Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen

I. Vorbemerkung

II. Technische Anforderungen

1. Struktur der Daten im PAS
2. Systemfunktionen
3. Anwendungsfunktionen
4. Rollen- und Berechtigungskonzept
5. Datenpräsentation
6. Systemzugang
7. Protokollierung / Auswertung von Protokolldaten
8. Technischer Betrieb, Administration

III. Anhang

Version 3, Stand: 26. November 2026

I. Vorbemerkung

Das vorliegende Papier ist der zweite Teil der „Orientierungshilfe Krankenhausinformationssysteme“ 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 (KIS). Sie nehmen auf die in Teil I der Orientierungshilfe dargestellten „Rechtlichen Rahmenbedingungen“ für den Einsatz von KIS Bezug und geben Hinweise zu einer datenschutzkonformen Gestaltung und einem datenschutzgerechten Betrieb dieser Systeme.

Dieser Teil der Orientierungshilfe 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 alle anderen Subsysteme eines KIS übertragbar. Das PAS wie das KIS 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.

Ein solches, datenschutzkonformes Zusammenwirken über Schnittstellen muss auch beim Einsatz von externen Komponenten und Systemen gewährleistet sein, die personenbezogene Daten aus dem KIS für ihre Funktionalität benötigen oder selbige an das KIS übertragen, um eine Weiternutzung dort zu ermöglichen. Beispielhaft seien hier die „elektronische Patientenakte“ (ePA) oder weitere Gesundheitsanwendungen genannt, welche über die sogenannte Telematikinfrastruktur der gematik an Systeme von Leistungserbringern angeschlossen sind. Diese (aus Sicht des KIS) externen Systeme müssen über besonders abgesicherte Schnittstellen angebunden werden, die mit technischen Maßnahmen Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen. Über solcherlei abgesicherte Schnittstellen könnten ebenso Datentransfers erfolgen, welche Forschungszwecken, Analysen im Big-Data-Kontext oder der Weiterverarbeitung durch KI-Systeme dienen. Für diese beispielhaft genannten Szenarien zur Nachnutzung personenbezogener Gesundheitsdaten sind über die Absicherung der genutzten Schnittstellen mithilfe technischer Maßnahmen hinaus vor allem auch rechtliche Anforderungen insbesondere bezüglich Verantwortlichkeiten und Rechtsgrundlagen zu klären.

Bei den im Folgenden dargestellten technischen 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 Art. 25, 32 Datenschutz-Grundverordnung (DSGVO) bzw. ggf. den entsprechenden Regelungen in den Landesdatenschutzgesetzen und kirchlichen Rechtsgrundlagen zurück; auf die jeweils relevanten Kontrollen bzw. Gewährleistungsziele wird in diesem Fall verwiesen.

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

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 Gewährleistungsziel erreicht wird.

Der datenschutzkonforme Einsatz eines KIS 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 und diese gemäß dem Stand der Technik umgesetzt sind. Einsetzende Institutionen sind angehalten entsprechende Funktionalitäten beim Hersteller des KIS einzufordern.

Im zweiten Schritt bedarf es einer Konfiguration des Systems, die im Betrieb die datenschutzrechtlichen Anforderungen berücksichtigt, indem datenschutzfreundliche Voreinstellungen zur Erfüllung der Anforderungen gemäß Art. 25 Abs. 2 DSGVO gewählt werden. Dies liegt in der Verantwortung der Betreiber der Systeme als datenschutzrechtlich Verantwortliche.

Technische und organisatorische Maßnahmen müssen dem Stand der Technik entsprechen. Die konkret erforderlichen Maßnahmen müssen auf Basis einer Risikoanalyse ermittelt werden. In aller Regel ist für die Verarbeitungen im Krankenhaus, die mit Hilfe des KIS und weiterer Subsysteme durchgeführt werden, eine Datenschutzfolgenabschätzung (DSFA) erforderlich. Zur Konkretisierung des Standes der Technik dienen u. a. einschlägige Normen, Standards und Empfehlungen. Für Krankenhäuser existiert mittlerweile ein Branchenstandard B3S, der für Betreiber Kritischer Infrastruktur verpflichtend ist, jedoch auch von anderen Häusern als Maßstab herangezogen werden solle. Zudem sind die Vorgaben neuerer Regelungen wie der NIS2-Richtlinie und der deutschen Umsetzungsgesetze zu beachten. Darüber hinaus sind bei Nutzung von Cloudressourcen die Anforderungen des § 393 SGB V sowie des C3A-Katalogs des BSI[2] zu beachten.

Entsprechend der jeweiligen Zuständigkeiten werden die Anforderungen 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 sowie die Wahl von datenschutzfreundlichen Voreinstellungen 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").

[2]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf?__blob=publicationFile&v=6

Bei nicht erfüllten zwingenden Anforderungen an Konfiguration und Nutzung des KIS durch den Betreiber ist ein datenschutzkonformer Betrieb des KIS nicht gegeben. Sofern passend und sinnvoll wird auf entsprechende Gewährleistungsziele des Standard-Datenschutzmodells referenziert, um anhand der dort aufgeführten (generischen) Umsetzungsmaßnahmen (ergänzt durch die vorhandenen Bausteine aus dem Maßnahmenkatalog) eine erste Orientierung zur Adressierung der genannten Anforderung zu bieten.

Die vorliegende dritte Fassung der Orientierungshilfe trägt dem Umstand Rechnung, dass mit der DSGVO nunmehr ein neuer Rechtsrahmen etabliert wurde, welcher vor allem auf Basis der Vorgaben nach Art. 32 i.V.m Art. 24, 25 und Art. 35 die technische und organisatorische Gestaltung von KIS prägt.

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, der Patientin bzw. dem Patienten, und einem Behandlungsfall zugeordnet. Es enthält Attribute, die sich nach ihrer Semantik in folgende Kategorien einteilen lassen:

- Identifikationsdaten der Patientin oder des Patienten,
- Verwaltungsdaten
- medizinische und pflegerische Daten.

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

Alle Daten, die einem Behandlungsfall zugeordnet sind, bilden die (einrichtungsinterne) Fallakte der Patientin bzw. des Patienten. Alle Fallakten zu einer Patientin bzw. einem Patienten bei ein und demselben Krankenhaus bilden ihre bzw. seine (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. 17).	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. 17).	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. 23).	B	Muss

1.4	Jedes Datenobjekt, das sich auf eine einzelne Patientin oder einen einzelnen Patienten bezieht, ist genau einer Fallakte, in Systemen mit mehreren Mandanten jede Fallakte genau einem Mandanten zuzuordnen (Teil I, Tz. 20, 23). Aus der Fallakte muss sich ergeben, welche leitende Ärztin bzw. welcher leitendende Arzt oder welche Ärztin bzw. welcher Arzt für die Behandlung zu gegebenem Zeitpunkt die Verantwortung tragen.	HB	Muss
1.5	Für Datenobjekte, welche Patientinnen oder Patienten betreffen, die ambulant in Nebentätigkeit einer privat liquidierenden Ärztin bzw. eines privat liquidierenden Arztes oder durch eine Belegärztin bzw. einen Belegarzt behandelt werden, muss das PAS die Möglichkeit bieten, Berechtigungen an diesen Status anknüpfen zu lassen, sofern für die behandelnde Ärztin bzw. den behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 11, 28)	H	Muss
1.6	Eine Fallakte muss Angaben aufnehmen können, welchen funktionsbezogenen Organisationseinheiten eine Patientin oder ein Patient derzeit zugeordnet ist. Flexible Mehrfachzuordnungen von Patientinnen oder Patienten zu Ärztinnen oder Ärzten bzw. medizinischen Organisationseinheiten (OE) müssen möglich sein (Teil I, Tz. 8). Hierbei soll zwischen Behandlung und Konsil unterschieden werden können. Ziel ist es, umfassende generelle Zugriffsrechte zu vermeiden und stattdessen die im Rahmen der Behandlung erforderlichen Zugriffe abzubilden bzw. technisch vorzusehen (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. Werden z. B. aus Haftungsgründen Bestätigungen (Vidierungen, 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 bestätigt wurde und ggf. durch wen .	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 Verantwortlichen sollen die Einteilung der Daten nach Kategorien nutzen, um den Zugriff von Beschäftigten auf die von ihnen für den Verarbeitungszweck benötigte Datengrundlage zu begrenzen. (Teil I, Tz. 1, 6)	B	Soll
1.9	Für jede Fallakte muss erkennbar sein, ob der Krankenhausaufenthalt beendet und ob der Behandlungsfall administrativ abgeschlossen ist (Teil I, Tz. 16).	HB	Muss
1.10	Das PAS muss die Möglichkeit bieten, einen Widerspruch der Patientin bzw. des Patienten gegen die Verarbeitung von Daten aus einer Vorbehandlung wirksam umzusetzen. (Teil I, Tz. 20).	H	Muss
1.11	Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält ob eine Auskunftssperre gilt.	H	Muss

1.12	Darüber hinaus sollte das System eine konfigurierbare Anzahl von deutlich wahrnehmbaren Kennzeichen aufnehmen können, die festhalten, welche weiteren Einwilligungen (z.B. zur Datenübermittlung an Folgebehandler) von den Patienten abgegeben oder verweigert wurden. Teil I, Tz. 4).	H	Sollte
1.13	In Systemfunktionen (z.B. Drucken von Arztbriefen) sind die Kennzeichen der Fallakte technisch zu beachten.	H	Muss
1.14	Fallakten sollen bei Bedarf dahingehend gekennzeichnet werden können, dass die Patientin bzw. der Patient zugleich Mitarbeiterin bzw. 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	Muss
	Das Kennzeichen darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden. (Teil I, Tz. 32)	B	Muss
1.15	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. 33). Die Kennzeichen nach dieser Tz. und Tz. 1.14 können in einem Kennzeichen zusammengefasst werden.	HB	Muss Muss
1.16	Die unter Tz. 1.11 bis 1.15 genannten Kennzeichen sollen nicht dazu verwendet werden können, gezielt nach solchen Patientinnen oder 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, 32, 33).	HB	Soll
1.17	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
1.18	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. Externe Komponenten für Auswertungen, die keinen Patientenbezug erfordern, dürfen nur dann auf den Datenbestand des PAS zugreifen, wenn eine Identifizierung von Patienten oder Patientinnen anhand der im Zugriff stehenden Daten ausgeschlossen ist (Datenminimierung, Nichtverkettung).	HB	Muss

2 Systemfunktionen

2.1	Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sollen präferiert werden (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 (Datenminimierung). Soweit eine redundante Datenhaltung unvermeidbar ist, müssen Zugriffsbeschränkungen und Löschungen in allen betreffenden Datenbeständen berücksichtigt werden (Teil I, Tz. 16, 21).	H HB	Sollte Muss
2.3	In das KIS sollte ein Single-Sign-On-Dienst integrierbar sein (siehe auch 6.2).	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. 23, 24).	HB	Muss
2.6	Kennzeichen nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.15 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 Kennzeichen nach Tz. 1.5 und 1.9 ist dies zwingend erforderlich (Teil I, Tz. 7, 28).	HB	Soll
2.7	Kennzeichen (z.B. die Verweigerung einer Einwilligung in eine Datenübermittlung) müssen bei der entsprechenden Verarbeitung nicht nur Warnhinweise auslösen, sondern technisch wirksam sein, z.B. durch das Verhindern von Druckausgaben. (siehe 1.13)	HB	Muss
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 aller zu einer Patientin bzw. einem Patienten im KIS gespeicherten Daten zu erzeugen (Teil I, Tz. 34 bis 36). Diese Funktionen dienen vor allem der Datenschutzkontrolle, der Transparenz, der Gewährung der Einsichtnahme in die Patientenakte nach § 630g BGB sowie der Beantwortung von Auskunftsersuchen gem. Art. 15 DSGVO.	H	Muss
2.9	Es muss möglich sein, zeit- und ereignisgesteuert die Zugriffsberechtigungen für abgeschlossene (siehe 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 einer Patientin bzw. eines 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. 16, 17).	H	Muss Soll

2.10	Das Krankenhaus muss einen Zeitraum von nicht länger als einem Jahr festlegen, nach dem der Zugriff auf abgeschlossene Fallakten gemäß Tz. 2.9 spätestens beschränkt wird (Teil I, Tz. 19).	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 (sog. „Soft Deletes"), 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. 21).	H	Muss
2.13	Das PAS muss über eine Funktion verfügen, die es ermöglicht, einzelne Datenfelder oder Behandlungsfälle zu löschen.	H	Muss
	Diese Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Beschäftigten eingesetzt werden oder gemäß der Regelungen im Löschkonzept.	B	Muss
2.14	Eine Komponente des 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. (Datenminimierung; Vertraulichkeit)	H	Soll
	Nicht-pseudonymisierte Daten dürfen nur dann ins Testsystem repliziert werden, wenn dies für die Fehleranalyse unabdingbar ist.	B	Muss
2.15	In das KIS muss ein Pseudonymisierungsdienst eingebunden werden, der verwendungszweckspezifisch temporäre Patientenkennzeichen oder Pseudonyme auf der Basis der gespeicherten Identitätsdaten generiert und verwaltet[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 (unbefugte) Offenlegung 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 Offenlegungen innerhalb des Krankenhauses unterbinden sollen, wirksam zu unterstützen (Tz. 2.18 bis 2.19).

[3] Dieser Pseudonymisierungsdienst ist eine technisch-organisatorische Datensicherheitsmaßnahme. Darf ein Empfänger nur pseudonymisierte Daten erhalten, muss zusätzlich geprüft und sichergestellt werden, dass eine Zuordnung eines Datensatzes zu der betroffenen Patientin bzw. dem betroffenen Patienten mit verhältnismäßigem Aufwand ohne zusätzliche Informationen nicht möglich ist. Die für eine solche Zuordnung benötigten zusätzlichen Informationen müssen gegen unbefugte Kenntnisnahme oder Nutzung geschützt werden.

2.16	Für die Übertragung von Patientendaten zwischen Komponenten des KIS soll eine Transportverschlüsselung verwendet werden.	HB	Soll
	Werden im Zuge des Datenaustauschs zwischen verschiedenen Komponenten des KIS Dienstleistungen externer Provider in Anspruch genommen, muss für eine Transportverschlüsselung gesorgt werden. Die Schlüssel dürfen sich nur in alleiniger Kontrolle des Krankenhauses befinden.	HB	Muss
2.17	Speichermedien, welche die Daten des KIS aufnehmen, müssen nach dem Stand der Technik verschlüsselt werden (durch Datenträger- oder Dateisystemverschlüsselung).	B	Muss
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	Bei der Nutzung von Clouddiensten muss der Cloudanbieter ein detailliertes Konzept zur Verschlüsselung vorlegen, das dann vom Krankenhaus auf seine Eignung hinsichtlich der Sensibilität der zu speichernden Daten geprüft wird. Insbesondere sollte daraus klarwerden, ob eine echte Ende-zu-Ende-Verschlüsselung vorliegt oder der Anbieter die technische Möglichkeit zur Kenntnisnahme der Daten hat. Auch die Verwaltungshoheit und Zugriffsmöglichkeiten auf das kryptographische Schlüsselmaterial müssen klar ersichtlich sein.	H B	Muss
2.20	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.	HB	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 sind, 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).	B	Muss

3.3	Die Nutzenden 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 Datenfelder sowie die in eine Suche einzubeziehenden Patientinnen bzw. 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)	H	Muss
3.5	Das PAS muss über eine Funktion verfügen, mit der im Rahmen der Aufnahme einer Patientin bzw. 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 einer Patientin bzw. 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. 21)	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. 10)	H	Muss
3.8	Ein PAS soll eine Funktion zur Bestätigung (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein. (Integrität, Transparenz)	H	Soll
3.9	Ein PAS soll es erlauben, Nutzende zur Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9). (Integrität, Transparenz)	H	Soll
3.10	Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden.	HB	Soll
3.11	Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten einer Patientin bzw. eines Patienten durch ein Pseudonym zu ersetzen[4].	HB	Soll
3.12	Die Speicherorte von Gesundheitsdaten sowie die Möglichkeit zum Export von Daten sollen durch Konfiguration beschränkbar sein, z. B. soll die lokale Datenspeicherung auf Arbeitsplatzrechnern unterbunden werden können. (Datenminimierung, Vertraulichkeit)	HB	Soll

[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.

4 Rollen- und Berechtigungskonzept

Berechtigungen regeln, wer auf welche Daten welcher Patientinnen bzw. Patienten wann bzw. zu welchem Zweck 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 sind und die Patientinnen und Patienten behandelt werden. Andere Berechtigungen ergeben sich über diese Zuordnung hinaus dynamisch, insbesondere aus Leistungsanforderungen und anderen ärztlichen Entscheidungen heraus. Damit diese Entscheidungen berechtigungswirksam werden, bedürfen sie der elektronischen Dokumentation und der Fähigkeit des Systems auf das Vorliegen der Anordnung zu reagieren. Schließlich können sich Berechtigungen auch situationsbezogen ergeben, insbesondere dann, wenn die Beschäftigten auf unvorhergesehene Umstände reagieren müssen. Diese Umstände können sowohl in einem medizinischen Ereignis begründet sein, als auch in ungeplanten organisatorischen Lagen. Eine gängige und zulässige Möglichkeit für den Umgang mit diesen speziellen Situationen ist unten in Tz. 4.9 beschrieben.

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

- Zuordnung der Patientin bzw. des Patienten zu Organisationseinheiten (Teil I, Tz. 7)
- Dokumentierte ärztliche Anweisungen (u.a. Leistungsanforderungen) und explizite Delegierungen (Teil I, Tz. 7, 8, 9)
- Datenkategorie (Teil I, Tz. 1, 7)
- Kennzeichen nach 1.4 bis 1.6, 1.9, 1.11 bis 1.15 (s. dort)
- Ersteller des Datenobjekts / eines Datenobjekts in der Patientenakte (Teil I, Tz. 9, 11, 16)

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 zur Patientin bzw. zum Patienten (Teil I, Tz. 7, 9), Sollte
- implizit oder explizit erklärtem Verarbeitungskontext (Teil I, Tz. 1, 7),
- einem Dienst- oder Bereitschaftsplan (Teil I, Tz. 13 und 14), und
- dem hinterlegten Behandlungspfad der Patientin bzw. des Patienten (Teil I, Tz. 8)

zu erteilen (vgl. Tz. 4.8)

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

- Ärztliche Beschäftigte (Teil I, Tz. 7ff.)
- Nicht-ärztliches medizinisches Fachpersonal (z. B. Pflegekräfte) (Teil I, Tz. 12ff.)

- Verwaltungskräfte
- Ausbildungskräfte
- Externe Kräfte (Teil I, Tz. 11)
- Technische Administration (Teil I, Tz. 29ff.)

4.3	Zur Definition von Rechten muss es möglich sein, Organisationseinheiten flexibel und überlappend zu definieren (Teil I, Tz. 7, 8). Beispielsweise überlappen sich die OE „psychiatrischer Konsiliardienst“ und „psychiatrische Fachabteilung“, wo beide bestehen, so dass es möglich sein muss, eine Fachärztin bzw. 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 jederzeit nachvollzogen werden kann. (Transparenz, Datenschutzkontrolle)	B	Muss
4.5	Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Nutzende vergebenen Berechtigungen in einer Übersicht darzustellen. (Transparenz, Datenschutzkontrolle). Die Übersicht muss auch für einen beliebigen Zeitpunkt in der Vergangenheit (analog zur Aufbewahrungsdauer der Protokollierungsdaten) erstellt werden können, um eventuell vorgeworfene Datenschutzverstöße aufklären zu können.	H	Muss Muss
4.6	Das PAS muss über eine Funktion verfügen, die es erlaubt, für bestimmte Berechtigungen in einer Übersicht diejenigen Nutzenden darzustellen, die über diese Berechtigung verfügen. Insbesondere muss es für ein gegebenes Datenobjekt effizient bestimmt werden können, welche Beschäftigten darauf schreibend oder lesend zugreifen können. (Transparenz, Datenschutzkontrolle) Die Übersicht muss auch für einen beliebigen Zeitpunkt in der Vergangenheit (analog zur Aufbewahrungsdauer der Protokollierungsdaten) erstellt werden können, um eventuell vorgeworfene Datenschutzverstöße aufklären zu können.	H	Muss
4.7	Das PAS muss über Funktionen verfügen, mit denen ein Behandlungsfall a) zur Mitbehandlung einer weiteren funktionsbezogenen Organisationseinheit oder einzelnen Behandelnden– bei Bedarf auch kurzfristig – dauerhaft, befristet oder auftragsbezogen zugewiesen werden kann (Teil I, Tz. 8, 9) und b) im Rahmen einer Verlegung einer anderen funktionsbezogenen Organisationseinheit dauerhaft zugewiesen werden kann. Das Rollen- und Berechtigungskonzept muss anknüpfend an die Zuweisung den Zugriff der anderen Organisationseinheit ermöglichen. (Teil I, Tz. 8, 13, 14)	H B	Muss Muss
4.8	Rollen und Berechtigungen z. B. für Bereitschaftsdienste oder Vertretungen müssen einer Benutzerkennung – bei Bedarf auch kurzfristig – 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. 9 und 13). Verantwortlichkeiten zur Rollen- und Berechtigungsvergabe sind im entsprechenden Rollen- und Berechtigungskonzept festzulegen.	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. 10), Zugriffe im Rahmen retrospektiver Prüfungen oder Zugriffe im Rahmen der Qualitätssicherung (Teil I, Tz. 16).	HB	Muss
	Dabei ist ein zweistufiges Verfahren vorzusehen, bei dem vor der Ausführung einer Transaktion in einem ersten Schritt	H B	Muss Soll
	• eine Begründung für die Erforderlichkeit der Transaktion eingegeben wird (vgl. Tz. 3.9) oder • die Bestätigung durch einen zweiten berechtigten Beschäftigten erfolgen muss (4-Augen-Prinzip)		
	und erst im zweiten Schritt der Zugriff eröffnet wird. Dabei soll die Möglichkeit bestehen, den Zugriff zeitlich zu beschränken (z. B. auf 24 Std.)		
	Auf die Erweiterung der Zugriffsrechte und die Protokollierung des Zugriffs (vgl. 7.11) soll zuvor hingewiesen werden.	H B	Muss Soll
4.10	Zur Authentisierung von Beschäftigten gegenüber dem KIS muss eine Multifaktor-Authentifizierung eingesetzt werden. Eine Ausnahme besteht für Fälle, in denen diese im Klinikalltag nicht praktikabel wäre und das erforderliche Schutzniveau auf andere Weise erreicht wird. Das KIS sollte es ermöglichen, Datenzugriffe an die Anwesenheit eines bestimmten Nutzenden, nachgewiesen z. B. durch Präsenz eines maschinenlesbaren Mitarbeiterausweises, eines RFID-Tags oder eines vergleichbaren Tokens zu knüpfen (Transparenz, Nichtverkettbarkeit, Vertraulichkeit).	HB	Muss
4.11	Es muss sichergestellt sein, dass es keinem der Nutzenden 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 (Nichtverkettbarkeit, Vertraulichkeit).	H	Muss
4.12	Der Umfang der Zugriffsberechtigungen einer Benutzerin oder eines Benutzers darf sich allein aus der Gesamtheit der ihr bzw. ihm zugeordneten strukturellen und funktionellen Rollen ergeben. (Nichtverkettbarkeit, Datenminimierung, 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 (Datenminimierung, 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. Die Berechtigungen von Sammelkonten müssen auf das unbedingt notwendige Maß reduziert werden, insbesondere im Hinblick auf Schreibzugriffe. (Transparenz, Integrität, Vertraulichkeit)	B	Muss

4.15	Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzerinnen bzw. Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Datenminimierung, Nichtverkettbarkeit, Vertraulichkeit, Integrität).	H	Muss
4.16	Die Benutzerverwaltung muss über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Beschäftigten automatisiert zu deaktivieren.	H B	Muss Sollte
4.17	Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer oder Benutzerinnen 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. 29 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 der Patientin bzw. des Patienten zu konfigurieren, z. B. für Schulungszwecke.	H	Muss
5.2	Das PAS soll es ermöglichen, in Abhängigkeit vom Verarbeitungskontext Teile der Patientenakte mit Pseudonymen oder temporären Patientenkennzeichen, die die Identitätsdaten der Patientin bzw. des Patienten ersetzen, darzustellen[5].	HB	Soll
5.3	Das PAS sollte die Oberflächen verschiedener Verarbeitungskontexte klar voneinander optisch (z. B. farblich) unterscheiden, um es Nutzenden 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, Nutzende aufzufordern, den Zugriff mit erweiterten Rechten nur solange zu nutzen, wie dies erforderlich ist.	H	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

5.4	Es muss die Möglichkeit bestehen die Kennzeichen nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.15 in Bildschirmmasken zu integrieren, um, wo es erforderlich oder hilfreich ist, Nutzenden einen Hinweis zu geben, im Kontext welches Mandanten sie operieren, ob für die Patientin bzw. den Patienten eine Auskunftssperre eingerichtet wurde, welcher bzw. welchen Organisationseinheiten eine Patientin bzw. ein Patient zugeordnet ist bzw. war, ob die Behandlung und/oder Abrechnung bereits abgeschlossen ist oder die Patientin bzw. der Patient einer besonders schutzwürdigen Gruppe angehört.	H	Muss

6 Systemzugang

6.1	Ein PAS muss einen schnellen Benutzerwechsel[6] 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 (siehe auch 2.3).	HB	Sollte
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. (Datenminimierung, Nichtverkettung, Vertraulichkeit)	HB	Muss
6.4	Wird beim Login (als einer der beiden einzusetzenden Faktoren) ein Token eingesetzt, so sollte nach Login von Nutzenden das Entfernen des Tokens zur Sperrung, das Einführen des Tokens zur Freischaltung der Arbeitsstation, insbesondere nach einer Bildschirmsperre (siehe 6.3) 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. (Datenminimierung, Nichtverkettung, Vertraulichkeit, Transparenz)	H H	Sollte Muss

7 Protokollierung / Auswertung von Protokolldaten

Die Vorgaben in diesem Kapitel dienen der Umsetzung der in Teil I, Tz. 34 bis 37 aufgeführten Anforderungen.

Hinsichtlich der Protokollierung wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Protokollierung in zentralen Verfahren der Gesetzlichen Krankenversicherung[7] übernommen, soweit sie inhaltlich

[6] „schneller Benutzerwechsel" ist ein stehender technischer Begriff. Hierbei kann ein neuer Benutzer am System angemeldet werden ohne den aktuellen Benutzer abmelden zu müssen

[7] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Orientierungshilfen/OH_ProtokollierungshilfeGKV.pdf?__blob=publicationFile&v=6

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. Darüber hinaus kann der Baustein 43 „Protokollieren“[8] aus dem Standard Datenschutzmodell, welches eine Systematisierung der rechtlichen Anforderungen der DSGVO mithilfe sogenannter Gewährleistungsziele erlaubt, Hinweise zu konkret umzusetzenden Maßnahmen geben.

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 Beschäftigtenvertretung. 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

[8] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf

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	Es darf technisch nicht möglich sein, vorgesehene Protokollierungen zu umgehen.	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 Gesundheitsdaten i.S.v. Art. 9 Abs. 1 DSGVO enthalten. (Datenminimierung, Vertraulichkeit)	HB	Soll
7.10	Neben der Anmeldung am Verfahren (Login/Logout) müssen die Zugriffe Nutzender mit zumindest folgenden Angaben protokolliert werden: - Zeitpunkt des Zugriffs, - Kennung der jeweiligen Benutzerin bzw. des jeweiligen Benutzers, - Kennung der jeweiligen Arbeitsstation, - aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung), - betroffene Patientinnen bzw. 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. Die Protokolle der Transaktionsausführungen mit besonderer Begründung (Tz. 4.9) sind getrennt von anderen Protokollen zu führen.	H H	Muss Soll
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. 30).	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. 31).	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. 31).	B	Muss
7.15	Die Löschung von Daten muss insoweit protokolliert werden, als für einzelne Daten der Zeitpunkt der Löschung und die jeweilige Benutzerin bzw. der jeweilige Benutzer,	HB	Muss

für Datensätze zusätzlich die jeweilige Fallnummer oder vergleichbare Identifikationsmerkmale festgehalten werden.

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 des Datenschutzbeauftragten 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. Abweichungen von der personellen Rollentrennung hinsichtlich dieser drei Bereiche sind nur ausnahmsweise, solange besondere, zu dokumentierende Gründe vorliegen, gerechtfertigt.	B 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. 31).	B	Muss
8.3	Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 31).	H	Soll
8.4	Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können, wobei die Systemkonsistenz zu wahren ist. (Vertraulichkeit, Integrität)	H	Muss
8.5	Fernwartungsarbeiten müssen über verschlüsselte Verbindungen und unter separaten, über Identifikations- und Authentisierungsmechanismen geschützten Benutzerkennungen durchgeführt werden. Hierbei ist immer eine MFA einzusetzen. Deren Zugriffsmöglichkeiten müssen auf das für die Durchführung der Wartungsarbeiten erforderliche Maß beschränkt sein; erforderlichenfalls sind mehrere Wartungskennungen einzurichten (Teil I, Tz. 31).	H, B	Muss
8.6	Die Inbetriebnahme von neuen Softwareversionen und eigenprogrammierten Änderungen muss nach den Regeln des Abschnitts Softwaretest und Freigaben des B3S-Standards erfolgen. Bei Systemen mit mehreren Mandanten ist die Mandantentrennung besonders zu testen.	B	Muss
8.7	Die im Rahmen des Betriebs des KIS notwendigen technischen und organisatorischen Maßnahmen des Datenschutzes sollen auf der Grundlage einer Risikoanalyse bzw. DSFA in einem Datenschutzkonzept und, soweit sie die Informationssicherheit betreffen, auf der Grundlage des B3S-Branchenstandards sowie der Vorgaben des IT-Grundschutzstandards 200-1 bis 200-4 des BSI bzw. der Vorgaben von NIS2 im Informationssicherheitskonzept festgelegt werden.	B	Soll
8.8	Beim Einsatz von Cloud gestützten PAS sind die Anforderungen aus § 393 SGB V zu beachten (Teil I, Tz. 40, 41). Weiterführende Maßnahmen i.S.d. Confidential Cloud Computing zur Erhöhung des Sicherheitsniveaus oder der digitalen Souveränität wie z.B. der der C3A Kriterienkatalog des BSI[9] sind zu prüfen.	HB	Muss

[9]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf?__blob=publicationFile&v=6

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 Patientinnen bzw. Patienten sie einsehen oder ändern dürfen als auch darauf, welche der zu der jeweiligen Patientin bzw. dem jeweiligen Patienten gespeicherten Daten eingesehen und welche eingegeben werden können. Je nach ihrer Rolle erhalten die Beschäftigten Zugriff auf die Daten der Patientinnen und Patienten nach deren Zuordnung zu Organisationseinheiten (Fachabteilungen, Stationen) oder auf der Grundlage einer ärztlichen Anweisung. In bestimmten strukturellen Rollen dürfen Beschäftigte von den ihnen regelhaft gesetzten Zugriffsbegrenzungen nach dem in Tz. 4.9 festgelegten Verfahren situationsbezogen und zeitlich limitiert abweichen.

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 der jeweiligen organisatorischen Struktur ab.

- Administrative Aufnahmekraft
- Medizinische Aufnahmekraft
- QS-Management
- Pflegekraft/Leitende Pflegekraft
- Funktionskraft
- Konsiliar
- Bereitschaftsdienst
- Belegärztin bzw. Belegarzt
- Behandelnde Ärztin bzw. behandelnder Arzt
- Honorar-Ärztin bzw. -Arzt
- Honorar-Pflegekraft
- Verwaltungsangestellte bzw. Verwaltungsangestellter
- Mitarbeiterin bzw. Mitarbeiter im Bereich der Forschung
- Controlling
- Datenschutzbeauftragte bzw. Datenschutzbeauftragter
- Revision
- Sekretariat / Hilfskraft
- Ausbildungskraft
- Wartung
- Anwendungsadministration

- Berechtigungsadministration
- Seelsorge

Beschäftigten können 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 einer Ärztin bzw. eines Arztes mit bestehendem Behandlungszusammenhang
    - Konsil
    - Behandlung im Bereitschaftsdienst außerhalb der fachlichen Zuordnung
    - Notbehandlung außerhalb eines Bereitschaftsdienstes und ohne fachliche Zuordnung der Patientin bzw. des Patienten zu einer OE der bzw. des Behandelnden
- 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 funktionellen Rollen finden sich in dem Standard ISO 21298:2017 Health informatics—Functional and structural roles.