Orientierungshilfe Krankenhausinformationssysteme

Stand März 2014

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

Vorwort zur 2. Fassung der Orientierungshilfe

Gesundheitsdaten sind sensible personenbezogene Daten, die als solche ebenso wie etwa Angaben zur religiösen Überzeugung oder über politische Meinungen einen besonderen Rechtsschutz genießen. Die Digitalisierung im Gesundheitswesen bietet neben Chancen für eine effizientere Gesundheitsversorgung auch Risiken für die schutzwürdigen Interessen von Patienten. Speziell für den Bereich der Krankenhausinformationssysteme haben deshalb nach einer initialen Entschließung 2008 die Datenschutzbeauftragten des Bundes und der Länder sowie kirchliche Datenschutzbeauftragte 2011 die von der dafür eingesetzten Arbeitsgruppe erarbeitete „Orientierungshilfe Krankenhausinformationssysteme" herausgegeben. Diese Orientierungshilfe soll es Betreibern und Herstellern von Krankenhausinformationssystemen erleichtern, den gesetzlichen Anforderungen und den gerechtfertigten Erwartungen der Patienten im komplexen System Krankenhaus gerecht zu werden.

Die Orientierungshilfe ist bei den betroffenen Verbänden durchweg auf Interesse gestoßen, hat aber bei einigen Krankenhausbetreibern und Herstellern von Krankenhausinformationssystemen auch Kritik hervorgerufen. In der Folge wurden seitens der Arbeitsgruppe die Stellungnahmen von Betreibern in öffentlich-rechtlicher, privater und kirchlicher Trägerschaft und ihren Verbänden sowie von einzelnen Krankenhausgesellschaften ausgewertet, Pilotprojekte zur Umsetzung der technischen Anforderungen aus der Orientierungshilfe begleitet und in verschiedenen Foren ein reger Austausch mit Vertretern der Hersteller und Betreiber geführt.

Ende 2012 fasste die Arbeitsgruppe auch nach Auswertung der Erfahrungen aus der Kontroll- und Beratungstätigkeit ihrer Mitglieder den Beschluss, die Orientierungshilfe zur Klarstellung einiger der fixierten Anforderungen und im Sinne einer besseren Lesbarkeit und Übersichtlichkeit zu überarbeiten. Parallel hierzu stand die Arbeitsgruppe in intensivem Austausch mit der Deutschen Krankenhausgesellschaft (DKG) und einigen Landeskrankenhausgesellschaften. Die hier gewonnenen Erkenntnisse flossen zum einen in die überarbeitete Fassung der Orientierungshilfe ein, zum anderen aber auch in ein Grundsatzpapier der DKG mit Hinweisen und Musterkonzepten für die Umsetzung der technischen Anforderungen der Orientierungshilfe, dessen Lektüre hier ausdrücklich empfohlen wird.[1]

Die nun vorliegende überarbeitete Fassung hat eine durchgehende redaktionelle Überarbeitung erfahren. Um Verständnisschwierigkeiten zu begegnen, wurde Teil I (Rechtliche Rahmenbedingungen) präzisiert. Speziell für einrichtungs- und mandantenübergreifende Zugriffe wurde zusätzlich ein Szenarienkatalog

[1] http://www.dkgev.de/dkg.php/cat/129/aid/11661/title/Hinweise_und_Musterkonzepte_fuer_die_Umsetzung_der_technischen_Anforderungen_der_%E2%80%9EOrientierungshilfe_Krankenhausinformationssysteme%E2%80%9C

bereitgestellt. In Teil II (Technische Anforderungen) der Orientierungshilfe wurde der durchgehende Bezug zu den rechtlichen Rahmenbedingungen verdeutlicht. Insgesamt wird nun klarer, dass den rechtlichen Anforderungen durch verschiedenartige System- und Prozessgestaltung entsprochen werden kann.

Mit dieser überarbeiteten Fassung der Orientierungshilfe werden keine neuen Themenbereiche erschlossen oder die Anforderungen der Ursprungsfassung revidiert. Statt dessen ist die Intention der Arbeitsgruppe, den Herstellern und Betreibern von Krankenhausinformationssystemen eine für die Praxis besser handhabbare Handreichung für die datenschutzgerechte Gestaltung und Nutzung von Krankenhausinformationssystemen zu bieten.

Begleitpapier zur Orientierungshilfe „Krankenhausinformationssysteme“

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

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

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

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

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

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

Glossar zur Orientierungshilfe Krankenhausinformationssysteme

Alias

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

Anonymisierung

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

Archiv (Altfälle)

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

Behandlungsfall

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.

Fallakte

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

Funktionsbezogene Organisationseinheit

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

Identifikationsdaten

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

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.

Krankenhausinformationssystem (KIS)

Unter dem Begriff „Krankenhausinformationssystem (KIS)“ wird die Gesamtheit aller in einem →*Krankenhaus* eingesetzten informationstechnischen Systeme zur Verwaltung und Dokumentation →*elektronischer Patientendaten* verstanden. Dabei handelt es sich in aller Regel um

einen Verbund selbständiger Systeme meist unterschiedlicher Hersteller. Auf einzelne Fachbereiche beschränkte Verfahren wie z.B. Labor-, Radiologie- oder Diagnosesysteme gehören als Subsysteme ebenfalls zum Krankenhausinformationssystem.

Löschung

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

Mandantenfähigkeit

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

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.

Patientenaktensystem (PAS)

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

Pseudonym

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

Pseudonymisierung

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

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

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

Rolle

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

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.

Temporäres Patientenkennzeichen

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

Trennung von Datenbeständen

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

Verarbeitungskontext

Als Verarbeitungskontext wird der sachliche und technische Zusammenhang bezeichnet, in dem Nutzer des KIS in einer bestimmten funktionellen Rolle Patientendaten verarbeiten. Verarbeitungskontexte leiten sich aus den Verarbeitungszwecken ab und verfeinern diese. Beispiele für Verarbeitungskontexte sind Behandlung eines der eigenen OE zugeordneten Patienten, Pflege eines Stationspatienten, OP-Assistenz, DRG-Controlling usw. Ein Verarbeitungskontext wird im PAS über kontextbezogene Benutzerrollen, Daten- und Funktionszugriffe und Bildschirmmasken abgebildet. So unterscheidet sich z.B. eine Suchfunktion bzw. die Präsentation von deren Ergebnissen im Verarbeitungskontext „Patientenaufnahme“ von der des Verarbeitungskontextes „Behandlung“.

Vertretung

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

Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen

Version 2 mit Stand vom März 2014
(korrigiert)

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

Aufnahme

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.

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 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.

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.

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.

Behandlung

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

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.

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.

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.

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 eigenen Behandlung) noch erforderlich ist.

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.

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.

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.

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 den pflegerischen Stationsdienst

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.

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.

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.

Zugriffe außerhalb der bettenführenden Fachabteilungen

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 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 sichergesellt sein, dass die einzelnen Schreibkräfte jeweils nur einer bestimmten Funktionseinheit mit entsprechenden Zugriffsrechten zugeordnet sind.

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.

Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls

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.

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

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 für Abrechnung, Controlling, Qualitätssicherung und Ausbildung

28. Die Krankenhausverwaltung / Abrechnungsabteilung darf nur Zugriff auf die für sie erforderlichen Patientendaten (Stammdaten, Diagnosen, Leistungen usw.) haben.

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.

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

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.

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.

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.

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

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.

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.

Technische Administration

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.

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.

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

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.

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

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.

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.

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

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.

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 Fachabteillung A).

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.

Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

Version 2, Stand vom März 2014

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

I. Vorbemerkung

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

Bei den 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 Datenschutzbeauftragten des Bundes und der Länder zur Protokollierung in zentralen Verfahren der Gesetzlichen Krankenversicherung[2] übernommen, soweit sie inhaltlich auf den Einsatz von Krankenhaussystemen übertragbar waren. Diese Protokollierungsanforderungen behandeln die aus Datenschutzsicht relevanten Aspekte; Protokollierungen, die im Rahmen des technischen Verfahrensbetriebs erfolgen und z. B. Betriebsparameter erfassen, werden nicht betrachtet.

Soweit konkrete Vorgaben zur Gestaltung oder Konfiguration gemacht werden, sind diese als musterhafte Umsetzungen zu verstehen, die aus 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.

---

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

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

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

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

Die Anforderungen werden daher nach drei Kategorien unterschieden:

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

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

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.

II. Technische Anforderungen

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 selbständigen Leistungserbringern genutzt werden soll, muss mandantenfähig sein. (Teil I, Tz. 32).	H	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	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
1.4	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
1.5	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 behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 15, 37)	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
1.7	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
1.8	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.	H	Muss
	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)	B	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	HB	Muss

	Methode bereitstellen, mit welcher festgestellt werden kann, ob die Fallakte gesperrt ist. (Teil I, Tz. 24).		
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
1.11	Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob für den Patienten eine Auskunftssperre gilt (Teil I, Tz. 4).	H	Muss
1.12	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.	H	Soll
	Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden. (Teil I, Tz. 41)	B	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
1.14	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
1.15	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 B	Soll Soll
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

2.1	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 (Datensparsamkeit). Soweit eine redundante Datenhaltung unvermeidbar ist, müssen Zugriffsbeschränkungen und Löschungen in allen betroffenen Datenbeständen berücksichtigt werden (Teil I, Tz. 22, 27).	H HB	Sollte Muss
2.3	In das KIS sollte ein Single-Sign-On-Dienst integrierbar sein.	H	Sollte
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
2.6	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).	HB	Soll
2.7	Berechtigungen auf Datenobjekte und ggf. Funktionen sollten in den verschiedenen Komponenten des KIS in gleicher Weise abgebildet werden können, jedenfalls insoweit sich die Nutzermengen überschneiden.	H	Sollte
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
2.9	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
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 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. 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).	H	Muss
	Sperr- und Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Mitarbeitern eingesetzt werden.	B	Muss
2.14	Jede Komponente eines PAS soll eine effiziente Replikation des Datenbestandes in ein Testsystem ermöglichen, das zur Fehlersuche und zum Test von Maßnahmen der Fehlerbehebung dient. Im Zuge der Replikation des Datenbestandes soll es möglich sein, eine Pseudonymisierung etwa durch Ersatz der Identifikationsdaten mit Dummy-Daten durchzuführen. (Datensparsamkeit; Zugriffskontrolle / Vertraulichkeit)	H	Soll
2.15	In das KIS muss ein Pseudonymisierungsdienst eingebunden werden, der verwendungszweckspezifisch temporäre Patientenkennzeichen oder Pseudonyme auf der Basis der gespeicherten Identitätsdaten generiert und verwaltet (Teil I, Tz. 30, 31)[3].	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

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

2.17	Speichermedien, welche Daten des KIS aufnehmen und nicht fest installiert sind, müssen verschlüsselt werden (durch Datenträger- oder Dateisystem-verschlüsselung). 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 B	Muss 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
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

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	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
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).	B	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
3.4	Ein PAS muss es ermöglichen, die Bearbeitungs- und Recherchefunktionen einschließlich der angebotenen Suchattribute und im Ergebnis anzuzeigenden	H	Muss

	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)		
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 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)	H	Soll
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
3.8	Ein PAS soll eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein. (Authentizität)	H	Soll
3.9	Ein PAS soll es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9). (Authentizität)	H	Soll
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
3.11	Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 30, 31)[4].	HB	Soll
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

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

[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.

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 (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 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
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

4.4	Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann. (Transparenz, Datenschutzkontrolle)	B	Muss
4.5	Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen. (Transparenz, Datenschutzkontrolle)	H	Muss
4.6	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
4.7	Das PAS muss über Funktionen verfügen, mit denen ein Behandlungsfall	H	Muss
	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	Muss
	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)		
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).	H	Muss Sollte
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).	HB	Muss
	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.)	H B	Muss Soll
	Auf die Erweiterung der Zugriffsrechte und die Protokollierung des Zugriffs (vgl. 7.11) soll zuvor hingewiesen werden.	H B	Muss Soll

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
4.11	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
4.12	Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben. (Zugriffskontrolle / Vertraulichkeit)	H	Muss
4.13	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
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
4.15	Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Zugriffskontrolle / Vertraulichkeit).	H	Muss
4.16	Die Benutzerverwaltung sollte über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Mitarbeitern automatisiert zu deaktivieren.	HB	Sollte
4.17	Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer für einen festgelegten Zeitraum keine Anmeldung mehr erfolgt ist.	H	Sollte
	Diese Funktion dient der Datenschutzkontrolle durch die Aufsichtsbehörden und die betrieblichen/behördlichen Datenschutzbeauftragten der Krankenhäuser. Einer missbräuchlichen Nutzung durch den Arbeitgeber muss durch das Berechtigungskonzept bzw. geeignete organisatorische Maßnahmen begegnet werden.	B	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

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. (Teil I, Tz. 30 und 31).	H	Muss
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)[5].	HB	Soll
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 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

6 Systemzugang

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

[5] 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

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
6.5	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 H	Sollte Muss

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.

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
7.3	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

7.4	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
7.5	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 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	Vorgesehene Protokollierungen dürfen nicht umgangen werden können.	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
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
7.11	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

7.12	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
7.15	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
7.16	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
7.17	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
7.18	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
7.19	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
7.21	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

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 sollten unterschiedlichen Personen zugewiesen werden (Teil I, Tz. 38).	B	Muss Sollte
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
8.3	Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 40).	H	Soll
8.4	Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können, wobei die Systemkonsistenz zu wahren ist. (Weitergabekontrolle / Vertraulichkeit)	H	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
8.6	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	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

III. Anhang

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.
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

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
    - 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

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

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 selbständige 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, 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 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 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 geführte Verarbeitungsprotokoll aufzunehmen.