DEUTSCHE
KRANKENHAUS
GESELLSCHAFT

Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme

2. überarbeitete Fassung

25. März 2014

Status: freigegeben

Kategorie: verbandsintern

Verteiler: Mitgliedsverbände, Fachausschuss

Inhaltsverzeichnis

Hinweis:

Das Dokument konzentriert sich auf thematische Schwerpunkte für die Umsetzung der Orientierungshilfe KIS.

Technischer Datenschutz im Krankenhaus

Mit der Veröffentlichung einer „Orientierungshilfe Krankenhausinformationssysteme“ im Herbst 2011 durch die Unterarbeitsgruppe Krankenhausinformationssysteme der Datenschutzbeauftragten des Bundes und der Länder wurde eine intensive und teilweise kontroverse Diskussion zu einheitlichen Vorgaben angestoßen, wie Patientendaten im Krankenhaus wirksam vor unbefugtem Zugriff geschützt werden müssen.

Inzwischen ist die Orientierungshilfe überarbeitet und Ende März 2014 in einer 2. Fassung herausgegeben worden. Im Vorfeld der Überarbeitung stand die DKG in intensivem Austausch mit der entsprechenden Unterarbeitsgruppe der LfDI (UAG). Die hier gewonnenen Erkenntnisse flossen sowohl in die überarbeitete Fassung der Orientierungshilfe als auch in die vorliegende Überarbeitung der DKG-Hinweise ein.

Informationsverarbeitende Systeme unterstützen die Behandlungsprozesse im Krankenhaus inzwischen in einem hohen Maße, dies wird künftig zunehmen. Dabei werden bei der administrativen Patientenaufnahme, der ärztlichen und pflegerischen Anamnese, bei der Dokumentation der Behandlung und Befundung (z. B. Labor- oder Röntgenbefunde) sowie der Pflege in der Pflegeeinheit bis hin zum Entlassbrief personenbezogene Daten erhoben und verarbeitet, die datenschutzrechtlichen Bestimmungen unterliegen. Der Schutzbedarf dieser personenbezogenen Daten erfordert wirksame technische und organisatorische Maßnahmen, damit eine unbefugte Kenntnisnahme oder Weitergabe ausgeschlossen ist.

Die Mitarbeiterinnen und Mitarbeiter des Krankenhauses müssen über alle im Rahmen der Behandlung des Patienten bedeutsamen Informationen verfügen, um ihre Tätigkeiten frei von Behinderungen ausführen zu können. Maßnahmen zur Gewährleistung des Datenschutzes müssen daher in die Abläufe im Krankenhaus integriert werden können. Insbesondere ist zu beachten, dass Mitarbeiterinnen und Mitarbeiter des Krankenhauses in ihrer täglichen Arbeit eine hohe Verantwortung gegenüber den Patienten tragen. Ein Klima des Misstrauens oder ein „Generalverdacht“ sind hier nicht gerechtfertigt, für die Akzeptanz der Maßnahmen ist die Transparenz der Regelungen maßgeblich.

Die „Orientierungshilfe Krankenhausinformationssysteme“ zielt in Teil II „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ darauf ab, konkrete „Maßnahmen zur technischen Umsetzung der bestehenden datenschutzrechtlichen Regelungen und Vorgaben zur ärztlichen Schweigepflicht beim Einsatz von Krankenhausinformationssystemen“ für die Hersteller und Betreiber zu formulieren. Die einzelnen technischen Anforderungen und ihre gehäufte Wiederholung in kontextuellen Variationen wirken sich jedoch nachteilig auf das Verständnis des Dokuments aus.

Das Dokument erweckt den Eindruck, es würde das Ziel verfolgt, eine technische Spezifikation eines Krankenhausinformationssystems vorzulegen. Tatsächlich könnte das Dokument auch als Prüfliste für die datenschutzrechtliche Überprüfung von bestehenden Installationen in Krankenhäusern genutzt werden, bei der das Vorhandensein konkreter, „spezifizierter“ technischer Ziele auf eine einfach abfragbare Ja-/Nein-Liste reduziert.

Die technischen Anforderungen sind Ausdruck einer Regulierung von technischen Implementierungsdetails, die wohl besonders dazu dient, Prüfungen unterstützen zu können. Das Krankenhaus muss ohne Frage erwarten können, dass eine gleichwertige, aber andere technische Lösung nicht zu seinen Lasten geht. Ein allseits anerkanntes Verfahren besteht darin, die gewollte Funktion eindeutig zu bestimmen, die technische Umsetzung aber nicht einseitig vorzugeben, sondern denen zu überlassen, deren Geschäft und Expertise gerade in der technischen Umsetzung besteht. In der Überarbeitung der Orientierungshilfe wurde diesem Aspekt in einzelnen Punkten

Rechnung getragen und einige Regelungsdetails zugunsten allgemeinerer Lösungsansätze ersetzt.

Die hier formulierten Hinweise zum technischen Datenschutz greifen die „Orientierungshilfe Krankenhausinformationssysteme“ nicht teilzifferbezogen auf, sondern formulieren aus Sicht der Autoren maßgebliche Hinweise zu Anforderungen an die Umsetzung des technischen Datenschutzes im Krankenhaus. Insbesondere sollen die Hinweise Krankenhäusern bei der praktischen Umsetzung der OH KIS als Hilfestellung dienen.

Die Hinweise sind dabei im Wesentlichen in den folgenden Teilkonzepten enthalten:

- Rollen- und Berechtigungskonzept (Zugriffskontrolle),
- Protokollierung,
- Zugriffsbeschränkungen auf Patientendaten,
- Löschen von Patientendaten

Darüber hinaus werden Sonderthemen, wie die Einbeziehung von Vorbehandlungsdaten, die Verschlüsselung von Daten oder Schutzmaßnahmen für besondere Patientengruppen (VIP, Mitarbeiter als Patienten) aufgegriffen. Der Anhang enthält Mustervorlagen für einzelne Teilkonzepte (Zugriffsbeschränken/Auslagern von Daten, Löschen von Patientendaten).

1 Rollen- und Berechtigungskonzept (Zugriffskontrolle)

Das Rollen- und Berechtigungskonzept (RBK) ist die datenschutzrechtliche Maßnahme des Krankenhauses, um „zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder entfernt werden können (Zugriffskontrolle)“ (Anlage zu § 9 Satz 1 BDSG).

Das Rollen- und Berechtigungskonzept des Krankenhauses muss eine zuverlässige Zugriffskontrolle durch Eingrenzung des Kreises der zugriffsberechtigten Mitarbeiter, die bei der Wahrnehmung ihrer Aufgaben auf Patientendaten zugreifen müssen, ermöglichen.

Das Rollen- und Berechtigungskonzept muss von der Geschäftsführung und dem IT-Verantwortlichen verbindlich festgelegt werden. Es ist mit den zuständigen Beteiligten im Krankenhaus, insbesondere den leitenden Abteilungsärzten abzustimmen und soll die tatsächlichen Berechtigungen und Abläufe bei Zugriffen auf Patientendaten im Behandlungskontext möglichst vollständig abbilden.

Folgende Personen/Rollen sollen bei der Entwicklung des Rollen- und Berechtigungskonzepts eingebunden sein:

- Verantwortlicher für IT-Sicherheit,
- Datenschutzbeauftragter des Krankenhauses,
- Mitarbeitervertretung,
- Berechtigungsverwaltung (IT-Administration).

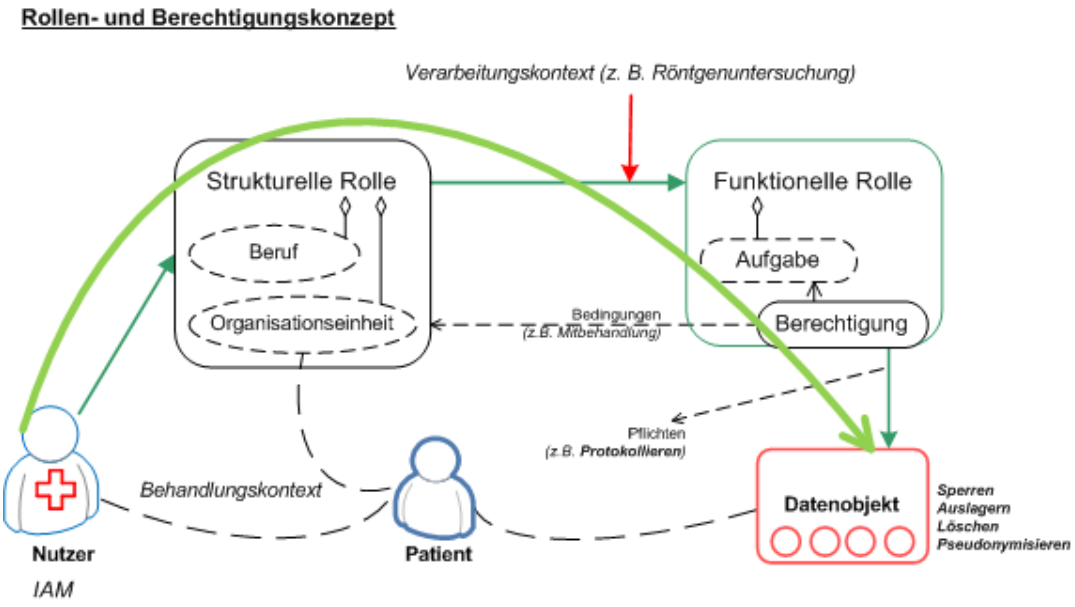
Bei der Ausgestaltung des Rollen- und Berechtigungskonzepts ist zu berücksichtigen, dass es nicht zu einer Kultur des Misstrauens und der Verdächtigung kommt. Die Mitarbeiter setzen das Leitbild des Krankenhauses mit großem persönlichem Einsatz um und stellen das Wohl des Patienten in den Mittelpunkt ihrer Arbeit. Die Wahrung des Vertrauensverhältnisses ist nicht nur eine arbeitsvertragliche Pflicht, sie wird durch klare Abgrenzung der Aufgaben und Verantwortung auch organisatorisch unterstützt. Technische Schutzmaßnahmen für Zugriffsrechte unterstützen dies. Sie geben den Mitarbeitern auch die Gewissheit, dass das Vertrauensverhältnis nicht durch unzulänglichen Schutz der Patientendaten gefährdet wird.

1.1 Vorgehen zur Festlegung der Rollen und Zugriffsrechte

Die Festlegung der erforderlichen Rollen und Zugriffsrechte hängt in ihrer konkreten Ausgestaltung von den Gegebenheiten des Krankenhauses ab. Für die Erarbeitung und Pflege des Katalogs der rollenbasierten Zugriffsrechte sind jedoch grundsätzlich in jedem Krankenhaus folgende Maßnahmen erforderlich:

1. Vollständige Auflistung aller **Organisationseinheiten**, in denen Mitarbeiter in Wahrnehmung ihrer Arbeitsaufgaben Patientendaten nutzen müssen,
2. Vollständige Zuordnung aller **Mitarbeiter** zu den Organisationseinheiten,
3. Vollständige Auflistung aller **Aufgaben** der Mitarbeiter in der Organisationseinheit unter Berücksichtigung ihrer beruflichen Qualifikation und Stellung innerhalb der Aufbau- und Ablauforganisation,
4. Vollständige Auflistung und Kategorisierung aller für die Aufgabenwahrnehmung benötigten **Patientendaten** („Datenobjekte“) mit ihrer konkreten Präsentationsform (z. B. Bildschirmmaske, Berichtsdokument, Einzelmerkmal),

5. Festlegung der erforderlichen **Zugriffsmethoden** (z. B. Erstellen, Schreiben, Ändern, Lesen).



Die Erteilung von Zugriffsrechten auf Patientendaten erfolgt grundsätzlich nicht personenbezogen, sondern durch Zuweisung der jeweiligen Mitarbeiter zu personenunabhängigen Rollen, denen aufgabenbezogen Zugriffsrechte eingeräumt werden.

Die berufliche Qualifikation (z. B. Arzt) und Zugehörigkeit zu einer Organisationseinheit (z. B. Fachabteilung Chirurgie) definiert die „strukturelle Rolle“ (z. B. Arzt in der Chirurgie), die die Wahrnehmung einer konkreten Aufgabe (funktionelle Rolle) ermöglicht. Funktionelle Rollen definieren die Beteiligung an der Behandlung eines Patienten und damit das Recht, Einblick in die Patientendaten im benötigten Umfang zu nehmen oder die Patientendaten durch eigene Einträge fortzuschreiben.

Die Berechtigungen selbst können an Bedingungen geknüpft sein, wie z. B. einen Auftrag zur Befundung/Mitbehandlung. Sie können auch zeitlich befristet sein, sowie die Erfüllung bestimmter Pflichten auslösen, z. B. Protokollierung des Zugriffs, ggf. ergänzt durch Eingabe einer besondere Begründung.

Weiter können organisatorische Maßnahmen dazu beitragen, das Rollen- und Berechtigungskonzept durchzusetzen, z. B. durch die zeitnahe Datenschutzauswertung von (geschützten) Protokollen in kontrollierter, datenschutzkonformer Form, die die Erstellung von Auswertungen über die protokollierten Mitarbeiter, insbesondere von Tätigkeitsprofilen, sicher ausschließt.

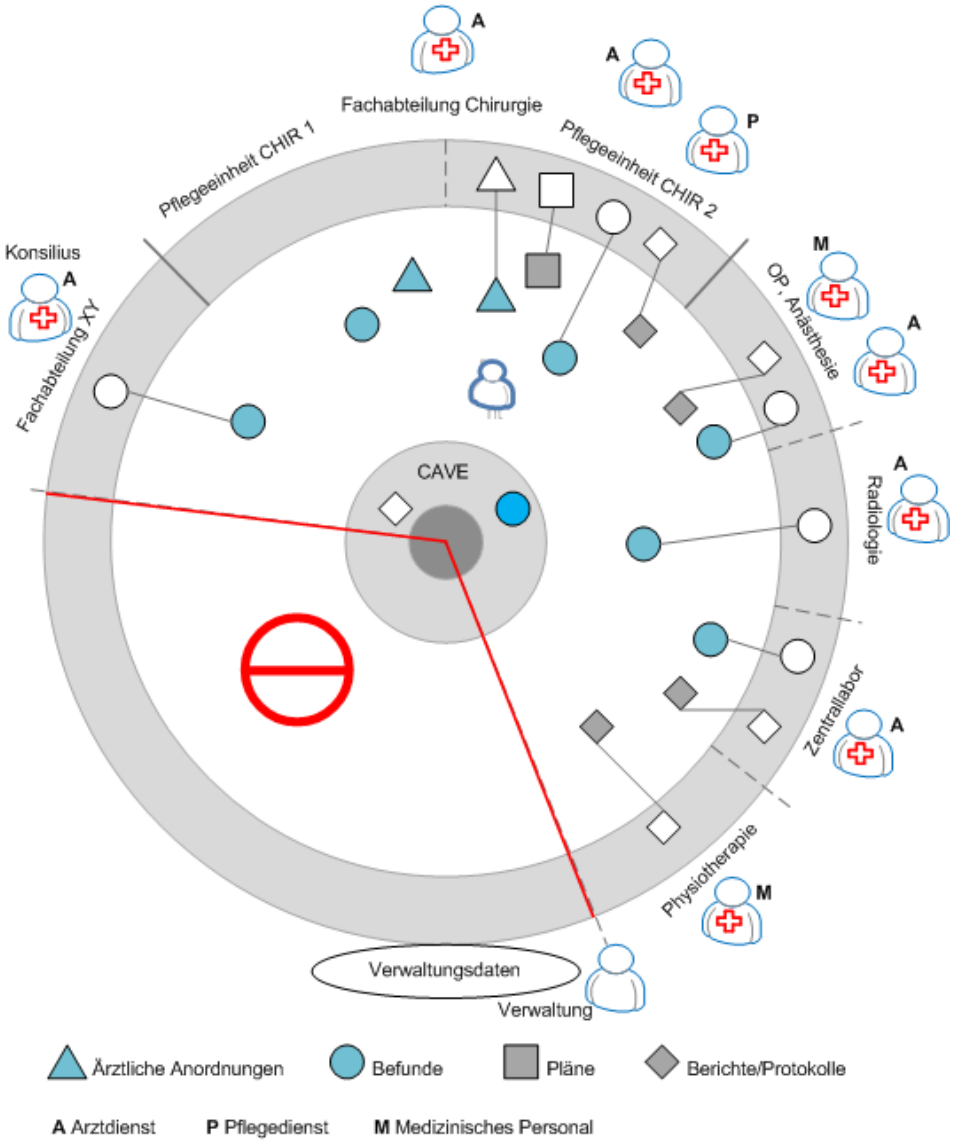
1.2 Patientendaten und Zugriffsmethoden

Jeder Patient hat im Krankenhaus einen Datenbereich, den man sich als segmentierten Kreis mit Kreisringen vorstellen kann.

Im Mittelpunkt befinden sich Patientenstammdaten, die zur Feststellung der Identität des Patienten allen Mitarbeitern zur Verfügung stehen müssen, die patientenbezogen Aufgaben in Bezug auf den Krankenhausaufenthalt wahrnehmen.

Die Patientenstammdaten sind umgeben von wichtigen medizinischen Informationen, z. B. über bekannte Allergien oder Arzneimittelunverträglichkeiten des Patienten. Diese Daten, müssen zur Vermeidung von Zwischenfällen allen medizinischen Mitarbeitern zur

Verfügung stehen (sog. „CAVE-Daten“, die sowohl dem Schutz der Patienten als auch dem Schutz der Mitarbeiter dienen). Der Zugriff auf diese Daten ist nur im Bedarfsfall zulässig. Das Krankenhaus muss Prinzipien der Zuordnung von Daten zu „CAVE-Daten“ festlegen. Die Zugriffsberechtigung auf diese Daten ergibt sich in der Regel aus den Berechtigungen zum Zugriff auf umfassendere Teile der Patientenakte, eine separate Berechtigung zum Zugriff ist daher regelhaft nicht erforderlich, im Einzelfall kommt die Nutzung von Sonderzugriffen (Verfahren B.3) in Betracht. Darum herum gruppieren sich die medizinischen Informationen der aktuellen Behandlung, ggf. mit Vorbehandlungsdaten wie z. B. Arztbriefe, Berichte, Befunde, Pflegeinformationen. Sie können in Daten der ärztlichen Dokumentation, der pflegerischen Dokumentation und der Dokumentation der Maßnahmen des therapeutischen Teams unterteilt werden (s. DKG: „Die Dokumentation der Krankenhausbehandlung“). In der nachfolgenden Abbildung werden beispielhaft die Kategorien „Ärztliche Anordnungen“, „Befunde“, „Pläne“ und „Berichte/Protokolle“ verwendet.



Die Daten sind grundsätzlich allen in die Behandlung einbezogenen Mitarbeitern verfügbar („zentrale Krankengeschichte“). Das Zugriffsrecht auf diese Patientendaten für einzelne Mitarbeiter ergibt sich aus den ihnen zugewiesenen Rollen, die ihre Einbeziehung in die Behandlung repräsentieren. Die Zugriffsmethoden (Lesen, Schreiben, …) für die einzelnen Rollen können sich unterscheiden.

Eine Zugriffsmöglichkeit auf alle medizinischen Daten, d.h. die gesamte verfügbare elektronische Behandlungsdokumentation, ist für die behandelnden Ärzte unerlässlich. Grundsätzlich müssen auch Pflegekräfte auf Teile dieser Daten zugreifen können. Die anderen medizinischen Berufe benötigen die für ihren Untersuchungs- oder Behandlungsauftrag erforderlichen Informationen, dazu kann z. B. bei Physiotherapeuten im Rahmen der Frühmobilisation der OP-Bericht gehören.

Weiter ist zu berücksichtigen, dass die Daten in einem unterschiedlichen Fertigstellungs-Zustand vorliegen können. Ein Zugriff auf Entwurfsfassungen darf für den Autor und dessen Vertreter nicht von der Freigabe durch den Inhaber der dafür verantwortlichen Rolle abhängig gemacht werden. (z. B. Anamnese im Entwurfsstadium und nach Freigabe).

Der äußere Ring enthält die Dokumente der jeweiligen Fachabteilungen oder Institute/Leistungsstellen mit auf diese Organisationseinheiten (ggf. auch intern unterschiedlich) begrenzten Zugriffsrechten. Die Dokumente werden mit der Freigabe Bestandteil der zentralen Krankengeschichte.

Eine allgemein anerkannte Unterteilung der Datenbereiche in solche Teile, die nur Ärzten, nur Pflegekräften und/oder nur anderen medizinischen Berufen zugeordnet werden könnten, ist nicht verfügbar. Die technische Umsetzung muss eine flexible Gestaltungsfreiheit enthalten, um notwendige Zugriffe nicht behindern. Die konkrete Ausgestaltung muss dem Krankenhaus überlassen bleiben, das unter den betroffenen Leitungen eine Abstimmung durchführen muss, um den Zugriff auf medizinische Daten nach Kategorien entsprechend der jeweils vorgenommenen Aufgabenteilungen einzugrenzen.

1.3 Ausgestaltung der Zugriffskontrolle auf Patientendaten

Die Ausgestaltung der Zugriffskontrolle im Krankenhaus kann sich an folgenden Grundsätzen orientieren:

Ärzte, Pflegekräfte und medizinisches Personal, die in die Behandlung des Patienten einbezogen sind, haben den für ihre Aufgaben benötigten Zugriff auf die medizinischen Daten des Patienten.

Mitarbeiter in administrativen Funktionen im Zusammenhang mit der Dokumentation der Behandlung haben einen begrenzten Zugriff auf dazu erforderliche medizinische Daten des Patienten (abrechnungsrelevante Informationen und abrechnungsfähige Leistungen).

Mitarbeiter in der administrativen Patientenaufnahme (und Pforte) haben im Rahmen ihrer Tätigkeit den erforderlichen Zugriff auf die Patientenstammdaten und Verwaltungsdaten des Patienten, sie haben keinen Zugriff auf medizinische Daten des Patienten. Bei ihrer Tätigkeit können sie allenfalls Kenntnis vom Vorhandensein medizinischer Dokumente (Einweisung, Arztbrief, Röntgenbilder), nicht aber von deren Inhalt erhalten.

Für die technische Ausgestaltung der Zugriffskontrolle kommt folgende Stufung in Betracht, die im Einzelnen weiter verfeinert werden kann:

A. Zugriffskontrolle auf Ebene der Pflegeeinheit und Fachabteilung

Die Zugriffsrechte werden Rollen zugewiesen, die auf die Zugehörigkeit zur Organisationseinheit (Pflegeeinheit bzw. Fachabteilung) abstellen, von der der Patient während seines Aufenthalts behandelt und versorgt wird..

Der Zuschnitt der Organisationseinheit kann für einzelne Berufsgruppen weiter unterschieden werden. Für Ärzte soll regelhaft die Fachabteilung in Abgrenzung zu anderen Fachabteilungen bestimmt werden [Rollenbeispiel: Arztdienst in der

Fachabteilung CHIR]. Eine Eingrenzung kommt dann in Betracht, wenn die berufliche Tätigkeit jeweils (überwiegend) in einer einzeln bestimmbaren Pflegeeinheit ausgeübt wird. Dies kann für Rollen im Pflegedienst gelten, indem in Abhängigkeit vom Aufgabenbereich die Fachabteilung insgesamt (z. B. Abteilungsleitung Pflegedienst) oder eine bestimmte Pflegeeinheit innerhalb der Fachabteilung als Organisationseinheit für die Rollendefinition herangezogen wird [Rollenbeispiel: Pflegedienst in der Pflegeeinheit CHIR 1]. Für die Dauer ihres dokumentierten Einsatzes werden Pflegekräfte im Springerdienst den dort beschäftigen Pflegekräften gleichgestellt.

B. Zugriffskontrolle auf Ebene von hinzugezogenen Organisationseinheiten

Eine Ausweitung auf andere Fachabteilungen oder fachabteilungsübergreifende Organisationseinheiten ist in den Fällen erforderlich, in denen Ärzte anderer Fachgebiete regelhaft konsiliarisch oder bei interdisziplinärer Behandlung in Fallkonferenzen einbezogen werden. Für Pflegekräfte gilt dies z. B. bei Einsatz im Springerdienst oder bei interdisziplinärer Fachpflege. [Rollenbeispiel: Pflegedienst im Springerdienst für die Pflegeeinheiten CHIR 1, CHIR 2, ORTH].

Für Ärzte und medizinisches Personal in zentralen medizinischen Leistungsstellen muss im Rahmen ihrer Einbeziehung in die Untersuchung und Behandlung ebenfalls der Zugriff auf die medizinischen Daten des Patienten geregelt sein.

Folgende Optionen kommen in Betracht:

B.1 Auftragsbezogene Zugriffsrechte

Rolleninhabern außerhalb der behandelnden Organisationseinheit werden anlassbezogen Zugriffsrechte eingeräumt, die sich aus einem konkreten Auftrag eines behandelnden Arztes ableiten.

Für alle Personen, die nicht der behandelnden Organisationseinheit angehören, besteht eine technische Sperre, die durch einen konkreten Auftrag über eine elektronische Auftragsnachricht („Order Entry“) aufgehoben werden muss. (In Eilfällen mit mündlichem oder telefonischem Auftrag soll der Auftrag vom Beauftragten in Verbindung mit der zu protokollierenden Begründung für einen Sonderzugriff (siehe B.3) dokumentiert werden.)

Der Nutzung auftragsbezogener Zugriffsrechte sollte der Vorzug gegenüber anderen Zugriffsmöglichkeiten gegeben werden.

B.2 Patientenindividuelle Zugriffsmöglichkeit

Rolleninhabern außerhalb der behandelnden Organisationseinheit, die aus technischen Gründen nicht auftragsbezogen im Einzelfall Zugriffsrechte erhalten können, werden Zugriffsrechte durch eine geplante, zeitlich begrenzte patientenindividuelle Zuordnung der betreffenden Organisationseinheit zu den Zugriffsberechtigten auf die relevanten medizinischen Daten des Patienten eingeräumt.

Dies kann z. B. Konsiliarärzte, Mitglieder einer Fallkonferenz, Personal in zentralen medizinischen Leistungsstellen (Zentrallabor, Radiologie, Apotheke u.a.) betreffen. Die datenschutzkonforme Protokollierung und ihre regelmäßige und zeitnahe Auswertung ist erforderlich, um unberechtigte Zugriffe frühzeitig erkennen und für die Zukunft verhindern zu können. In diesen Fällen kommt beispielsweise ein Abgleich der erfolgten Zugriffe gegen erbrachte Leistungen in Frage.

B.3 Sonderzugriffsrechte (mit Protokollierung des Zugriffs)

Mitarbeiter in fachabteilungsübergreifenden oder zentralen Diensten, denen über das Rollen- und Berechtigungskonzept kein Zugriff (B.1 oder B.2) eingeräumt wird, müssen bei Erfordernis die Möglichkeit haben, über eine „Sonderfunktion“ mit Begründung die benötigten Daten des Patienten einzusehen. Für die Begründung sollen Vorgabetexte anhand einer Auswahlliste herangezogen werden können.

Da es sich hier um „Routinefälle“ unter bestimmten Einzelfallkonstellationen handeln kann, wenn die Zugriffsrechte zu eng angelegt werden, müssen solche Sonderzugriffe ausdrücklich ermöglicht werden. Hier kann es sich z. B. handeln um:

- Datenzugriff durch den Laborarzt oder Radiologen (einschließlich Assistenten) aufgrund eines zeitkritischen Untersuchungsauftrags in Notfällen, sofern keine reguläre Zugriffsberechtigung besteht, z. B. für bestimmte Patienten mit einer Zugriffssperre,
- Datenzugriff von Ärzten oder Pflegekräften der „alten“ Pflegeeinheit im Rahmen einer „Nachlaufzeit“ nach interner Verlegung auf den Datenbestand in der „neuen“ Pflegeeinheit,
- Datenzugriff im Zusammenhang mit ungeplanten Vertretungen und Bereitschaftsdiensteinsätzen. („Spontanfälle“)

Auch hier ist eine datenschutzkonforme Protokollierung erforderlich, um unberechtigte Zugriffe frühzeitig erkennen und für die Zukunft verhindern zu können. Ebenso ist zu berücksichtigen, das der erhebliche Umfang der Protokollierung zwangsläufig einen hohen Auswertungsaufwand zur Folge hat.

C. Zugriffskontrolle auf Ebene der Verwaltung

C.1 Administrative Patientenaufnahme (Patientenstammdaten)

Die administrative Patientenaufnahme verantwortet die Übernahme der Patientenstammdaten in die Datenhaltung des Krankenhauses und besorgt das Zustandekommen des Krankenhausbehandlungsvertrags mit den dabei erforderlichen Erklärungen des Patienten.

Die Patientenstammdaten mit ihren vertraglichen Ergänzungen (Wahlleistungen) stehen der behandelnden Fachabteilung zur Verfügung und werden z. B. zur Zuweisung der Unterbringung oder für eine Kontaktaufnahme mit Angehörigen/Ansprechpartnern des Patienten verwendet.

Wenn der Patient bereits im Krankenhaus behandelt wurde, muss die administrative Aufnahmekraft eine Information über die Zeiten der Vorbehandlungen erhalten. Handelt es sich um eine Wiederaufnahme bei einem noch nicht abgeschlossenen Fall, steht ihr auch die Information über die Fachabteilung zur Verfügung, in der zuvor die Behandlung erfolgte.

Einen Sonderfall stellt die Pforte dar, die für Auskunftszwecke Zugriff auf Patientenstammdaten, die nicht mit einer Auskunftssperre belegt sind, benötigt.

C.2 Patientenabrechnung (Verwaltungsdaten und medizinische Daten)

Datenzugriffe, die im Zusammenhang mit der Wahrnehmung gesetzlicher Dokumentationsverpflichtungen von Mitarbeitern der Verwaltung durchgeführt werden, müssen auch medizinische Daten des Patienten umfassen können.

Hierzu zählt z. B. die Verwendung aller für Zwecke der Abrechnung mit den Kostenträgern (einschließlich Prüfverfahren) notwendigen medizinischen Unter-

lagen, für Zwecke der internen und externen Qualitätssicherung sowie für die Organisation von Versorgungsprozessen im Zusammenhang mit dem Fall- und Entlassmanagement (auch durch Sozialdienst, Seelsorge). In Abhängigkeit von der Aufgabe, z. B. MDK-Prüfverfahren, Qualitätssicherung) haben auch die der behandelnden Organisationseinheit zugeordneten Rollen (Arztdienst der Fachabteilung) Zugriff.

D. Zugriffskontrolle in Verbindung mit besonderen Nutzungen

Besondere Nutzungen von Patientendaten wie z. B. für statistische Auswertungen und Ausbildungszwecke erfordern eine Pseudonymisierung (oder Anonymisierung) neben der Begrenzung der Zugriffs im Rollen- und Berechtigungskonzept.

2 Protokollierung

Die (datenschutzrechtliche) Protokollierung dient der Erfüllung von Auskunftspflichten an den Patienten und der Überprüfung der Wirksamkeit der Datenschutzkontrollmaßnahmen, z. B. des Rollen- und Berechtigungskonzepts für die Zugriffskontrolle.

Das Krankenhaus muss ein Konzept zur Protokollierung von Zugriffen auf Patientendaten und ein Konzept zur Auswertung der Protokolldaten erarbeiten. Die notwendige Protokollierungstiefe ist von der Differenzierung des Berechtigungskonzeptes abhängig.

Die Protokollierung muss nachvollziehbar dokumentieren, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat. Die Protokollierung darf nur zweckgebunden erfolgen. Die Zweckbindung ergibt sich aus der Kontrolle von Zugriffen auf Patientendaten. Sie ist auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.

Die Protokollierung muss in einem Protokollierungskonzept von der Geschäftsführung und dem IT-Verantwortlichen verbindlich festgelegt werden. Es ist mit den zuständigen Beteiligten im Krankenhaus abzustimmen. Folgende Personen/Rollen sollen bei der Entwicklung des Protokollierungskonzeptes eingebunden sein:

- Verantwortlicher für IT-Sicherheit,
- Datenschutzbeauftragter des Krankenhauses,
- Mitarbeitervertretung,
- Berechtigungsverwaltung (IT-Administration).

Das Protokollierungskonzept muss Festlegungen enthalten zu:

1. Art und Umfang der Protokollierung,
2. Verfahrensweisen zur Speicherung und Auswertung der Protokolldaten,
3. Schutzmaßnahmen für die Rechte der Mitarbeiter,
4. Aufbewahrungsdauer der Protokolldaten.

Das Protokollierungskonzept soll auch Festlegungen zur Prüfung der Protokolldaten, Bewertung der Auswertungsergebnisse und geeigneten Maßnahmen bei Auffälligkeiten enthalten.

2.1 Festlegungen zu Art und Umfang der Protokollierung

Die Protokollierung korrespondiert mit den bestehenden Zugriffsregelungen. Bei hinreichend eng ausgestaltetem Zugriffsschutz können die Anlässe der Protokollierung in Verbindung mit dem Rollen- und Berechtigungskonzept reduziert werden.

a) Zugriffe auf Anwendungsebene

Lesen von Patientendaten

In den Fällen, in denen der Kreis der Zugriffsberechtigten im Rollen- und Berechtigungskonzept eng begrenzt ist, z. B. bei Pflegekräften auf die Pflegeeinheit, kann die Protokollierung auf Lesezugriffe außerhalb der Regelberechtigung des Berechtigungskonzepts beschränkt werden. Für Auskünfte kann dann die Nennung des Kreises der Regelberechtigten ausreichen. Wenn erforderlich, kann der Personenkreis anhand der Dienstpläne konkret benannt werden.

Eine regelhafte Protokollierung ist dagegen erforderlich, wenn im Rollen- und Berechtigungskonzept allgemein eingeräumten Zugriffsrechte (Option B.2) oder Sonderzugriffsrechte (Option B.3) vergeben werden.

Eine regelhafte Protokollierung ist weiter bei „kritischen" Suchanfragen erforderlich, bei denen zu Patienten mit unbestimmten Patientenstammdaten anhand einer „wildcard-Suche" (Autovervollständigen) versucht wird, den Namen, Wohnort, Geburtsdatum zu erhalten oder bei Lesezugriffen auf Patientendaten besonderer Personengruppen (z. B. Mitarbeiter, VIPs). Eine Protokollierung des Ergebnisses der Anfrage ist genau dann nicht erforderlich, wenn dieses Ergebnis ex post nachvollzogen werden kann, zumindest in Bezug auf die angezeigten Patientennamen oder Fallnummern. Bei Vorliegen eines differenzierten Rollen- und Berechtigungskonzepts ist das Ergebnis in aller Regel problemlos rekonstruierbar (ggf. unter Einbeziehung archivierter Datenbestände).

Im Rahmen der Weitergabekontrolle sind alle Exporte von Patientendaten zu protokollieren und zu prüfen.

Schreiben von Patientendaten

Grundsätzlich wird das Schreiben von neuen Dokumentenversionen protokolliert. Das Schreiben von Entwurfsfassungen wird nur protokolliert, wenn die geschriebenen Daten über den Autor hinaus auch von anderen Beschäftigten eingesehen werden können. Sofern eine Freigabe von Entwurfsfassungen erforderlich ist, wird das Schreiben mit der Freigabe protokolliert.

Das Löschen von Anwendungsobjekten (Dokumente, Inhalte der Fallakte) ist immer zu protokollieren.

b) Zugriffe auf Ebene der IT-Administration:

Bei Maßnahmen der Rechteadministration sowie bei Zugriffen im Rahmen der Fernwartung erfolgt eine Protokollierung aller Zugriffe.

Auch der Zugriff auf die Protokolldaten ist für eine Datenschutzauswertung zu protokollieren.

Inhalt der Protokollierung (Umfang)

Im datenschutzrechtlichen Protokoll sind bei Einträgen folgende Merkmale zu protokollieren:

- der Zeitpunkt des Zugriffs auf die Patientendaten (Systemzeit),
- die Kennung des jeweiligen Benutzers,

- die Kennung der aufgerufenen Transaktion des Nutzers (Anzeige, Abfragefunktion, Reportname, Maskenbezeichnung),
- die Identität des betroffenen Patienten,

Zusätzlich:

- eine Verweis auf die Begründung für einen begründungsabhängigen Zugriff (bei Sonderzugriffen),
- die verwendeten Suchkriterien und Folgeaktion zum Anzeigen von Patientenstammdaten bei „kritischen“ Suchanfragen.

2.2 Verfahrensweisen zur Speicherung und Auswertung der Protokolldaten

Vorgesehene Protokollierungen dürfen nicht umgangen werden können. Protokolldaten sind technisch gegen nachträgliche Veränderung zu schützen. Hierbei kommt z. B. eine kryptografische Absicherung, Speicherung auf WORM-Medien in Betracht.

Die Auswertung der Protokollierung muss dem engen Kreis der dafür Berechtigten eine Information ermöglichen, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat oder unberechtigt nutzen wollte. Die Informationen dienen dazu, die Wirksamkeit des Rollen- und Berechtigungskonzepts zu überprüfen.

Eine weitere wesentliche Funktion ist die Auskunftserteilung für Patienten über Zugriffe auf die eigenen Patientendaten.

Das Auskunftsrecht des Patienten über seine im Krankenhaus gespeicherten, personenbezogenen Daten muss gewährleistet werden. Ist bei hinreichend differenziertem Zugriffsschutz eine Protokollierung verzichtbar, muss eine Auskunft an den Patienten über den Kreis der Berechtigten möglich sein.

Die Auswertung der Protokollierung muss datenschutzkonform ausgestaltet und im Rollen- und Berechtigungsmanagement geregelt werden. Die Auswertung ist stichprobenartig oder anlassbezogen anzulegen. Sie darf nur einem dafür berechtigten Personenkreis als Lesezugriff gestattet werden.

Für die Auswertung von protokollierten Zugriffen auf Patientendaten kann der Datenschutzbeauftragte des Krankenhauses die Unterstützung geeigneter Mitarbeiter des Krankenhauses in Anspruch nehmen. Die Auswertung soll in einem gestuften Verfahren erfolgen, z.B. zunächst eine Prüfung allgemeiner Auffälligkeiten ohne Personenbezug, danach bei Auffälligkeit personenbezogene Prüfung unter Hinzuziehung weiterer Personen, z.B. Mitarbeitervertretung. Für eine effektive Unterstützung der Auswertung sind sowohl eine zweckorientierte Begrenzung der Protokollierung als auch die technische Unterstützung der Auswertung über einen speziell dafür nutzbaren „Datenschutzarbeitsarbeitsplatz“ im KIS notwendig.

2.3 Festlegungen zu Schutzmaßnahmen für die Rechte der Mitarbeiter

Der Mitarbeiter soll als Patient die Möglichkeit haben, seine Patientendaten mit einer Mitarbeiterkennzeichnung versehen zu lassen. Die Mitarbeiterkennzeichnung kann dazu verwendet werden, im Rahmen des Rollen- und Berechtigungskonzepts eine zusätzliche Eingrenzung des Kreises der Zugriffsberechtigten vorzunehmen. Das gilt insbesondere bei weiter gefassten Zugriffsrechten.

Bei ihrer Tätigkeit im Krankenhaus werden Mitarbeiter regelhaft bei Zugriffen auf Patientendaten entsprechend Protokollierungskonzept in den Protokollen ausgewiesen. Die Mitarbeiter müssen über die Anlässe ihrer Protokollierung, ihre Einsicht-

möglichkeit in die Protokolle und die datenschutzkonforme Verarbeitung, Nutzung und Löschung der Protokolldaten unterrichtet werden.

2.4 Festlegungen zur Aufbewahrungsdauer der Protokolldaten

Im Regelfall sollen Protokolldaten für 12 Monate aufbewahrt werden. Mit dem Wegfall der Erforderlichkeit für die Aufgabenerfüllung sind die gespeicherten Protokolldaten zu löschen.

3 Zugriffsbeschränkungen auf Patientendaten

Eine Beschränkung der Zugriff auf Patientendaten kann an die Stelle einer datenschutzrechtlich erforderlichen Löschung treten, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Das Krankenhaus muss ein Konzept zur Zugriffsbeschränkung festlegen, durch das Zugriffe auf Patientendaten nach Ablauf von dort definierter Fristen („unter einem Jahr") beschränkt und regelhaft auf begründete Sonderfälle eingegrenzt werden.

Das Konzept zur Zugriffsbeschränkung muss von der Geschäftsführung und dem IT-Verantwortlichen verbindlich festgelegt werden. Es ist mit den zuständigen Beteiligten im Krankenhaus abzustimmen. Folgende Personen/Rollen sollen bei der Entwicklung des Konzept zur Zugriffsbeschränkung eingebunden sein:

- Verantwortlicher für IT-Sicherheit,
- Datenschutzbeauftragter des Krankenhauses,
- Berechtigungsverwaltung (IT-Administration).

Im Kern handelt es sich bei dem Konzept zur Zugriffsbeschränkung um ein „Fristenkonzept", in dem die Fristen/Ereignisse für den Beginn der Zugriffsbeschränkung festgelegt werden.

3.1 Zugriffsbegrenzende Ereignisse

Der Zugriff auf Patientendaten soll mit Eintritt definierter Ereignisse, die den Abschluss der Behandlung kennzeichnen, eingeschränkt werden. Alternativ können die Daten ausgelagert werden.

Für die unterschiedlichen Berufsgruppen eines Krankenhauses als auch Patientengruppen sind jeweils verschiedene Ereignisse und Fristen zu berücksichtigen, mit denen der Zugriff auf Daten eines Behandlungsfalles nicht mehr notwendig und somit zu begrenzen ist.

Als mögliche zugriffsbegrenzende Ereignisse, die den Abschluss eines Behandlungsfalls bestimmen können, kommen in Betracht:

- Abschluss einer Beauftragung mit Zugriffserfordernis auf die Patientendaten,
- Interne Verlegung des Patienten in eine andere Fachabteilung,
- Entlassung des Patienten,
- Übermittlung der Schlussrechnung nach Entlassung,
- Bestätigung der Schlussrechnung durch die Krankenkasse über Zahlungseingang zur Schlussrechnung,
- Fristablauf für Nachprüfungen zum Behandlungsfall durch den MDK (= 6 Wochen nach Rechnungszustellung),
- Ablauf einer vom Krankenhaus vorgegebenen Frist von z. B. x Tagen nach der Entlassung des Patienten oder allgemein x Tage nach Eintritt des zugriffsbegrenzenden Ereignisses.

Das Krankenhaus muss in sein Konzept zur Zugriffsbeschränkung eine eindeutige Regelung aufnehmen, welche der möglichen Ereignisse für welche Rollen eine Zugriffsbegrenzung auslösen müssen. Dabei soll auch ein nach Berufsgruppen (Rollen) unterschiedlich definierter Beginn der Beschränkung vorgesehen werden, z. B. eine frühere Zugriffsbeschränkung für Pflegekräfte im Vergleich zu dem Personal in der Abrechnung.

Die Fristen sollten sich an den geschäftsüblichen Arbeitsabläufen orientieren, d. h. die betroffenen Mitarbeiter sollen in der üblichen Durchführung ihrer Aufgaben nicht behindert werden. Ausnahmefälle sollen nicht zur Begründung unnötig langer Fristen herangezogen werden.

Für Ärzte der behandelnden Fachabteilung wird der Zugriff (bis zum Löschen der Patientendaten) nicht beschränkt, insbesondere um ihnen im Rahmen ihrer aktuellen Behandlungsplanung eine Überprüfung anhand ähnlicher Fallkonstellationen zu ermöglichen.

Nur zeitweilig in die Behandlung einbezogene Ärzte (z.B. Ärzte im Bereitschaftsdienst, Konsiliarärzte, Laborärzte) haben im Rahmen von Sonderzugriffsmöglichkeiten nach B.3 (1.3 Ausgestaltung der Zugriffskontrolle auf Patientendaten) auch nach Abschluss der Behandlung anlassbezogen die Möglichkeit, auf zugriffsbeschränkte Daten zuzugreifen.

Für die meisten anderen Beschäftigten entfallen nach Eintritt der festgelegten zugriffsbegrenzenden Ereignisse sowohl die regulären als auch Sonderzugriffsrechte auf die Daten der jeweiligen Patienten.

Aufgrund der sehr unterschiedlichen Zugriffsbeendigungsfristen je Berufsgruppe erscheint eine Umsetzung im Rahmen des Rollen- und Berechtigungskonzeptes am wirkungsvollsten.

Tritt nach Beschränkung des Zugriffs ein Ereignis ein, das den erneuten Zugriff für bestimmte an der seinerzeitigen Behandlung beteiligte Berufsgruppen erfordert, kommen Sonderzugriffe entsprechend Rollen- und Berechtigungskonzept auf die benötigten medizinischen Daten des Patienten in Betracht. Ein Zugriff ist dann nur einem festgelegten eingeschränkten Kreis von Berechtigten (Rollen) für eindeutig beschriebene Aufgaben, wie z. B. Klärung von Abrechnungsfragen, MDK-Auskünfte, Qualitätssicherungsfragen, möglich. Hierzu muss anhand der Identitätsdaten des Patienten (Name, Geburtsdatum, Geburtsort, Wohnort) eine Suche in den zugriffsbeschränkten Daten möglich sein. Dazu muss erkennbar sein, welche Datensätze dem regulären Zugriff entzogen sind.

Sofern über das Rollen- und Berechtigungskonzept während der Behandlung zeitlich befristete Zuweisungen von Zugriffsrechten erteilt werden können (z. B. bei ärztlichen Aufträgen), muss die Beendigung des Zugriffsrechts mit Abschluss des Auftrags im Konzept zur Zugriffsbeschränkung nicht mehr betrachtet werden.

3.2 Maßnahmen

Die technische Umsetzung der Zugriffsbegrenzung kann u. a. durch Verwendung von Kennzeichen zur Zugriffsbeschränkung, Auslagerung von Daten aus dem aktiven System sowie (vorzugsweise) im Rahmen des Rollen- und Berechtigungskonzeptes erfolgen.

Bei Verwendung von Kennzeichen zur Zugriffsbeschränkung ist darauf zu achten, dass für die unterschiedlichen Zugriffsfristen der verschiedenen Berufsgruppen auch eine ausreichende Anzahl von Kennzeichen zur Zugriffsbeschränkung vom System zur Verfügung stehen müssen bzw. deren Einsatz flexibel gestaltet werden kann.

Eine Auslagerung von Datenbeständen zum Entzug des regulären Zugriffs sollte nur in Betracht gezogen werden, wenn die Fristen der Zugriffsbegrenzung über die verschiedenen Berufsgruppen weitgehend einheitlich sind oder aber andere Maßnahmen zur Begrenzung des regulären Zugriffs vorgeschaltet sind.

Für Kontrollzwecke ist ein Report zur Anzeige der dem regulären Zugriff entzogenen Datensätze sowie über die Protokollierung der genutzten Sonderzugriffe einzurichten.

4 Löschen von Patientendaten

Gespeicherte Patientendaten müssen gelöscht werden, wenn ihre Kenntnis für das Krankenhaus zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. An die Stelle einer Löschung gespeicherter Patientendaten kann in bestimmten Fällen eine Zugriffsbeschränkung treten, [siehe Konzept zur Zugriffsbeschränkung].

Das Krankenhaus muss ein Löschkonzept zur Löschung von Patientendaten erstellen.

Das Löschkonzept muss von der Geschäftsführung und dem IT-Verantwortlichen verbindlich festgelegt werden. Es ist mit den zuständigen Beteiligten im Krankenhaus abzustimmen. Folgende Personen/Rollen sollen bei der Entwicklung des Löschkonzepts eingebunden sein:

- Verantwortlicher für IT-Sicherheit,
- Datenschutzbeauftragter des Krankenhauses,
- Anwendungsverwaltung (IT-Administration),
- Beauftragter für Risikomanagement bzw. Versicherungswesen.

Das Löschkonzept muss Festlegungen zu den Fristen enthalten, nach denen die Patientendaten gelöscht werden müssen. Bei den zu löschenden Patientendaten handelt es sich um Daten, die entsprechend Konzept zur Zugriffsbeschränkung dem operativen Datenbestand bereits entzogen wurden.

4.1 Ausgangslage

Die Dokumentation der Krankenhausbehandlung ist ein Teil der dem Patienten geschuldeten Leistungen aus dem Behandlungsvertrag. Darüber hinaus folgt die Dokumentationspflicht aus dem Berufsrecht der Ärzte und aus spezialgesetzlichen Regelungen. Die Pflicht zur Führung der Krankengeschichte umfasst auch die Pflicht zur Aufbewahrung der im Zusammenhang mit einer Behandlung anfallenden wesentlichen und für die Dokumentation des Behandlungsverlaufs erforderlichen Krankenunterlagen.

Das Speichern von personenbezogenen Daten kann grundsätzlich nur zweckgebunden geschehen. Zwecke einer Speicherung personenbezogener Patientendaten in einem Krankenhaus können u. a. sein:

- Gewährleistung der internen und externen Prozesse der Patientenbehandlung,
- Gewährleistung der Leistungsabrechnung mit den Kostenträgern,
- Dokumentation der Behandlung,
- Einhaltung der verschiedenen Aufbewahrungsvorschriften.
- Entlastungsmöglichkeit bei Rechtsstreitigkeiten.

Fällt der Zweck der Speicherung fort, sind die gespeicherten Daten zu löschen. Bei der Annahme eines Fortfalls des Speicherungszwecks ist zu beachten, dass die Behandlungsdokumentation i.d.R. das einzige dem Urkundsbeweis zugängliche Beweismittel über das Geschehen im Krankenhaus darstellt. Ein Fehlen kann zu nachteiligen Konsequenzen bei einer gerichtlichen Beweiserhebung (fehlende Entlastungsmöglichkeit) führen. Die Folgen der Nichterweisbarkeit einer Tatsache treffen – entsprechend der Verteilung der Beweislast – sowohl den Krankenhausträger als auch den Patienten.

Im Anwendungsbereich des Bundesdatenschutzgesetzes regelt § 6 die unabdingbaren Rechte der von einer Erhebung und Verarbeitung von Daten Betroffenen. Hierzu gehören u. a. auch die Rechte auf Berichtigung, Löschung und Zugriffsbeschränkung und die

damit korrespondierenden Pflichten der verantwortlichen Stellen, unabhängig davon, ob der Betroffene einen entsprechenden Anspruch geltend macht. Die Rechte auf Berichtigung, Löschung und Zugriffsbeschränkung können nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Löschen ist nach der Legaldefinition in § 3 Abs. 4 Nr. 5 BDSG das Unkenntlichmachen der gespeicherten personenbezogenen Daten. Ein Unkenntlichmachen liegt bei jeder Handlung vor, die irreversibel bewirkt, dass eine Information nicht länger aus den gespeicherten Daten gewonnen werden kann.

4.2 Löschfristen (Aufbewahrungsfristen)

Generell unterliegen die Behandlungsunterlagen einer Aufbewahrungsfrist von mindestens 10 Jahren (§ 10 Abs. 3. MBO-Ä) nach Abschluss der Behandlung. Dies gilt für stationäre wie auch ambulante Behandlungen, sofern nicht nach anderen gesetzlichen Verpflichtungen eine längere Aufbewahrungspflicht besteht. Beginn der Frist ist das Ende des Behandlungsjahres. Daten einer Vorbehandlung können, wenn sie für eine aktuelle Behandlung genutzt werden, kopiert bzw. dieser zugeordnet werden mit der Folge, dass sie erst mit den Daten dieser nachfolgenden Behandlung gelöscht werden. Dies entspricht gebräuchlichem Vorgehen mit Papierakten.

Aus zahlreichen spezialgesetzlichen Regelungen ergeben sich jedoch auch deutlich längere Aufbewahrungsfristen, z. B.

- 30 Jahre für Aufzeichnungen über die Röntgenbehandlung (§ 28 Abs. 3 RöV und § 85 Abs. 3 StrSchV),

- 10 Jahre für Röntgenbilder und die Aufzeichnungen über Röntgenuntersuchungen (§ 28 Abs. 3 Satz 2 RÖV), bei Personen unter 18 Jahren bis zur Vollendung des 28. Lebensjahrs (§ 28 Abs. 3 Satz 3 RöV),

- 15 Jahre für ärztliche Unterlagen und Röntgenfilme über Schwer-Unfallverletzte bei Zulassung zum Verletzungsartenverfahren der gesetzlichen Unfallversicherungsträger,

- 15 bis 30 Jahre für bereichsspezifische Regelungen nach Maßgabe der Apothekenbetriebsordnung, des Transfusionsgesetzes, Transplantationsgesetzes, SGB VII, der Medizinproduktesicherheitsplanverordnung,

- 30 Jahre für die Patientendokumentationen, sofern es sich nicht um im Krankenhaus Verstorbene handelt, für die eine Aufbewahrungsdauer von 20 Jahren gilt (§ 39 der Berliner Krankenhaus-Verordnung).

Letztlich ist zu berücksichtigen, dass Schadensersatzansprüche, die auf einer Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis verjähren. Aus Beweissicherungsgründen auch für zivilrechtliche Schadenersatzansprüche des Patienten ist generell bei Behandlungsunterlagen eine Aufbewahrungsfrist von 30 Jahren ableitbar.

In ihren Hinweisen zur Dokumentation der Krankenhausbehandlung empfiehlt die DKG auch weiterhin „eine Aufbewahrungsfrist für Krankenunterlagen von 30 Jahren“. Zugleich wird festgestellt: „ob sich das Krankenhaus unter Beachtung der gesetzlichen Vorgaben (spezialgesetzliche Regelungen, z. B. gem. RöV) im Einzelfall dennoch zu einer kürzeren Aufbewahrung von Krankenunterlagen entschließt, ist eine Entscheidung, die der Krankenhausträger im Rahmen seines Risikomanagements unter Abwägung aller

Umstände treffen kann. Hierbei sollte auch die Haftpflichtversicherung einbezogen werden, um für den jeweiligen Krankenhausträger eine versicherungstechnisch tragbare Lösung im Einzelfall zu finden.“

4.3 Maßnahmen

Die Gewährleistung der für das Krankenhaus relevanten Aufbewahrungsvorschriften darf durch das Löschkonzept nicht beeinträchtigt werden.

Vom Krankenhaus ist ein unternehmensweites Konzept zur Löschung von gespeicherten Daten nach Wegfall der Zweckbestimmung der Speicherung zu erstellen und durch die Geschäftsführung verbindlich vorzugeben.

Ein differenziertes Löschen einzelner Daten/Datenbereiche zur Behandlung entsprechend dem Wegfall des jeweiligen Speicherzweckes ist wünschenswert, in Praxis wird aufgrund der Zusammengehörigkeit der Daten als auch der technisch kaum differenziert möglichen Umsetzung der Datenlöschung meist nur die vollständige Löschung aller Daten einer Behandlung möglich sein.

Das Löschkonzept ist grundsätzlich unabhängig von den aktuell bestehenden technischen Möglichkeiten der eingesetzten Krankenhausinformationssysteme zu definieren. Die Löschung selbst ist entsprechend den von den Datenhaltungssystemen angebotenen technischen Möglichkeiten vorzunehmen. Dabei müssen Löschaufträge an angebundene Subsysteme über die vorhandenen Schnittstellen weitergegeben werden können. Bieten die vorhandenen Systeme keine zuverlässige Löschmöglichkeit, sind diese Einschränkungen zu dokumentieren und der betroffene Systemhersteller zur Bereitstellung einer Löschfunktion aufzufordern.

Die mit Einwilligung des Patienten vorgehaltenen Daten einer vom Krankenhaus angebotenen Patientenakte müssen von der Löschung ausgenommen werden können.

Über die Datenlöschungen sollten Löschprotokolle erstellt werden. Dies gilt besonders für Löschungen vor Ablauf von 30 Jahren.

Die Löschprotokolle sollen als Verfahrensprotokolle Auskunft geben über:

- das Datum der Löschung,
- das gültige Löschkonzept (Version, Datum),
- das betroffene Verfahren,
- die angewandte Löschregel,
- die Anzahl der gelöschten Daten.

Das Löschprotokoll darf keine personenbezogenen medizinischen Daten des Patienten enthalten.

5 Spezielle Fragestellungen

5.1 Subsysteme

Bei der Einbeziehung von Subsystemen sollte zunächst eine Lösung für diejenigen Subsysteme im Vordergrund stehen, die mit dem PAS integriert sind und eine Propagation über (standardisierte) Schnittstellen unterstützen. Ergänzend ist zu klären, welche Löschverfahren für isolierte Subsysteme in Betracht kommen, dabei ist zu berücksichtigen, dass die Isolation der Subsysteme mit eigenen Schutzmaßnahmen bereits eine Verknüpfung der Daten verhindert. Neben einem kontrollierten Zugriff auf die Daten der isolierten Subsysteme stehen hier insbesondere der durch Verschlüsselung geschützte Export von Daten auf externe Speicher und die Protokollierung zur Bereitstellung von Daten/Übersichtslisten zur Datenschutzkontrolle im Vordergrund.

5.2 Vorbehandlungsdaten

Ein Sonderfall, bei dem alle Mitarbeiter von einem Ausschluss der Nutzung von Patientendaten aus der Vergangenheit betroffen sind, ist die ausdrückliche Erklärung des Patienten, dass Daten aus Vorbehandlungen nicht genutzt werden dürfen. In der Regel wird der Patient schon aus Eigeninteresse an einer erfolgreichen Behandlung einer Nutzung von Vorbehandlungsdaten im Rahmen des Behandlungsvertrags zustimmen. Den behandelnden Ärzten müssen grundsätzlich alle vorhandenen medizinischen Informationen vorliegen, um eine optimale Behandlung durchführen zu können

Widerspricht der Patient ausdrücklich der Nutzung von vorhandenen Vorbehandlungsdaten, muss der Widerspruch wirksam durchgesetzt werden. Zugleich sollen die behandelnden Ärzte über den Widerspruch informiert werden und dadurch die Möglichkeit haben, mit dem Patienten die Aufhebung des Widerspruchs zu besprechen.

Für die technische Umsetzung einer Information der behandelnden Ärzte über einen erklärten Widerspruch ist darauf zu achten, dass diese Information nach einem erfolglosen Versuch zur Aufhebung nicht weiter angezeigt werden muss. Dies würde ggf. erneute erfolglose Wiederholungsversuche provozieren. Dazu sollte auch erkennbar sein, dass der Patient seinen Widerspruch nach einem ärztlichen Gespräch nicht aufgehoben hat.

Wird der Widerspruch nicht aufgehoben, ist im Einzelfall über den Behandlungsvertrag zu entscheiden.

Ausgenommen von der Widerspruchsmöglichkeit sind Wiederaufnahmen, Rückverlegungen sowie Vorbehandlungen in derselben Fachabteilung. Für die technische Umsetzung ist davon auszugehen, dass dies nicht nur dann gilt, wenn der vorbehandelnde Arzt persönlich wieder behandelt.

5.3 Pseudonymisierte/anonymisierte Patientendaten

Für bestimmte Zwecke ohne unmittelbaren Bezug zur Behandlung des Patienten, wie z. B. Testmaßnahmen, Schulungen, statistische Auswertungen, Zugriff „externer Komponenten“ für Auswertungen muss eine Identifikation des Patienten durch Pseudonymisierung oder Anonymisierung ausgeschlossen werden.

5.4 Besondere Patientengruppen (Mitarbeiter, VIP)

Die Daten besonders schutzwürdiger Personen im Krankenhaus werden durch das Rollen- und Berechtigungskonzept geschützt; ggf. auch unter Verwendung eines Pseudonyms.

Für die technische Umsetzung des Schutzes sind folgende Konkretisierungen erforderlich:

- Eine besondere Einschränkung von Zugriffsrechten im Rahmen der Behandlung von Mitarbeitern oder VIP ist grundsätzlich nicht erforderlich. In die Behandlung dieser Patientengruppen werden in aller Regel keine speziellen Mitarbeiter neben bzw. anstelle der „Regelbesetzung" der Pflegeeinheit eingesetzt. Im Rollen- und Berechtigungskonzept sollten möglichst eng gefasste Zugriffsberechtigungen (Rollen) vergeben werden.

- Eine besondere Einschränkung kann ausschließlich für Mitarbeiter in der Abrechnung des Behandlungsfalls in Betracht kommen, sofern diese Einschränkung nicht ihre Aufgabenwahrnehmung (Rechnungsstellung) behindert.

Voraussetzung für besondere Zugriffsregelungen für die Fallabrechnung ist die Bekanntgabe der Mitarbeitereigenschaft von dem betroffenen Mitarbeiter-Patienten. Eine Überprüfung von Patienten bei der Aufnahme auf ihre Mitarbeitereigenschaft ist nicht zulässig.

Auch für Personen öffentlichen Interesses (VIP-Patienten), die nach Feststellung der Klinikleitung „einer besonderen Gefährdung oder einem erhöhten Interesse" an einem Zugriff auf ihre Daten ausgesetzt sind, ist eine Konkretisierung der Kriterien erforderlich, nach denen die Geschäftsführung ihre Feststellung trifft. Bei den Personen, für die eine VIP-Einstufung mit hoher Wahrscheinlichkeit erwartet werden kann, kann darauf hingewiesen werden, dass in der Regel dann auch geeignete organisatorische Maßnahmen ergriffen werden, die als „Einzelregelung" umgesetzt werden können. Hier könnte technisch eine noch zu realisierende Lösung sinnvoll sein, bei der Patientenaufnahme einen zusätzlichen „fiktiven Namen" (Alias) zu erzeugen, der während der Behandlung als „Arbeitsnamen" verwendet wird und dessen Auflösung auf den echten Namen nur einem begrenzten Kreis möglich ist.

5.5 Verschlüsselung

Grundsätzlich ist davon auszugehen, dass Patientendaten, die physisch durch Zugangskontrolle (Rechenzentrum) und durch ein Rollen- und Berechtigungskonzept (Zugriffskontrolle) geschützt sind, nicht verschlüsselt werden müssen.

Insbesondere eine Verschlüsselung des zugriffsgeschützten operativen Datenbestands ist in der Regel nicht erforderlich. Dies gilt auch für eine gezielte Verschlüsselung von Datenbereichen für Patienten mit besonderem Datenschutzbedarf, eine verschlüsselte Datenhaltung zum Schutz gegen die Systemadministration oder die (Soll-) Verschlüsselung von Protokolldaten. Grundsätzlich ist bei der Entscheidung, ob Verschlüsselung eingesetzt wird, zwischen dem erzielten Sicherheitsgewinn und den entstehenden Kosten insbesondere in Bezug auf die Performanz der Verfahren abzuwägen. Dieses Verhältnis variiert in Abhängigkeit von der Ebene, auf der die Verschlüsselung erfolgt (Datenträger, Datenbank oder Anwendung).

Für die technische Umsetzung ist zu beachten, dass nur aus dem o.g. Schutzbereich exportierte Patientendaten bei Übermittlung, z. B. im Rahmen von Fernwartung, oder bei Speicherung auf externen Datenträgern (einschließlich Synchronisationskopien auf mobilen Arbeitsplätzen) unter Kontrolle des Krankenhauses zu verschlüsseln sind, sofern sie nicht pseudonymisiert/anonymisiert exportiert werden.

6 Anhang

6.1 Musterformular Konzept zur Zugriffsbeschränkung (Zugriffsbeschränkung/Auslagern von Daten, Begrenzung des regulären Zugriffs nach Behandlungsende)

Krankenhaus: _____

1. Liste der Verfahren und der dort gespeicherten (personenbezogenen) schutzbedürftigen Patientendaten:

Patientendaten	**Verfahren**					
	A	**B**	**C**	**D**	**E**	**F**
Identifikationsdaten (Name, Geburtsdatum, Wohnort, …)						
Versicherungsdaten						
Medizinische Daten						
Pflegedaten						
Befunde						
…						
…						

Verfahren A: _____

Verfahren B: _____

2. Eingesetzte Systeme zur Speicherung personenbezogener, schutzbedürftiger Patientendaten

System	**Merkmale**	**Einzelangaben**
System A	Hersteller	
	Programmversion	
	Hardware	
	Datenbank	
	…	
System B	Hersteller	

3. Begrenzung des regulären Datenzugriffs auf Behandlungsfälle für die Berufsgruppen des Krankenhauses mit Eintritt der aufgeführten Ereignisse und Fristen

   Die folgende Tabelle „**Fristen zur Zugriffsbeschränkung**“ enthält ein Beispiel für die Festlegung von ereignisgebundenen Zugriffsbeschränkungen.

Rolle/Berufsgruppe	**Ereignisse**							**Fristen zur Zugriffs-beschränkung**
	Erledgung eines Auftrags (Labor-, Röntgenbefund)	Erledgung einer Aufgabe (z. B. Konsiliarius)	Interne Verlegung/ Entlassung	Schlussrechnung	Rechnungsabschluss (mit Zahlungseingang)	Ablauf einer „Wiederaufnahmefrist“ nach Verlegung/Entlassung	…	
Arzt (in der Fachabteilung)				x				
Hinzugezogene Ärzte (Labor, …)	x							+ 6 Wochen
Konsiliarärzte		x						+ 6 Wochen
Pflegepersonal (in der Pflegeeinheit)			x					+ 1 Woche
Mitarbeiter im Funktionsdienst			x					+ 1 Woche
Mitarbeiter im medizinisch-technischen Dienst	x							
Patientenaufnahme						x		
Patientenverwaltung				x				
Patientenabrechnung					x			+ 1 Woche
Empfang			x					
Medizincontrolling					x			+ 6 Wochen (MDK-Frist)
…								

4. Umsetzung der Zugriffsbegrenzungen

Zugriffsbegrenzungen		**System**			
		A	**B**	**C**	**D**
Inhaltliche Umsetzung					
	Gemäß Tabelle „Fristen zur Zugriffsbeschränkung				
	Tab. „Fristen zur Zugriffsbeschränkung“ mit folgenden Abweichungen: - … - …				
Technische Umsetzung					
	Rollen- und Berechtigungskonzept				
	Kennzeichen zur Zugriffsbeschränkung				
	Datenauslagerung in System …				
	…				
Datenzugriff nach Zugriffsbeschränkung					
	Protokollierter Sonderzugriff mit Begründung				
	Befristete Wiedereinrichtung des regulären Zugriffs - Beschränkt auf bestimmte Rollen: o …				
	…				

5. Die Protokollierung der erfolgten Sonderzugriffe sowie die Übersicht über die zugriffsbeschränkten (dem regulären Zugriff entzogenen) Datensätze werden durch den Datenschutzbeauftragten regelmäßig überprüft.

Datum, Unterschrift Geschäftsführung

6.2 Musterformular Löschkonzept

Krankenhaus: _____

1. Liste der Verfahren und der dort gespeicherten (personenbezogenen) schutzbedürftigen Patientendaten:

Patientendaten	**Verfahren**					
	A	**B**	**C**	**D**	**E**	**F**
Identifikationsdaten (Name, Geburtsdatum, Wohnort, …)						
Versicherungsdaten						
Medizinische Daten						
Pflegedaten						
Befunde						
…						
…						

Verfahren A: _____

Verfahren B: _____

2. Eingesetzte Systeme zur Speicherung personenbezogener, schutzbedürftiger Patientendaten

System	**Merkmale**	**Einzelangaben**
System A	Hersteller	
	Programmversion	
	Hardware	
	Datenbank	
	…	
System B	Hersteller	

3. Aufbewahrungsvorschriften und technische Umsetzung der Löschung

Patientendaten	**Verfahren**	**Löschfrist**	**Anmerkungen**
Identifikationsdaten (Name, Geburtsdatum, Wohnort, …)			
Versicherungsdaten			
Medizinische Daten			
Pflegedaten			
Befunde			
…			
…			

4. Besondere Verkürzung der Aufbewahrung?

   Für folgende Daten werden verkürzte Aufbewahrungsfristen festgelegt:

   _____

   _____

   Vor Löschung ist als Teil des Risikomanagements eine Prüfung der Zulässigkeit durchzuführen und dabei auch die vertraglichen Bedingungen zu klären. Die Freigabe erfolgt ausdrücklich durch _____

   Es werden keine verkürzten Aufbewahrungsfristen vorgesehen.

5. Löschfristen

   Durch die IT-Leitung ist die Löschung aller mit Ablauf der festgelegten Aufbewahrungsfrist zur Löschung freigegebenen Patientendaten sicherzustellen. Die Löschung soll ___ Wochen nach Eintritt der Löschfrist abgeschlossen sein.

6. Löschprotokolle

   - Löschprotokolle sind zu erstellen und für ____ Jahre aufzubewahren

     Die Löschprotokolle sollen als Verfahrensprotokolle Auskunft geben über das Datum der Löschung, das gültige Löschkonzept (Version, Datum), das betroffene Verfahren, die angewandte Löschregel und die Anzahl der gelöschten Daten. Das Löschprotokoll darf keine personenbezogenen medizinischen Daten enthalten.

   - Löschprotokolle werden nicht erstellt

Datum, Unterschrift Geschäftsführung