Zeitraum keine Anmeldung mehr erfolgt ist. 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.	H Sollte B Muss
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	4.18 Das PAS muss es ermöglichen, dass für die Verfahrensbetreuung und die Berechtigungsverwaltung unterschiedliche Personen mit separaten Benutzerkennungen festgelegt werden können (Teil I, Tz. 38 und Teil II, 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 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	5.1 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. (Teil I, Tz. 30 und 31).	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~~)[11].	HB soll	5.2 Das PAS soll es ermöglichen, in Abhängigkeit vom Verarbeitungskontext Teile der Patientenakte mit Pseudonymen oder temporären Patientenkennzeichen, die die Identitätsdaten des Patienten ersetzen, darzustellen (Teil I, Tz. 30 und 31)[12].	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	5.3 Das PAS sollte die Oberflächen verschiedener Verarbeitungskontexte klar voneinander optisch (z. B. farblich) unterscheiden, um es den Nutzern zu erleichtern, die ggf. je nach Verarbeitungskontext variierenden Berechtigungen nachzuvollziehen. Dies gilt insbesondere für die Oberfläche des Sonderzugriffs. Hier dient die optische Hervorhebung zusätzlich dazu, den Nutzer aufzufordern, den Zugriff mit erweiterten Rechten nur solange zu nutzen, wie dies erforderlich ist.	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	5.4 Es muss die Möglichkeit bestehen die Angaben nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 in Bildschirmmasken zu integrieren, um, wo es erforderlich oder hilfreich ist, den Nutzern einen Hinweis zu geben, im Kontext welchen Mandantens sie operieren, ob für den Patienten eine Auskunftssperre eingerichtet wurde, welcher bzw. welchen Organisationseinheiten ein Patient zugeordnet ist bzw. war, ob die Behandlung und/oder Abrechnung bereits abgeschlossen oder der Patient einer besonders schutzwürdigen Gruppe angehört.	H Muss

[11] 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.

[12] Dies ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf ein 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

OH Kis Version 1.0		OH Kis Version 2.0	
6 ~~Nutzungsergonomie~~		**6 Systemzugang**	
6.1 Ein PAS muss einen schnellen Benutzerwechsel ermöglichen (vgl. Tz. 3.2).	H muss	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	6.2 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	6.3 An Arbeitsplätzen des PAS muss eine Bildschirmsperre oder ein Auto-Logout auf Betriebssystem- oder Anwendungsebene eingerichtet sein. Die Zeitdauer bis zur Aktivierung von Sperre oder Logout muss sich an dem Risiko unberechtigten Zugangs zu dem Arbeitsplatz ausrichten. (Zugriffskontrolle / Vertraulichkeit)	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	6.4 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 sollte H muss	6.5 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. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)	H Sollte H 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 Protokollierung / Auswertung von Protokolldaten**	
		Die Vorgaben in diesem Kapitel dienen der Umsetzung der in Teil I, Tz. 43 bis 45 und 47 aufgeführten Anforderungen.	

OH Kis Version 1.0			OH Kis Version 2.0	
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)~~.	7.1	H muss	7.1 Für Zwecke der Datenschutzkontrolle muss eine Protokollierung relevanter Ereignisse vorhanden sein. Die Protokollierung muss darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Neben der Speicherung personenbezogener Daten und deren Änderung müssen auch lesende Zugriffe auf sie nachvollzogen werden können.	H Muss
			7.2 Art und Umfang der Protokollierung, die Verfahrensweisen zur Speicherung, die getroffenen Schutzmaßnahmen, das Vorgehen zur Auswertung der Protokolle sowie die Aufbewahrungsdauer der Protokolldaten sind in einem Protokollierungs- und Auswertungskonzept festzulegen, unter Einbeziehung des behördlichen/betrieblichen Datenschutzbeauftragten und der Mitarbeitervertretung. Die Verpflichtung zur Protokollierung und Auswertung der Protokolle (s. Tz. 7.3ff.) kann jedoch nicht durch Betriebsvereinbarung ausgeschlossen werden.	B 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 muss ~~B muss~~		7.3 Art und der Umfang der Protokollierung müssen sich am Schutzbedarf der jeweiligen Daten orientieren. Die Protokollierung ist auf das erforderliche Maß zu beschränken. Sie kann inhaltlich reduziert werden, wenn ein differenziertes Rollen- und Berechtigungskonzept vorhanden ist. Umgekehrt steigt ihre Bedeutung in Bereichen mit weit gefassten (Abfrage-) Berechtigungen. Bei Zugriffen, die technisch festgelegt in wiederkehrender Weise aufeinander folgen (Workflow) ist eine Protokollierung der einzelnen Verfahrensschritte entbehrlich. In diesem Fall ist es ausreichend, den Start des Workflows zu dokumentieren.	HB 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 Protokollierung muss alle relevanten Zugriffe erfassen. Eine stichprobenweise Protokollierung oder die Protokollierung lediglich eines bestimmten Anteils von Zugriffen sind für eine effektive Datenschutzkontrolle untauglich.	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~~		7.5 Bei der Protokollierung muss zwischen Zugriffen, die aus der fachlichen Nutzung des Verfahrens resultieren (Zugriffe zu Zwecken der Behandlung, der Leistungsabrechnung und Verwaltung, der Ausbildung, der Forschung, der Erfüllung von Dokumentations- und Mitteilungspflichten etc.) und technisch-administrativen Zugriffen im Rahmen des System- und Verfahrensbetriebs differenziert werden.	B 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 Rechnung.	H sollte		7.6 Die Protokollierung sollte auf der Ebene der Anwendungsfunktionen erfolgen, um die Nutzung des PAS nachvollziehen zu können. Eine Protokollierung auf Datenbankebene oder eine technische Protokollierung ohne Bezug zum sachlichen Zusammenhang eines Zugriffs trägt dem nicht Rechnung.	H Sollte
7.7 ~~Protokollfunktionen müssen revisionssicher ausgestaltet sein, d.h., vorgesehene Protokollierungen dürfen nicht umgangen werden können~~ und	H muss		7.7 Vorgesehene Protokollierungen dürfen nicht umgangen werden können.	H Muss
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 Eine nachträgliche Veränderung von Protokolldaten darf nicht möglich sein.	HB Muss
			7.9 Protokolle sollen so konfigurierbar sein, dass sie keine medizinischen Daten enthalten. (Datensparsamkeit / Vertraulichkeit)	HB Soll

OH Kis Version 1.0		OH Kis Version 2.0	
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	7.10 Neben der Anmeldung am Verfahren (Login/Logout) müssen die Zugriffe der Nutzer mit zumindest folgenden Angaben protokolliert werden: – Zeitpunkt des Zugriffs, – Kennung des jeweiligen Benutzers, – Kennung der jeweiligen Arbeitsstation, – aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung), – betroffene Patienten/Behandlungsfälle Bei Aufruf einer Suchfunktion muss das Protokoll mindestens enthalten: – verwendete Such- bzw. Abfragekriterien (z. B. Patientennummer, Fallnummer, Name, Geburtsdatum, Wohnort, Diagnose etc.), – Angaben zum 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).	HB 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 Ist für die Ausführung einer Transaktion die Eingabe einer besonderen Begründung vorgesehen (vgl. Tz. 4.9) muss diese von der Protokollierung erfasst werden.	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 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.	~~H muss~~ ~~soll~~	2.19 Zur Wahrung der Vertraulichkeit, Integrität und Authentizität der Daten in Protokollen, die zu Zwecken der Datenschutzkontrolle geführt werden, sollten 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.	Sollte
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~~	7.19 Zugriffe auf Protokolldaten sollten nur nach dem Vier-Augen-Prinzip und unter Beteiligung eines Datenschutzverantwortlichen erfolgen.	HB 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:~~	~~B muss~~		

OH Kis Version 1.0		OH Kis Version 2.0	
~~- 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 sollte	7.12 Aufgrund der Reichweite technisch-administrativer Funktionen bedarf deren Nutzung einer besonderen Kontrolle. Die Protokollierung von Zugriffen im Rahmen der System- und Verfahrensadministration muss alle Zugriffe erfassen, die Auswirkungen auf Art oder Umfang der Verarbeitung personenbezogener Daten haben (Teil I, Tz. 39)	H Muss
		7.13 Es muss nachvollziehbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt wurden, insbesondere welche Zugriffe auf personenbezogene Daten hierbei erfolgt sind (Teil I, Tz. 40).	H Muss
		7.14 Hierzu müssen die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festgehalten werden (Teil I, Tz. 40).	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.		7.15 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.	HB Sollte
7.19 Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten auswerten zu können. Hierzu ~~sollten bereits~~ im Verfahren selbst Auswertungsmöglichkeiten vorgesehen werden~~, die eine schnelle Selektion prüfungsrelevanter Datensätze nach folgenden Gesichtspunkten erlauben:~~ ~~- Verarbeitungskontext~~ ~~- Begründungspflicht für die Transaktion (vgl. 4.9)~~ ~~- Benutzerkennung,~~ ~~- Arbeitsstation,~~ ~~- Funktionen/Transaktionen,~~ ~~- Suchkriterien,~~ ~~- Patientennummer / Fallnummer,~~ ~~- Zeitraum.~~ ~~(Teil I Tz. 38)~~.	H muss sollte	7.16 Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten auswerten zu können. Hierzu sollen im Verfahren selbst Auswertungsmöglichkeiten und ein Datenschutzarbeitsplatz vorgesehen werden.	H Muss Soll
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	7.17 Die Auswertung muss nach den in Tz. 7.10 genannten Gesichtspunkten möglich sein. 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 auswertbares Format überführt werden können.	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~~	~~HB soll~~		

OH Kis Version 1.0		OH Kis Version 2.0	
~~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.~~			
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	7.18 Das Rollen- und Berechtigungskonzept muss es erlauben, den Zugriff auf Protokolldaten für Auswertungszwecke separat zu vergeben. Hierfür ist eine Rolle einzurichten, die über die erforderlichen Funktionen verfügt. Es muss gewährleistet sein, dass eine Einsichtnahme nur Personen möglich ist, in deren Aufgabenbereich Auswertungen von Protokolldaten fallen.	HB muss
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~~	7.19 Zugriffe auf Protokolldaten sollten nur nach dem Vier-Augen-Prinzip und unter Beteiligung eines Datenschutzverantwortlichen erfolgen.	HB Sollte
		7.20 Krankenhäuser müssen Auffälligkeits- und Stichprobenauswertungen der Zugriffsprotokolle vorsehen. Die Protokolle über Sonderzugriffe unter Verwendung eines Verfahrens nach Tz. 4.9 müssen dabei mit einer angemessenen Prüfdichte einbezogen werden.	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	7.21 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. Gleiches gilt für Zugriffe, die im Rahmen der Fernwartung erfolgt sind.	B Muss
		7.22 Daten aus der Protokollierung administrativer Zugriffe sind, soweit sie Konfigurationsänderungen und Datenübermittlungen betreffen, als Teil der Verfahrensdokumentation anzusehen. Hier müssen längere Aufbewahrungsfristen als unter Tz. 7.21 genannt, orientiert an der Dauer des Einsatzes eines Verfahrens vorgesehen werden.	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 Technischer Betrieb, Administration**	
8.1 Die Administration eines KIS muss in die Bereiche - technische Administration der genutzten IT-Komponenten, - Anwendungsadministration / Verfahrensbetreuung und - Berechtigungsverwaltung ~~Getrennt~~ werden. Die jeweiligen Rollen ~~sollen~~ unterschiedlichen Personen zugewiesen werden(Teil I TZ. ~~2~~).	B muss B soll	8.1 Die Administration eines KIS muss in die Bereiche – technische Administration der genutzten IT-Komponenten, – Anwendungsadministration / Verfahrensbetreuung und – Berechtigungsverwaltung getrennt werden. Die jeweiligen Rollen sollten unterschiedlichen Personen zugewiesen werden (Teil I, Tz. 38).	B Muss B Sollte
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	8.2 Das Krankenhaus muss sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann (Teil I, Tz. 40).	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 Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 40).	H Soll
8.3 Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können ~~(Teil I, Tz. 33)~~.	H muss	8.4 Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können, wobei die Systemkonsistenz zu wahren ist. (Weitergabekontrolle / Vertraulichkeit)	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 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. 40).	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~~		

OH Kis Version 1.0			OH Kis Version 2.0	
	~~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	8.6 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.40).	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	8.7 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 und, 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 Auswertungsmöglichkeiten (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 Aufbewahrungsfristen als unter Tz. 7.24 genannt, orientiert an der Dauer des Einsatzes eines Verfahrens vorgesehen werden.~~	~~B muss~~		

III. Anhang

Rollen werden in Version 1 in Teil 2 unter 3.1 und 4.3 beschrieben, in der überarbeiteten Version der OH KIS im Anhang. Um daher die in der OH KIS erfolgte Darstellung der Rollen vergleichen zu können, wurden die Textstellen aus den verschiedenen Bereichen zusammengeführt.

OH Kis Version 1.0	OH Kis Version 2.0
	Die Einrichtung von Rollen und Verarbeitungskontexten in einem PAS dient der Eingrenzung der Zugriffsmöglichkeiten der Beschäftigten auf das für ihre jeweilige Tätigkeit erforderliche Maß' sowohl in Bezug darauf' die Daten welcher Patienten sie einsehen oder ändern dürfen als auch darauf' welche der zu dem jeweiligen Patienten gespeicherten Daten eingesehen und welche eingegeben werden können. Je nach ihrer Rolle erhalten die Beschäftigten Zugriff auf die Daten der Patienten nach deren Zuordnung zu Organisationseinheiten (Fachabteilungen' Stationen) oder auf der Grundlage einer ärztlichen Anweisung. In bestimmten strukturellen Rollen dürfen Beschäftigte zudem die ihnen regelhaft gesetzten Zugriffsbegrenzungen in dem Verfahren nach Tz. 4.9 überschreiten.
~~4.3 Das Rollenmoell muss zumindest nach folgenden strukturellen Rollen differenzieren:~~ • 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	Im Folgenden sind einige strukturelle Rollen aufgeführt' die regelmäßig in Krankenhäusern zu finden sind. PAS-Produkte sollen die Betreiber unterstützen' diese Rollen in ihrem Berechtigungskonzept umzusetzen. Welche Rollen in einem konkreten Krankenhaus abgebildet werden müssen' hängt von seiner organisatorischen Struktur ab. • 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

~~3.1 Mindestens folgende Verarbeitungskontexte soll ein PAS unterscheiden (soweit die entsprechenden funktionellen Rollen durch das PAS unterstützt werden):~~
• 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
	Beschäftigten können selbstverständlich auch mehrere der genannten Rollen zugeordnet werden. Verarbeitungskontexte bestimmen die Sicht der Beschäftigten auf die Daten und ihre Verarbeitungsmöglichkeiten. In einigen Rollen steht den Beschäftigten nur ein spezifischer Verarbeitungskontext offen' in anderen Rollen oder bei Übernahme mehrerer struktureller Rollen können die Beschäftigten von einem Verarbeitungskontext in einen anderen wechseln' der ihrer jeweiligen aktuellen Tätigkeit entspricht. Gängige Verarbeitungskontexte sind:
	• Administrative Patientenaufnahme
	• Behandlung
	  • Behandlung nach fachlicher Zuordnung
	  • Mitbehandlung auf Anfrage oder Anordnung eines Arztes mit bestehendem Behandlungszusammenhang

OH Kis Version 1.0	OH Kis Version 2.0
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 • 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.~~	• 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 • 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 Weitere Hinweise zu strukturellen und funktionalen Rollen finden sich in dem Standard ISO/TS 21298:2008 Health informatics—Functional and structural roles.

Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern

OH Kis Version 1.0	OH Kis Version 2.0
	I. Vorbemerkung Eine enge Zusammenarbeit zwischen stationären und ambulanten Leistungserbringern dient dem Wohl des Patienten. Sie ist erklärtes Ziel der Gesundheitspolitik. Vielfach befinden sich durch Ausgründungen und Übernahmen Leistungserbringer aus beiden Sektoren in gleicher Trägerschaft und in großer räumlicher Nähe. Teilweise haben Krankenhäuser Abteilungen und Einrichtungen für die ambulante Versorgung in juristisch selbstständige Leistungserbringer wie z.B. Medizinische Versorgungszentren eingebracht. Die enge Verzahnung mit dem „Mutterunternehmen“ ist für die Patienten von Vorteil, die Leistungen von beiden Einrichtungen in Anspruch nehmen. Die enge Zusammenarbeit ruft den naheliegenden Wunsch nach einem unkomplizierten Zugriff einer Einrichtung auf Daten der anderen hervor. Soweit dieser dem Wunsch und Interesse eines Patienten entspricht, steht auch datenschutzrechtlich der Gewährung eines solchen Zugriffs nichts entgegen. Der Nutzen für die einen, darf jedoch nicht mit Einschränkung der Rechte der anderen bezahlt werden. Wer nur in einer Einrichtung behandelt wird, dessen Daten haben in der anderen erst einmal nichts zu suchen: Auch in der Konstellation einer engen Zusammenarbeit zwischen zwei Einrichtungen ist die ärztliche Schweigepflicht zu wahren, darf eine Übermittlung nur erfolgen, wenn sie datenschutzrechtlich zulässig ist. Während eine Reihe von Rechtsgrundlagen bundeseinheitlich zur Anwendung kommen, wie das Strafgesetzbuch, das auf Einrichtungen in privater Trägerschaft anwendbare Bundesdatenschutzgesetz und das vornehmlich die Beziehungen zu den Sozialleistungsträgern regelnde Sozialgesetzbuch, so sind die rechtlichen Rahmenbedingungen doch stark durch das Landesrecht geprägt. Während die Ärztekammern zwar eigenständige, aber doch noch weitgehend deckungsgleiche Berufsordnungen beschlossen haben, variieren die Landesdatenschutzgesetze und deutlich mehr noch die Landeskrankenhausgesetze in ihrer Regelungstiefe und der Breite der Erlaubnis und gesetzten Voraussetzungen für die Offenbarung von Patientendaten an Ärzte anderer Leistungserbringer und deren Gehilfen. Weitgehend ungeregelt hat der Gesetzgeber die Offenbarung von Berufsgeheimnissen an technische Dienstleister gelassen, die nicht als Gehilfen eines ambulant tätigen Arztes einzuordnen sind, weil sie im Rahmen eines vom Leistungserbringer rechtlich unabhängigen Unternehmens tätig sind. Als einzige Rechtsgrundlage für derartige Offenbarungen verbleibt daher lediglich die Einwilligung der Patienten. Diese ist nur wirksam, wenn sie freiwillig erteilt wird. Eine freie Entscheidung setzt eine freie Wahl unter annähernd gleichwertigen Alternativen voraus. Diese sind bei eng mit einem Krankenhaus verbundenen Leistungserbringern jedoch oft nur mit erheblichen Abstrichen zu finden. Der Gesetzgeber ist daher gefordert, mit einer sorgfältig austarierten Gewährung der Befugnis zur Offenbarung von Patientendaten an qualifizierte Dienstleister, die diese Daten im Auftrag verarbeiten, die derzeit eingesetzten Einwilligungslösungen mit zweifelhafter rechtlicher Tragfähigkeit entbehrlich zu machen. Der vorliegende Szenarienkatalog setzt sich das Ziel, einige Wege durch das rechtliche Minenfeld zu weisen, in dem die medizinischen Leistungserbringer im Rahmen ihrer Kooperation wandeln. Die Aufzählung von Ausgestaltungsformen zulässiger Zusammenarbeit ist gewollt nicht vollständig und kann dies aufgrund der erwähnten föderalen Vielgestaltigkeit auch nicht sein. Weitere Wege stehen offen. Wir empfehlen ihre Erörterung im vertrauensvollen Dialog mit der zuständigen Datenschutzaufsichts- bzw. -kontrollbehörde.
	II. Szenarien Sämtliche Szenarien gehen von der Zusammenarbeit eines Krankenhauses mit einem ambulanten Leistungserbringer der fachärztlichen Versorgung aus, mit dem es in besonderer Weise verbunden ist. Als typisches Beispiel für letzteren wählen wir ein Medizinisches Versorgungszentrum (MVZ). Die Szenarien sind jedoch auf andere Leistungserbringer,

OH Kis Version 1.0	OH Kis Version 2.0
	die zur vertragsärztlichen Versorgung zugelassen sind, übertragbar. Andere Regeln gelten, wenn das Krankenhaus selbst ambulante Leistungen erbringt, auf vertraglicher Grundlage nach § 116b Sozialgesetzbuch Fünftes Buch (SGB V) oder aufgrund einer Ermächtigung des Zulassungsausschusses nach §§ 117 bis 119 SGB V. Diese Situationen werden hier nicht erfasst.
	Szenario 1: Zulässige Auftragsdatenverarbeitung **Szenario 1a: Gleichwertige Alternativen** Ein von einem Krankenhaus errichtetes MVZ wurde zur vertragsärztlichen Versorgung zugelassen. Das Krankenhaus möchte, um Kosten zu sparen, den Betrieb des Patientenverwaltungssystems von der eigenen IT-Stelle im hauseigenen Rechenzentrum betreiben lassen. Bei ihrem erstmaligen Besuch erhalten die Patienten die Information über den Betrieb der MVZ-IT durch das Krankenhaus. In der gleichen Stadt sind Vertragsärzte ansässig, die das Leistungsspektrum des MVZ insgesamt abdecken. Die Patienten erklären im Zuge der Anmeldung schriftlich ihr Einverständnis mit dieser Datenverarbeitung außer Haus. **Szenario 1b: Ersatzverfahren** Im Unterschied zu dem vorigen Szenario sucht Patient P für die Nachbehandlung einer komplizierten Operation, die er am Universitätsklinikum in M hat durchführen lassen einen Spezialisten, der in der Umgebung ausschließlich am MVZ zu finden ist. Das MVZ hat erkannt, dass für einige seiner Patienten die Behandlung am MVZ alternativlos ist und bietet für diejenigen, die das Risiko einer Offenbarung ihrer Daten am Krankenhaus scheuen, ein einfaches papierbasiertes Alternativverfahren für die Führung der Behandlungsakten an. Daher kann sich das MVZ erfolgreich auf die schriftlichen Einverständniserklärungen seiner Patienten stützen, da aufgrund des Alternativverfahrens eine tatsächliche Freiwilligkeit der Einwilligung gewährleistet ist. **Vertragliche, technische und organisatorische Anforderungen** Ein Auftragsdatenverarbeitungsverhältnis (ADV) setzt eine vertragliche Vereinbarung voraus, in dem ein gesetzlich vorgegebener Katalog von Regelungen getroffen werden muss. Unter anderem ist festzuhalten, dass das Krankenhaus die Daten des MVZ nur nach Weisung der Leitung des rechtlich selbständigen MVZ speichern und verarbeiten darf, welche technischen und organisatorischen Maßnahmen das Krankenhaus zum Schutz der Daten des MVZ zu treffen hat, und wie das MVZ die korrekte Ausführung des Auftrags kontrollieren kann. Zumindest bei großen MVZ liegt es nahe, das im MVZ keine Praxissoftware, sondern ein Modul des Krankenhausinformationssystems zum Einsatz kommt. Zulässig ist dies dann, wenn für das MVZ ein separater Mandant eingerichtet wird. Zu den Anforderungen an die Mandantentrennung vgl. die OH zu diesem Thema, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegeben wurde. Insbesondere müssen die Zugriffsrechte von Mitarbeitern des MVZ unabhängig von denen des Krankenhauses eingerichtet werden. Dies darf nur nach Weisung der hierzu beauftragten Beschäftigten des MVZ geschehen. Personen, die sowohl vom Krankenhaus als auch vom MVZ beschäftigt werden, müssen zwei verschiedene Benutzerkonten zugeordnet werden. Jede Angabe zu einem Patienten muss sich eindeutig einem der beiden Mandanten zuordnen lassen, wofür mehrere technische Ausgestaltungsmöglichkeiten denkbar sind. Für einen mandantenübergreifenden Zugriff auf Patientendaten bedarf es stets einer Übermittlungsbefugnis (s.u.). Dies gilt auch für die Stammdaten der Patienten. Vor der gemeinsamen Anzeige von Daten, die aus Krankenhaus und MVZ stammen, ist die Übertragung in den Mandanten, bei dem die nutzende Person angemeldet ist, technisch abzubilden. Ist vorgesehen, dass Personal des MVZ auch von Geräten des Krankenhauses aus auf Daten von Patienten des MVZ zugreifen soll, muss dies in dem ADV-Vertrag geregelt werden.
	Szenario 2: Übermittlung zur Erfüllung eines Konsilauftrages **Szenario 2a: Konsilauftrag an das MVZ** Patient P wird im Krankenhaus behandelt. Der behandelnde Arzt A möchte die fachliche Meinung einer im

OH Kis Version 1.0	OH Kis Version 2.0
	ambulanten Bereich tätigen Kollegin B einholen. Dies teilt A dem P im Laufe einer Visite mit. Im Nachgang zur Visite wird der Konsilauftrag im Patientenaktensystem (PAS) des Krankenhauses dokumentiert. Dies führt zu einer Übertragung der relevanten Teile der Patientenakte an das MVZ und einer automatisierten Mitteilung an B. Diese nimmt den Konsilauftrag an und sieht die nunmehr freigegebenen Patientendaten ein. Ihr Bericht wird zunächst im AIS gespeichert und dann an das Krankenhaus übertragen, wo er dem A im PAS zur Verfügung steht. Hätte P der Beauftragung von B widersprochen, so wäre der Konsilauftrag nicht zustande gekommen oder A hätte ihn an die Praxis des Kollegen C gerichtet, sofern P nicht auch gegen dessen Einbeziehung Einwände erhebt. **Szenario 2b: Konsilauftrag an ein Labor des Krankenhauses** Wie im vorigen Szenario erfolgt ein Konsilauftrag, den hier die ambulant tätige Ärztin B mit Wissen von Patientin Q nicht an eine einzelne Person, sondern an ein Speziallabor des Krankenhauses richtet. Der im AIS eingegebene Auftrag wird an das Krankenhaus übertragen, der Befund geht ebenfalls elektronisch den umgekehrten Weg. **Rechtliche, organisatorische und technische Ausgestaltung** Durch den Konsilauftrag kommt ein Vertrag zwischen Beauftragtem und Auftraggeber zustande, der den Rahmen für die Übermittlungen darstellt. Der Konsilauftrag kann technisch sowohl vom System des Auftraggebers aufgenommen und an den Auftragnehmer über einen sicheren Kanal an den beauftragten Leistungserbringer übertragen werden, als auch direkt von einer Anwendung des Beauftragten entgegengenommen werden, wiederum über einen sicheren Kanal. Bei Anwendung einer Mandantenlösung begründet die Möglichkeit der Übernahme von Konsilen jedoch nicht die Zulässigkeit des Zugriffs einer Beschäftigten einer Einrichtung auf das PAS bzw. AIS der jeweils anderen.
	Szenario 3: Übermittlung zur Nachbehandlung **Szenario 3a: Im Rahmen der ambulanten Behandlung** Patient P wurde im Krankenhaus K operiert. Nach Abschluss seiner stationären Behandlung sucht P zur Nachbehandlung die Ärztin M des krankenhauseigenen MVZ auf. Ärztin M benötigt zur Weiterführung der Behandlung Unterlagen über die Operation im Krankenhaus. Sie informiert P, dass sie die Unterlagen anfordern wird, und nutzt eine Funktion des Arzt-Informationssystems (AIS) des MVZ, um das Krankenhaus über die Weiterbehandlung zu informieren und um Zugang zu der Fallakte des P zu erbitten. Ein hierzu beauftragter Mitarbeiter des Krankenhauses prüft die Anforderung der Unterlagen und überträgt dann die gewünschten Unterlagen aus der Patientenakte des P in einen Zwischenspeicher, aus dem sie automatisiert in das AIS des MVZ übernommen werden. Der Fakt der Übertragung wird ebenso automatisiert in der Patientenakte des P vermerkt. Die rechtliche Grundlage für diese Übermittlung ergibt sich je nach Landeskrankenhausrecht aus einer konkludenten Einwilligung oder einer gesetzlichen Befugnis. **Szenario 3b: Konkludente Einwilligung im Zuge einer Einweisung** Patient P begibt sich zu seinem Facharzt im MVZ. Der behandelnde Arzt erkennt, dass die ambulante Behandlung nicht zum Ziel führt und weist P in das Krankenhaus ein. P begibt sich in das Krankenhaus. Der dort behandelnde Arzt erkennt, dass er weitergehende Unterlagen aus der ambulanten Behandlung benötigt und ruft bei seinem ihm persönlich bekannten Kollegen im MVZ an. Dieser exportiert die Unterlagen aus dem AIS des MVZ und übermittelt sie elektronisch an das Krankenhaus. Dort werden die Daten in die elektronische Patientenakte des P überführt und stehen in der Folge als Informationsgrundlage für die Behandlung zur Verfügung. **Rechtliche, organisatorische und technische Ausgestaltung** Für eine Übermittlung zwischen Krankenhaus und angeschlossenem MVZ gilt zunächst nichts anderes als für Übermittlungen zwischen dem Krankenhaus und irgendeinem anderen Leistungserbringer: Stützt sich eine Übermittlung auf Aussagen des Empfängers (über das Bestehen eines Behandlungsverhältnisses, über das Vorliegen einer Einwilligung, über das Bestehen einer Notsituation, bei der Gefahr für Leib und Leben des Patienten besteht), so sind diese Aussagen nach Möglichkeit der Umstände zu überprüfen und das Ergebnis zusammen mit der Angabe über die durchgeführte Übermittlung in der Patientenakte zu vermerken. Stellt sich der Anlass der Übermittlung so dringend dar, dass eine Überprüfung im Vorhinein nicht möglich ist, so kann und muss sie im Nachhinein nachgeholt

OH Kis Version 1.0	OH Kis Version 2.0
	werden. Einer Übermittlung steht die Bereitstellung zum Abruf gleich. Näheres hierzu siehe in den Erläuterungen zu dem folgenden Szenario.
	Szenario 4: Abruf für einen neuen Behandlungsvorgang **Szenario 4a: Einwilligung in die Bereitstellung zum Abruf aus einer einrichtungsübergreifenden Patientenakte** Nach Abschluss seiner Behandlung fragt eine Beschäftigte des Krankenhauses den Patienten P, ob er einverstanden sei, dass Angaben über seine Behandlung in eine einrichtungsübergreifende elektronische Patientenakte eingestellt werden, aus der das Krankenhaus selbst und an einem Behandlungsnetzwerk beteiligte ambulante Einrichtungen Daten abrufen können. P sind alle Leistungserbringer bekannt, die an dem Behandlungsnetzwerk teilnehmen. Derart informiert gibt P seine schriftliche Einwilligung und erhält ein zum Zugriff erforderliches Token/erforderlichen Code. Als P anderthalb Jahre später im MVZ (das am Behandlungsnetzwerk beteiligt ist) zur Behandlung einer anderen Erkrankung erscheint,, erkennt die behandelnde Ärztin, dass sie zur Abschätzung der Risiken eines von ihr in Betracht gezogenen Behandlungsweges die Unterlagen aus der früheren Behandlung im Krankenhaus benötigt. Sie fragt P, ob das Krankenhaus seine Daten zum Abruf bereithalte und führt, nachdem P dies bejaht und das Token/den Code übergibt, den Abruf durch. **Szenario 4b: Gefahr für Leib und Leben** Patient P kommt während eines depressiven Schubes in die Sprechstunde von Neurologin N im MVZ. N ist über den Zustand von P sehr besorgt und möchte die Suizidgefährdung von P mit Hilfe der Unterlagen aus einer früheren Behandlung im Krankenhaus einschätzen. Sie hält P nicht für fähig, eine rationale Entscheidung für oder gegen einen derartigen Datenabruf zu treffen. Sie bittet unter Hinweis auf die Notsituation um Einsicht in die Unterlagen des Krankenhauses. Ein ärztlicher Mitarbeiter des psychiatrischen Fachbereichs des Krankenhauses beurteilt die Erforderlichkeit des Abrufs nach den ihm vorliegenden Unterlagen und lässt dann den Zugriff von N auf die Akten des P freischalten. **Rechtliche, organisatorische und technische Ausgestaltung** Für eine Bereitstellung zum Abruf durch den jeweils anderen Leistungserbringer genügt eine einmalige schriftliche Einwilligung und Schweigepflichtentbindung durch den Patienten, die sich an beide (oder den bestimmten Kreis der) Adressaten richten muss. Der Zweck und die Laufzeit der Einwilligung müssen konkret benannt werden. Je unbestimmter der Zweck, bis hin zur zukünftigen Behandlung noch nicht aufgetretener oder bestimmbarer Erkrankungen, desto enger sollte die Laufzeit gefasst werden. Nicht behandlungsbezogene Einwilligungen (Forschung, Qualitätssicherung) bedürfen in jedem Fall der separaten und expliziten, auf das spezifische Vorhaben oder Verfahren ausgerichteten Einwilligung. Der Patient kann die Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen. Eine Bereitstellung zum Abruf setzt eine schriftliche Vereinbarung gemäß dem jeweils anwendbaren Bundes- oder Landesdatenschutzrecht voraus. Beispielhaft sei § 10 Bundesdatenschutzgesetz genannt. Auch hier sind die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Dies gilt auch im Falle der ADV, wenn die Maßnahmen nur von einer Seite ausgeführt werden, zum einen für sich selbst und zum anderen für die andere Seite in derem Auftrag. Zum Abruf bereitgestellte Daten sollten in einen Zwischenspeicher überführt werden. Dies gilt insbesondere dann, wenn der Abruf über Weitverkehrsnetze abgewickelt wird, damit aus diesen kein direkter Durchgriff auf das PAS bzw. das AIS ermöglicht wird. Ein Abruf darf ausschließlich über einen besonders gesicherten verschlüsselten Kanal erfolgen, bei dessen Aufbau sich beide Seiten gegenseitig authentisieren müssen, Die Struktur des Zwischenspeichers muss gewährleisten, dass die Daten eines Patienten bei einem Widerruf der Einwilligung unmittelbar und vollständig gelöscht werden können, ohne die Dokumentation der getätigten Abrufe zu berühren. Sind Abrufe zwischen zwei Mandanten ein und desselben Systems vorgesehen, so genügt es, die zum Abruf bereitgestellten Daten als solche zu kennzeichnen. Der tatsächliche Abruf verwirklicht sich durch einen Kopiervorgang aus dem Datenbestand des einen in den Datenbestand des anderen Mandanten. In beiden Ausgestaltungsformen sind Abrufe wie Übermittlungen in das zu Zwecken der Datenschutzkontrolle

OH Kis Version 1.0	OH Kis Version 2.0
	geführte Verarbeitungsprotokoll aufzunehmen.