Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

-Synopse-

Version 1.4 mit den Ergebnissen der Sitzung am 28. August 2013

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

Neue Fassung	Alte Fassung	Hinweise
- *Schriftfarbe schwarz* ➔ *keine Änderung erfolgt* - *Schriftfarbe rot* ➔ *neuer Text in neuer Fassung* - *Schriftfarbe grün* ➔ *Verschobener Text*	- *Schriftfarbe schwarz* ➔ *keine Änderung erfolgt* - *Schriftfarbe blau* ➔ *in neuer Fassung gelöschter Text* - *Schriftfarbe grün* ➔ *Verschobener Text*	

I. Vorbemerkung		
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.	Das vorliegende Papier ist der zweite Teil der Orientierungshilfe „Krankenhausinformationssysteme (KIS) datenschutzgerecht gestalten und betreiben“ der Arbeitskreise „Technik“ sowie „Gesundheit und Soziales“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Es beschreibt Maßnahmen zur technischen Umsetzung der bestehenden datenschutzrechtlichen Regelungen und der Vorgaben zur ärztlichen Schweigepflicht beim Einsatz von Krankenhausinformationssystemen. Sie nehmen auf die in Teil I der Orientierungshilfe dargestellten normativen Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus Bezug und geben Hinweise zu einer datenschutzkonformen Gestaltung und einem datenschutzgerechten Betrieb von Krankenhausinformationssystemen.	
Unter dem Begriff „Krankenhausinformationssystem (KIS)“ wird im Folgenden die Gesamtheit aller zur Verwaltung und Dokumentation von elektronischen Patientendaten eingesetzten informationstechnischen Systeme eines Krankenhauses verstanden.	Unter dem Begriff „Krankenhausinformationssystem (KIS)“ wird im Folgenden die Gesamtheit aller zur Verwaltung und Dokumentation von elektronischen Patientendaten eingesetzten informationstechnischen Systeme verstanden.	

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.	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.	
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.	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.	
Bei nicht erfüllten zwingenden Anforderungen an Konfiguration und Nutzung des KIS durch den Betreiber ist ein datenschutzkonformer Betrieb des KIS nicht gegeben.	Bei nicht erfüllten Muss-Anforderungen ist ein datenschutzkonformer Betrieb eines KIS nicht gegeben.	

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 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.	In die vorliegende Fassung sind weiterhin Anregungen und Kritik von Hersteller- und Betreiberseite eingeflossen.	

II. Technische Anforderungen		
1 Struktur der Daten im PAS	**1 Datenmodell**	
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.	Die Datenbasis eines PAS besteht aus Datenobjekten.	Verschobener Text aus 1.6 alt
1.1	**1.1**	
Jedes PAS, das in einem Umfeld eingesetzt wird, in dem es von mehreren rechtlich selbständigen Leistungserbringern genutzt werden soll, muss mandantenfähig sein. (Teil I, Tz. 32).	Jedes PAS muss mandantenfähig sein (Teil I Tz. 17,30,36).	

1.2		
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).	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).	
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.	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.	

1.4	**1.2**	
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).	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).	
1.5	**1.3**	
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 behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 15, 37)	Für Datenobjekte, welche Patienten betreffen, die ambulant in Nebentätigkeit eines privat liquidierenden Arztes oder stationär durch einen privat liquidierenden Chefarzt bzw. durch einen Belegarzt behandelt werden, muss die entsprechende Zuordnung in einem Statuskennzeichen ausgewiesen werden, sofern für den behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 30).	Alt: H Muss Neu: B Muss

1.6	**1.4**	
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).	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).	
1.7	**1.5**	
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).	Für jedes patientenbezogene Datum mus sich unabhängig vom Inhaltstyp bestimmen lassen, wer es wann erstellt und wer es wann wie modifiziert hat. Werden z.B aus Haftungsgründen Vidierungen (Freigabenachweise; Teil I, Tz. 10; vgl. auch Tz. 3.9) verwendet, muss sich für jedes hierfür vorgesehene Datum bzw. sachlich zusammenhängenden und gemeinsam zur Anzeige gebrachten Datensatz (Befund, Diagnose) erkennen lassen, ob er vidiert wurde und ggf. durch wen.	

1.8	1.6	
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.	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).	
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)	Beispiele für solche Datenobjekte sind Einzelbefunde, Einträge in die Pflegedokumentation, Einträge in die Liste der abrechenbaren Leistungen. PAS sollen eine Trennung von Patientenstammdaten und Daten der anderen Kategorien ermöglichen.	Teilweise verschoben in den einleitenden Absatz dieses Abschnitt und durch neuen Text ersetzt

	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.	
1.9	**1.8**	
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).	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).	

1.10	**1.9**	
	Für Datenobjekte innerhalb einer Fallakte soll die Möglichkeit bestehen, Kennzeichen zu setzen, das festhält, dass der Patient der Hinzuziehung dieser Vorbehandlungsdaten ganz oder teilweise widersprochen hat. Das Kennzeichen muss jederzeit wieder gelöscht werden können. Vergabe/Rücknahme des Kennzeichens sollen durch das Rollen- und Berechtigungskonzept geregelt werden (Teil I Tz. 4, 7).	Gestrichen
Das PAS muss die Möglichkeit bieten, einen Widerspruch des Patienten gegen die Hinzuziehung von Daten aus einer Vorbehandlung wirksam umzusetzen. (Teil I, Tz. 26).	Das PAS soll die Möglichkeit bieten, das Widerspruchskennzeichen in Abhängigkeit vom Verarbeitungskontext bei nachfolgenden Zugriffen anzuzeigen oder zu unterdrücken.	Neu: H Muss Alt: H Soll
1.11	**1.10**	
Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob für den Patienten eine Auskunftssperre gilt (Teil I, Tz. 4).	Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob und ab wann für den Patienten eine Auskunftssperre gilt (Teil I Tz. 6).	

1.12	**1.11**	
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.	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).	Alt: HB Muss Neu: H Soll
Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden. (Teil I, Tz. 41)	Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden.	
1.13	**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 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).	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).	Alt: H Muss Neu: HB Muss

Die Kennzeichen nach dieser Tz. und Tz. 1.12 können in einem Kennzeichen zusammengefasst werden.		Neu: HB Soll
1.14	**1.13**	
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).	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).	
1.15	**1.14**	
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).	Warnhinweise administrativer oder medizinischer Natur sollen nur mit einem (konfigurierbaren) Wertevorrat belegt werden können und nicht als Freitextfelder gestaltet sein (Teil I Tz. 3).	Alt H Soll Neu: HB Soll

1.16	**1.15**	
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).	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.	
2 Systemfunktionen	**2 Systemfunktionen**	
2.1	**2.1**	
Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren (Transparenz).	Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren.	

2.2	**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).	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.	
2.4	**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).	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).	

	2.5	
	Werden im Zuge des Datenaustauschs zwischen verschiedenen Komponenten des KIS Dienstleistungen externer Provider in Anspruch genommen, muss für eine Transportverschlüsselung gesorgt werden. Die Schlüssel dürfen sich nur in alleiniger Kontrolle des Krankenhauses befinden.	Verschoben nach 2.16 neu, 2.5 neu fehlt
2.6	**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).	Kennzeichen nach 1.2 bis 1.4 und 1.7 bis 1.11 sollen in den verschiedenen Komponenten des KIS abgebildet werden können, sofern sie für deren Nutzung nicht offensichtlich irrelevant sind. (Bsp: Eine Tumordokumentation muss keine Angaben über eine Auskunftssperre i.S.v. Teil I Nr. 6 enthalten.) Für die Kennzeichen nach 1.3 und 1.7 ist dies zwingend erforderlich (Teil I, Tz. 10).	
2.7	**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.	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).	

	2.8	
	Speichermedien, welche Daten des KIS aufnehmen, müssen eine Verschlüsselung ermöglichen (Datenträger- / Datenbank- / Dateisystem-verschlüsselung). Dies gilt insbesondere für Datensicherungen und Daten, welche sich auf mobilen Systemen befinden.	Verschoben in den Unterabschnitt „Verschlüsselung“ 2.17 neu und teilweise umformuliert
	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.	Verschoben in den Unterabschnitt „Verschlüsselung“ 2.18 neu
2.8	**2.9**	
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.	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.	

2.9	2.10	
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.	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.	
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).	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).	Alt: H Muss Neu: H Soll
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).	Das Krankenhaus muss einen Zeitraum von unter einem Jahr festlegen, nach dem abgeschlossene Fallakten gesperrt oder ausgelagert werden.	Letzter Absatz von 2.10 alt bildet 2.10 neu

2.11	**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).	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).	
2.12	**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).	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).	
2.14	**2.14**	
Im Zuge der Replikation des Datenbestandes soll es möglich sein, eine Pseudonymisierung etwa durch Ersatz der Identifikationsdaten mit Dummy-Daten durchzuführen. (Datensparsamkeit; Zugriffskontrolle / Vertraulichkeit)	Im Zuge der Replikation des Datenbestandes soll es möglich sein, eine Pseudonymisierung etwa durch Ersatz der Identifikationsdaten mit Dummy-Daten durchzuführen.	

2.15	**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)[1].	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)[2].	
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).		

[1] 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.

[2] 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.

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.		Verschoben aus 2.5 alt
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.		Verschoben aus 2.8 alt erster Absatz und umformuliert

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.		Verschoben aus 2.8 alt
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.		verschoben aus 7.12 alt

3 Anwendungsfunktionen	**3 Anwendungsfunktionen**	
	3.1	
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.	Anwender interagieren mit dem PAS innerhalb der ihnen zur Verfügung stehenden Verarbeitungskontexte durch Ausführung von Transaktionen[3] 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).	
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)	Die Verarbeitungskontexte müssen derart konfigurierbar sein, dass ein Verarbeitungskontext lediglich die Transaktionen zur Verfügung stellt, die zur Ausübung der funktionellen Rolle erforderlich ist, denen er zugeordnet ist.	

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

	• 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)	In den Anhang verschoben

	Für die Erfüllung der Aufgaben auf verschiedenen Funktionsebenen des Krankenhauses sollten verschiedene Verarbeitungskontexte abgebildet werden können	gestrichen
3.2	**3.2**	
	Bei Beginn der Sitzung und vor jeder Transaktion, deren Ausführung vom Verarbeitungskontext abhängt, muss es möglich sein einen Benutzerwechsel oder einen Wechsel des Verarbeitungskontexts zu vorzunehmen. Beachte jedoch 4.4. Ein Benutzerwechsel/Wechsel des Verarbeitungskontexts muss eine an den neuen Benutzer und dessen Zugriffsrechte angepasste Datenpräsentation und Anwendungsfunktionen zur Folge haben (Teil I, Tz. 10,18,21,24,27). Bei einem Wechsel der Verarbeitungskontexte kann ein Bezug der im alten Verarbeitungskontext geöffneten Fallakte (Fall-ID) an den neuen Verarbeitungskontext übergeben werden, sofern und soweit gewährleistet ist, dass diese Fallakte im neuen Verarbeitungskontext nur geöffnet wird, falls sie im Ergebnis einer im neuen Verarbeitungskontext zulässigen Suche oder Abfrage gefunden werden kann.	Teilweise verschoben nach 3.3 neu

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).		Verschoben aus 3.4 alt
3.3	**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.	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).	Alter Text gestrichen und teilweise ersetzt aus 3.2 alt

3.4	**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)	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).	Alt: HB muss Neu: H muss Verschoben nach 3.2 neu
3.5	**3.5**	
Das PAS muss über eine Funktion verfügen, mit der im Rahmen der Aufnahme eines Patienten eine Kurzübersicht mit den zugelassenen Daten zurück-liegender Behandlungsfälle erzeugt werden kann (Teil I, Tz. 1 - 3).	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).	

3.6	**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)	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.	3.6 alt gestrichen und ersetzt durch neues Kriterium 3.6 neu
	3.7	
	Übersichtslisten mit Patientendaten (etwa Stationslisten) müssen in Abhängigkeit vom Verarbeitungskontext konfigurierbar sein (Teil I, Tz. 10,18,21,24,27).	Zusammengefasst mit 3.4 neu
3.7	**3.8**	
Für Sonderzugriffe muss systemseitig die Eingabe einer Begründung gefordert werden können, ggf. auch im Nachhinein. (vgl. Tz. 4.9). (Teil I, Tz. 14)	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).	

3.8	**3.9**	
Ein PAS soll eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein. (Authentizität)	Ein PAS muss eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein.	
3.9	**3.10**	
Ein PAS soll es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9). (Authentizität)	Ein PAS muss es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9).	Alt: muss Neu: Soll
3.10	**3.11**	
Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden. (Teil I, Tz. 30, 31)	Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden.	
3.11	**3.12**	
Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 30, 31)[4].	Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 28)[5].	

[4] 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.

	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).	gestrichen
	3.14	
	Das PAS muss über eine Funktion verfügen, mit der eine Übersicht erstellt werden kann, welche Personen während der Dauer der Speicherung eines Behandlungsfalles auf diesen zugegriffen haben (vgl. Tz. 7). Soweit unter Berücksichtigung der unter Tz. 7.2/7.8 genannten Anforderungen lesende Zugriffe nicht protokolliert werden, muss die Übersicht erkennen lassen, welche Stellen grundsätzlich zugriffsberechtigt waren (Teil I Tz. 40).	Inhaltlich ähnlich 4.7 alt und deshalb mit 4.7 neu verschmolzen
	3.15	

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

	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.	gestrichen

3.12	**3.16**	
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)	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.	
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	4.1	
• 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) 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)	• 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 dem Ort des Zugreifenden, insbesondere im Verhältnis zum Patienten, • einem Dienst- oder Bereitschaftsplan, und • dem hinterlegten Behandlungspfad des Patienten zu erteilen (Teil II 4.8)	

4.2	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.)	Das Rollen- und Berechtigungskonzept muss grundsätzlich folgende Benutzerkategorien unterscheiden: - Ärztliche Mitarbeiter - Nicht-ärztliches medizinisches Fachpersonal (z.B. Pflegekräfte) - Verwaltungskräfte - Ausbildungskräfte - Externe Kräfte - Administration	

	4.3	
	Das Rollenmodell muss zumindest nach folgenden strukturellen Rollen differenzieren: - 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	gestrichen

4.3	**4.4**	
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.	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.	
4.4	**4.5**	
Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann. (Transparenz, Datenschutzkontrolle)	Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann.	
4.5	**4.6**	
Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen. (Transparenz, Datenschutzkontrolle)	Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen.	

4.6	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. Insbesondere muss es für ein gegebenes Datenobjekt effizient bestimmt werden können, welche Mitarbeiter darauf schreibend oder lesend zugreifen können. (Transparenz, Datenschutzkontrolle)	Das PAS muss über eine Funktion verfügen, die es erlaubt, für bestimmte Berechtigungen in einer Übersicht die Benutzer darzustellen, die über diese Berechtigung verfügen.	
4.7	**4.8**	
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)	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.	4.7 jetzt vollständig Musskriterium sowohl für H als auch für B

4.8		
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 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).		Verschoben aus 4.10 alt

4.9	**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). • 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.	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. • 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	

	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).	Verschoben nach 4.8 neu
4.10	**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 z. B. durch Präsenz eines maschinenlesbaren Mitarbeiterausweises, eines RFID-Tags oder eines vergleichbaren Tokens zu knüpfen (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit).	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).	

4.11	**4.12**	
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).	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).	
4.12	**4.13**	
Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben. (Zugriffskontrolle / Vertraulichkeit)	Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben.	

4.13	4.14	
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).	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).	
4.14	**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. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)	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.	

4.15	**4.16**	
Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Zugriffskontrolle / Vertraulichkeit).	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).	
4.16	**4.17**	
Die Benutzerverwaltung sollte über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Mitarbeitern automatisiert zu deaktivieren.	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).	
4.18	**4.19**	
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.	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.	

	4.20	
	Für ein gegebenes Datenobjekt muss effizient bestimmt werden können, welche Mitarbeiter darauf schreibend oder lesend zugreifen können.	Inhaltlich ergänzt in 4.10 neu
5 Datenpräsentation	**5 Datenpräsentation**	
5.1	**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).	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).	

5.2	**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)[6].	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)[7].	
5.3	**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.	Das PAS sollte die Oberflächen verschiedener Verarbeitungskontexte klar voneinander optisch (z.B. farblich) unterscheiden. Dies gilt insbesondere für die Oberfläche des Notfallzugriffs.	

[6] 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

[7] 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

5.4	**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.	Es muss die Möglichkeit bestehen Kennzeichen nach 1.2 bis 1.4 und 1.7 bis 1.12 in Bildschirmmasken zu integrieren.	
6 Systemzugang	**6 Nutzungsergonomie**	
6.3	**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)	Im PAS muss eine (arbeitsplatzabhängige) automatische Arbeitsplatzsperre eingerichtet werden.	

	6.5	
	Jedem Nutzer muss ein Standard-Verarbeitungskontext zugeordnet werden können (Teil I, Tz. 10,18,21,24,27).	
6.5	**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. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)	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.	
	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).	gestrichen

	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).	gestrichen
	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.	gestrichen
	6.10	

	Zur Interpretation und Zulässigkeitsprüfung von Datenzugriffen sollte das PAS eine transparente Verknüpfung von Protokolldaten, Inhaltsdaten und ggf. Dienstplänen ermöglichen.	gestrichen
	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.	gestrichen
	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.	gestrichen
	6.13	

	Durch Schulungen müssen die Beschäftigten regelmäßig für Datenschutzfragen sensibilisiert werden um sicher zu stellen, dass die Sicherheitsfunktionen des KIS ordnungsgemäß genutzt werden.	gestrichen
7 Protokollierung / Auswertung von Protokolldaten	**7 Protokollierung**	
Die Vorgaben in diesem Kapitel dienen der Umsetzung der in Teil I, Tz. 43 bis 45 und 47 aufgeführten Anforderungen.		
7.1	**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.	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).	

7.3	7.2	
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.	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.	

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.	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.	
7.4	**7.3**	
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.	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).	
	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).	Satz 1 gestrichen. Satz 2 integriert in 7.2 neu
7.5	**7.9**	
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.	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).	

	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).	
7.6	**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.	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.	

7.7	**7.7**	
Vorgesehene Protokollierungen dürfen nicht umgangen werden können.	Protokollfunktionen müssen revisionssicher ausgestaltet sein, d.h., vorgesehene Protokollierungen dürfen nicht umgangen werden können und	
7.8		
Eine nachträgliche Veränderung von Protokolldaten darf nicht möglich sein.	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).	
7.9		
Protokolle sollen so konfigurierbar sein, dass sie keine medizinischen Daten enthalten. (Datensparsamkeit / Vertraulichkeit)		Verschoben aus 7.11 alt

7.10	7.8	
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: - 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).	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 - 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)	Alt: H Muss Neu: HB muss

7.11	**7.10**	
Ist für die Ausführung einer Transaktion die Eingabe einer besonderen Begründung vorgesehen (vgl. Tz. 4.9) muss diese von der Protokollierung erfasst werden.	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).	
	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.	Erster Satz nach 7.9 neu verschoben
7.12	**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)		Verschoben aus 8.9 alt

	Das Rollen- und Berechtigungskonzept muss es erlauben, den Zugriff auf Protokolldaten zu beschränken.	Verschoben nach 7.18 neu und ergänzt
	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.	Verschoben in den UA Verschlüsselung 2.19 neu
7.13	**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).		Verschoben aus 8.5 alt

	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.	Inhaltlich nach 7.19 neu verschoben
7.14	**7.14**	
Hierzu müssen die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festgehalten werden (Teil I, Tz. 40).	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).	Gestrichen und ersetzt durch Absatz aus 8.5 alt

	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.	gestrichen
	7.16	
	Der konkrete Umfang der Protokollierung muss im Rahmen der Grundkonfiguration des Verfahrens mit dem behördlichen/betrieblichen Datenschutzbeauftragten des Krankenhauses abgestimmt werden.	Inhaltlich in 7.2 neu enthalten

	7.17	
	Neben der Anmeldung am Verfahren (Login/Logout) müssen insbesondere Aufrufe von Transaktionen bzw. Reports zu folgenden Datenkategorien protokolliert werden : - Datensätze besonderer Personengruppen (z.B. Mitarbeiterdaten, VIPs), soweit besonders gekennzeichnet, - Daten außerhalb des primären Zuständigkeitsbereichs des Benutzers, - abgeschlossene Fälle, - Rückweisungen aufgrund fehlender Berechtigungen, - Datenexporte; (Teil I Tz. 25, 37).	Gestrichen, da bereits in 7.8 alt und 7.10 neu enthalten
7.16	**7.19**	
Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten auswerten zu können.	Es müssen geeignete Mechanismen zur Verfügung stehen, um die Protokolldaten auswerten zu können.	

Hierzu sollen im Verfahren selbst Auswertungsmöglichkeiten und ein Datenschutzarbeitsplatz vorgesehen werden.	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).	
	7.20	
	Es muss eine Auswertung möglich sein, welche Benutzer wann mit welchen Rechten eingerichtet worden sind.	Inhaltlich mit 7.21 alt in 7.17 neu zusammengefasst

7.17	**7.21**	
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.	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.	Inhaltlich Übernahme auch aus 7.20 alt
	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.	gestrichen

	Krankenhäuser müssen die vorbeugende Datenschutzkontrolle in ihrem Protokollierungskonzept berücksichtigen, und datenschutzrechtliche Auffälligkeits- und Stichprobenauswertungen vorsehen, zumindest insoweit, wie das Berechtigungskonzept unberechtigte Zugriffe nicht ausschließt. Eine (teil-)automatisierte Protokollauswertung mit Benachrichtigungsfunktion sollte ermöglicht werden.	Verschoben nach 7.20 neu
7.18	**7.23**	
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.	Im Rahmen der Zugriffskontrolle muss gewährleistet sein, dass eine Einsichtnahme nur den Personen möglich ist, in deren Aufgabenbereich Auswertungen von Protokolldaten fallen.	
7.19		
Zugriffe auf Protokolldaten sollten nur nach dem Vier-Augen-Prinzip und unter Beteiligung eines Datenschutzverantwortlichen erfolgen.		Zusammengefasst aus 7.13 alt

7.20		
Krankenhäuser müssen Auffälligkeits- und Stichpro-benauswertungen der Zugriffsprotokolle vorsehen.		Verschoben aus 7.22 alt
Die Protokolle über Sonderzugriffe unter Verwendung eines Verfahrens nach Tz. 4.9 müssen dabei mit einer angemessenen Prüfdichte einbezogen werden,		
7.21	**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. Gleiches gilt für Zugriffe, die im Rahmen der Fernwartung erfolgt sind.	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.	
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.		Verschoben aus 8.10 alt

	7.25	
	Für Protokolldaten, die nicht im unmittelbaren Zugriff stehen müssen, sollte über ein Archivierungskonzept eine Auslagerung vorgesehen werden.	gestrichen
8 Technischer Betrieb, Administration	**8 Technischer Betrieb, Administration**	
8.1	**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).	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).	
8.2	**8.2**	
Das Krankenhaus muss sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann (Teil I, Tz. 40).	Das Krankenhaus muss sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann (Teil I, Tz. 33).	

8.3		
Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 40).	Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 33).	
8.4	**8.3**	
Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können, wobei die Systemkonsistenz zu wahren ist. (Weitergabekontrolle / Vertraulichkeit)	Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können (Teil I, Tz. 33).	
8.5	**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. 40).	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).	

	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).	Verschoben nach 7.13 neu
	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.	Verschoben nach 7.14 neu
8.6	**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).	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).	

	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.	
8.7	**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 und, soweit sie die Informationssicherheit betreffen, auf der Grundlage der IT-Grundschutzstandards 100-1 bis 100-4 des BSI im Informationssicherheitskonzept festgelegt werden.	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.	

	8.9	

	Aufgrund der Reichweite administrativer Funktionen bedarf ihre Nutzung einer besonderen Kontrolle. Die Protokollierung von Zugriffen im Rahmen der technischen und fachlichen Verfahrensbetreuung muss alle Zugriffe erfassen, die Auswirkungen auf Art oder Umfang der Verarbeitung personenbezogener Daten haben, insbesondere: Maßnahmen der Installation / Deinstallation von Software, - Änderungen der Anwendungskonfiguration (z.B. Festlegen von Residenzzeiten / Löschfristen, Login-Parametern, Anzeigeparametern, usw.), - Zugriffe im Rahmen einer etwaigen Mandantenverwaltung, - die Anlage, Änderung und Löschung von Rollen, - die Vergabe, Änderung und Löschung von Berechtigungen, - die Administration von Benutzern (Anlage, Sperre, Löschung, Rollenzuweisung), -die Einrichtung / Änderung standardmäßig vorgegebener Auswertungs-möglichkeiten (Reports), -der Import / Export von Datenbeständen, -Datenübermittlungen, -Prozesse zur Aggregierung, Pseudonymisierung / Anonymisierung von Datenbeständen (Date Warehouse), -Archivierungen / Datensicherungen;	Teilweise verschoben nach 7.12

	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.	Verschoben nach 7.22 neu