Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen

Version 3 mit Stand: 26. November 2026

Allgemeines

Ziel des datenschutzgerechten Einsatzes eines Krankenhausinformationssystems (KIS) ist, dass jede und jeder Mitarbeitende auf diejenigen Patientendaten zugreifen können soll, die für die konkrete Aufgabenerfüllung erforderlich sind. Bei der Ausgestaltung eines Rollen- und Berechtigungskonzeptes und dessen technischer Umsetzung sind die Anforderungen des Klinikbetriebes zu berücksichtigen. Das eingesetzte KIS sollte dabei eine dynamische und kurzfristige Rechtevergabe unter Beachtung der Grundsätze der Datensicherheit und des Datenschutzes unterstützen. Das Ziel sollte sein, den Beschäftigten die von ihnen für ihre vorhersehbare tägliche Aufgabenerfüllung erforderlichen Zugriffsrechte auf Patientendaten bei Bedarf auch kurzfristig, mühelos und nachvollziehbar zuzuweisen. Aufgrund akuter Behandlungssituationen erforderliche Sonderzugriffe sollten soweit wie möglich vermieden werden.

Aufnahme

Bei der Aufnahme einer Patientin bzw. eines Patienten in das Krankenhaus spielen sowohl administrative als auch medizinische Belange eine Rolle. Abfolge und handelnde Beschäftige unterscheiden sich von Krankenhaus zu Krankenhaus und danach, ob es sich um eine geplante oder eine Notfallaufnahme handelt. In jedem Fall gilt: Der Umfang der Daten, welche die Beschäftigten jeweils verarbeiten dürfen, richtet sich nach den ihnen zugewiesenen Aufgaben. Der folgende Abschnitt verdeutlicht diese Einschränkung auf das Erforderliche für Beschäftigte, deren Wirkungskreis sich auf die administrativen Belange beschränkt.

1. Die Aufnahmekraft darf bei Eingabe der Identifikationsdaten der neuen Patientin bzw. des neuen Patienten (Suchfunktion) vom System erfahren, ob die Patientin bzw. der Patient schon einmal in demselben Krankenhaus behandelt wurde. Dies umfasst zunächst nur Identifikationsdaten (Name, Vorname, Patientennummer, etc.). Dabei kann zur klaren Identifizierung die Wild-Card-Funktion (abgekürzte Suche oder Ähnlichkeits-Suche) zugelassen werden (Ausschluss einer Doppelregistrierung derselben Person mit verschiedenen Schreibweisen) und in der Trefferliste neben Identifikationsdaten auch der Zeitraum des letzten stationären Aufenthalts angezeigt werden.

2. Eine Zugriffsmöglichkeit der administrativen Aufnahmekraft auf medizinische Daten mit Ausnahme der Einweisungsdiagnose ist mangels Erforderlichkeit nicht zulässig. Die Offenbarung einer vorbehandelnden funktionsbezogenen Organisationseinheit ist bei der administrativen Aufnahme zulässig.

3. Die Aufnahmekraft darf auch – möglichst standardisierte – Warnhinweise im Datensatz der Patientin bzw. des Patienten zur Kenntnis nehmen, die bereits vor der medizinischen Aufnahme administrative Maßnahmen erfordern. Dies gilt für frühere Betrugsversuche / Zahlungsunfähigkeit von Selbstzahlerinnen bzw. Selbstzahlern und für Hinweise auf die Trägerschaft multiresistenter Keime, die umgehend besondere Schutzmaßnahmen erfordern.

4. Das Krankenhaus muss die Möglichkeit vorsehen, Auskünfte über den Patientenaufenthalt durch die Pforte, andere Auskunftsstellen und das Stationspersonal zu sperren. (Ob diese als Regel einzurichten ist und eine Aufhebung der Einwilligung bedarf, oder ob eine Widerspruchslösung genügt, hängt von den landesgesetzlichen Regelungen ab. Für psychiatrische Patientinnen bzw. Patienten ist die Sperrung grundsätzlich einzurichten.) Die Einrichtung einer Auskunftssperre muss zur Folge haben, dass bei der Patientensuche durch Auskunftsstellen kein Treffer angezeigt wird. Bei anderen Stellen – insbesondere auf der jeweiligen Station – muss der Umstand der Auskunftssperre erkennbar werden.

5. Die medizinische und die administrative Aufnahme können von der gleichen Person abgewickelt werden. Im Zuge der medizinischen Aufnahme ist im erforderlichen Umfang die Kenntnisnahme und Verarbeitung von medizinischen Daten zulässig.

Behandlung

6. Jeder an der Behandlung beteiligte Mitarbeitende darf auf die Patientendaten zugreifen, die zur Erfüllung der ihm zugewiesenen Aufgaben im aktuellen medizinischen Kontext erforderlich sind, um eine optimale Gesundheitsversorgung sicherzustellen. Dies gilt auch im Hinblick auf Vorbehandlungsdaten.

Zugriffe im Rahmen der medizinischen und therapeutischen Behandlung

7. Eine Patientin bzw. ein Patient ist grundsätzlich zu jedem Zeitpunkt der Behandlung fachlich einer oder mehrerer funktionsbezogener Organisationseinheiten (OE) zuzuordnen. Der Zugriff auf die Patientendaten ist zunächst allen Mitarbeitenden der OE technisch zu gewähren. Ob von dieser Zugriffsmöglichkeit im Einzelfall Gebrauch gemacht wird, bestimmt sich nach der Erforderlichkeit für die Tätigkeit der einzelnen Mitarbeitenden.

8. Die Zuordnung der Patienten im weiteren Behandlungsverlauf zu einer oder mehrerer zusätzlichen OE, ist auf der Grundlage einer fachlichen dokumentierten Entscheidung jederzeit möglich.

9. Im Falle einer nur vorübergehenden Beteiligung von OE bzw. einzelner Personen an der Patientenbehandlung wie z.B. im Rahmen des Bereitschaftsdienstes oder bei einem medizinischen Konsil entscheidet die Einrichtung auf der Grundlage des Rollen- und Berechtigungskonzeptes, ob und gegebenenfalls für welche Dauer diese Zuordnung der Patienten mit den daraus resultierenden Zugriffsmöglichkeiten bestehen bleibt.

10. Ein darüberhinausgehender Sonderzugriff auf Patientendaten außerhalb des differenzierten Berechtigungskonzepts kann ausnahmsweise erforderlich sein. In diesem Fall ist die zugreifende Person durch einen automatisch erscheinenden Hinweis darüber aufzuklären, dass sie außerhalb ihrer Berechtigung zugreift, einen Zugriffsgrund angeben muss und der Zugriff protokolliert und anschließend kontrolliert wird. Die Kontrolle ist hinsichtlich der Methode und der kontrollierenden und auswertenden Personen vorher unter Beteiligung der Beschäftigtenvertretung und der/des betrieblichen bzw. behördlichen Datenschutzbeauftragten festzulegen. Mindestens regelhafte stichprobenartige Kontrollen durch das Krankenhaus sind geboten (siehe auch unten Tz. 31 und 35 ff.).

11. Belegärztinnen und -ärzte erhalten als eigene datenschutzrechtliche Verantwortliche nur Zugriff auf die Daten der von ihnen behandelten Patientinnen bzw. Patienten. Für die konkret an der Behandlung beteiligten Beschäftigten eines Beleg-Krankenhauses gilt Tz. 6.

Zugriffe im Rahmen der pflegerischen Behandlung

12. Das Pflegepersonal einer OE erhält die Zugriffsmöglichkeit auf alle der OE zugeordneten Patientendaten.

13. Sofern Pflegepersonal in unterschiedlichen OE eingesetzt wird (Springer), sind die Zugriffsrechte je nach konkretem Einsatzort und der hierfür benötigten Berechtigungen einzuräumen bzw. zu beschränken. Der Einräumung der Berechtigung sollte eine dokumentierte Zuweisung der konkreten Pflegeperson zu der jeweiligen OE zugrunde liegen.

14. Die in der Praxis zu beobachtende häufige Rotation des Pflegepersonals zwischen verschiedensten OE erfordert ein effizientes System der Vergabe und Dokumentation von Berechtigungen. Keinesfalls darf die notwendige Flexibilität und Agilität der Berechtigungsvergabe die Anforderungen an Transparenz oder das Need-to-Know-Prinzip außer Kraft setzen. Von den Herstellern werden geeignete Konzepte zur Berechtigungsvergabe erwartet.

Zugriffe außerhalb der bettenführenden Fachabteilungen

15. Ob und in welchem Umfang, unter welchen Voraussetzungen und für welche Dauer Personen im Krankenhausbetrieb mit fachrichtungsübergreifender Funktion (u. a. Seelsorge, Sozialdienst, Labor, Schreibdienst, Qualitätssicherung) Zugriffsbefugnisse auf Patientendaten erhalten, entscheidet die Einrichtung unter Beachtung der datenschutzrechtlichen Vorgaben und nach Einbindung des internen Datenschutzmanagements. Die Entscheidung ist im Rollen- und Berechtigungskonzept zu dokumentieren.

Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls

16. Nach Abschluss des Behandlungsfalles und Abwicklung der ihn betreffenden medizinischen und verwaltungsmäßigen Routinevorgänge sind die für Zwecke der unmittelbaren Behandlung und deren Abrechnung eingerichteten Zugriffsmöglichkeiten nicht mehr erforderlich und daher einzuschränken. Zur Erfüllung anderer, festgelegter Aufgaben kann der Zugriff für einen organisatorisch festgelegten Personenkreis bestehen bleiben.

17. Eine Übertragung dieser Aufgaben und Zugriffsrechte auf ein zentrales Patienten-/Fallmanagement bedarf zusätzlicher Sicherungsmaßnahmen (ggf. Buchstaben-Zuständigkeit, nur Leserecht, Protokollierung, Suche nur nach Fallnummern, ggf. nach vollem Patientennamen ohne Mustersuche u.a.), um einen zeitlich wie inhaltlich unbeschränkten Zugriff auf alle Patientenakten des Krankenhauses zu vermeiden.

18. Diese Zugriffsbeschränkung hat als technisch-organisatorische Maßnahme unabhängig davon zu erfolgen, ob und wann nach datenschutzrechtlichen Vorschriften eine Einschränkung der Verarbeitung i. S. v. Art. 18 Datenschutz-Grundverordnung (DSGVO) vorzunehmen ist.

19. Das Krankenhaus hat eine angemessene Frist (regelmäßig nicht länger als ein Jahr) nach Abschluss des Behandlungsfalls entsprechend den jeweiligen organisatorischen Abläufen im Krankenhaus festzulegen, innerhalb derer die Einschränkung der Zugriffsmöglichkeiten spätestens zu erfolgen hat.

20. Wird eine Patientin bzw. ein Patient nach Wirksamwerden der Zugriffsbeschränkung erneut behandelt, darf die Beschränkung des Zugriffs auf Daten aus früheren Behandlungsfällen aufgehoben werden. Der Zugriff auf Vorbehandlungsdaten ist aber nur soweit zulässig, wie das Landeskrankenhausrecht oder das Berufsrecht dies gestattet.

Löschung

21. Die Krankenhäuser trifft die Pflicht, zu prüfen, ob eine Löschung von Patientendaten vorzunehmen ist. Eine Löschung ist vorzunehmen, wenn die betreffenden personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden (insb. zur Durchführung des Behandlungsvertrags) nicht mehr notwendig (vgl. Art. 17 Abs. 1 Buchst. a DSGVO) und etwaige gesetzliche Aufbewahrungsfristen abgelaufen sind sowie kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange der Betroffenen beeinträchtigt werden. Das Verfahren zur Löschung ist in einem Löschkonzept festzulegen.

22. Patientendaten sind in zu löschen, wenn die betroffene Person dies verlangt und weder rechtliche Vorgaben oder die Regelungen im Löschkonzept einer Löschung entgegenstehen.

23. Krankenhäuser, die – eventuell über ihren Träger – einem öffentlichen oder kirchlichen Archiv zugeordnet sind, müssen ihr Löschkonzept mit dem jeweiligen Archiv abstimmen und somit die jeweils geltende Archivordnung einhalten. Bei der Abstimmung mit dem Archiv sind die grundsätzlich oder eventuell archivwürdigen Datenarten zu bestimmen und die Verfahren der Anbietung bzw. die Übergabe an das Archiv zu regeln. Die Übernahme durch das Archiv ersetzt im Sinne des Datenschutzrechts die Löschung.

Verarbeitung durch verschiedene Leistungserbringer

24. Patientinnen bzw. Patienten, die in anderen Krankenhäusern oder Einrichtungen des Trägers des Krankenhauses (z. B. in Medizinische Versorgungszentren gleich welcher Rechtsform) behandelt werden, werden dadurch nicht zugleich Patientinnen bzw. Patienten des Krankenhauses. Sie dürfen daher nur in den Patientenbestand der tatsächlich behandelnden Einrichtung aufgenommen werden. Ein gemeinsames (Krankenhaus und andere Einrichtung bzw. anderes Krankenhaus umfassendes) KIS ist allenfalls bei Trennung der Datenbestände in verschiedene Mandanten möglich.

25. Einrichtungs- und insbesondere mandantenübergreifende Zugriffe stellen datenschutzrechtlich Übermittlungen dar, deren Zulässigkeit sich nach geltendem Arzt- und Datenschutzrecht richtet. Beispiele für die zulässige Ausgestaltung derartiger Übermittlungen sind dem als Anlage zu dieser Orientierungshilfe beigefügten Szenarienkatalog zu entnehmen.

26. Eine Person kann mehreren Mandanten als Beschäftigte oder Beschäftigter zugeordnet werden. Greift eine solche Person im Zuge ihrer Tätigkeit für einen Mandanten auf Daten zu, die diesem Mandanten bereits zugeordnet sind, dann liegt keine Übermittlung vor.

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

28. Übermittelte Daten sind in die Primärdokumentation des empfangenden Krankenhauses zu übernehmen. Benutzen übermittelndes und empfangendes Krankenhaus unterschiedliche Mandanten des gleichen KIS, so müssen die übermittelten Daten von dem empfangenden Mandanten in seinen Datenbestand übernommen werden.

29. Ambulant in Nebentätigkeit von Krankenhaus-Ärztinnen bzw. -Ärzten behandelte Privatpatientinnen bzw. -patienten sind grundsätzlich nicht Patientinnen bzw. Patienten des Krankenhauses, sondern der insoweit berechtigten Ärztinnen oder Ärzte. Für Behandlungsakten von ambulant in Nebentätigkeit behandelten Privatpatientinnen bzw. Patienten hat die betreffende Ärztin bzw. der betreffende Arzt die alleinige datenschutzrechtliche Verantwortung. Soll die entsprechende Dokumentation im KIS erfolgen, sind entsprechende vertragliche Regelungen zwischen den Ärztinnen und Ärzten und dem Krankenhaus zu treffen.

30. Für gutachterliche Tätigkeiten sind vom Krankenhaus Prozesse zu etablieren, die sicherstellen, dass personenbezogene Daten von Patientinnen und Patienten Gutachtern, die in eigener datenschutzrechtlicher Verantwortung handeln, ohne Zugriff auf das KIS zur Verfügung gestellt werden.

Technische Administration

31. Durch technische und administrative Rollenteilung (z. B. zwischen Systemadministration und Administration der einzelnen Anwendungen) ist missbräuchlichen Datenzugriffen vorzubeugen. Die Zugriffsrechte und Eingriffsebenen der Administratoren sind entsprechend ihren spezifischen Aufgaben zu begrenzen.

32. Die Aktivitäten der Administratoren sind zu protokollieren. Dies gilt auch für eine eventuell notwendige Möglichkeit, Patientendaten auf Datenträger zu kopieren. Für die Nutzung der Protokolldaten zu Kontrollzwecken ist ein Auswertungskonzept zu erstellen (vgl. Tz. 10 und 35 ff.). Bei Remote-Zugriffen auf Arbeitsplatzrechner ist sicherzustellen, dass sie ausschließlich mit Kenntnis und Einwilligung der bzw. des Nutzenden erfolgen (können) und automatisch dokumentiert werden.

33. Bei einer (Fern-)Wartung durch Dritte/Externe sind besondere Maßnahmen erforderlich, damit die Wartung nur mit Wissen und Wollen des Krankenhauses im zugelassenen Umfang stattfinden kann.

Besonders schutzwürdige Patientengruppen

34. Beschäftigte des Krankenhauses als Patientinnen bzw. Patienten müssen davor geschützt werden, dass Kolleginnen bzw. Kollegen, deren Aufgabenbereich nicht betroffen ist (insb. die nicht unmittelbar an der Behandlung beteiligt sind), von ihrem Behandlungsaufenthalt erfahren (können). Soweit dies nicht bereits durch die oben beschriebenen Maßnahmen erreicht wird, kommt (zusätzlich) u.U. eine Aufnahme unter einem Pseudonym in Betracht. Dem ausdrücklichen Wunsch einer bzw. eines Beschäftigten nach Aufnahme unter einem Pseudonym ist – sofern keine zwingenden legitimen Interessen entgegenstehenden - zu entsprechen. Die Zuordnung von Pseudonym zu tatsächlichem Namen ist geschützt und nur einem eng begrenzten Personenkreis zugänglich aufzubewahren. Für Einzelfälle, in denen Pseudonymisierungen technisch nur mit unverhältnismäßigem Aufwand umgesetzt werden können, müssen funktionsäquivalente kompensatorische Schutzmaßnahmen genutzt werden.

35. Für Patientinnen bzw. Patienten, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, gilt grundsätzlich dasselbe. Die Festlegung trifft die Klinikleitung auf Antrag der Patientin bzw. des Patienten. Patientinnen bzw. Patienten sind über die Möglichkeit zur Pseudonymisierung oder den Einsatz funktionsäquivalenter kompensatorischer Schutzmaßnahmen in geeigneter Weise zu informieren.

Zugriffsprotokollierung und Datenschutzkontrolle

36. Aufgrund von Art und Umfang der in einem KIS verarbeiteten medizinischen und administrativen Daten bedarf es einer Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Diese ist Voraussetzung, um z. B. Nachweispflichten (vgl. Art. 5 Abs. 2 DSGVO) bezüglich getroffener technischer und organisatorischer Maßnahmen (vgl. Art. 32 DSGVO) zur Gewährleistung datenschutzrechtlicher Grundsätze wie Integrität und Vertraulichkeit (vgl. Art. 5 Abs. 1 Buchst. f DSGVO) zu erfüllen. Grundlage hierfür ist eine aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe sowie geeignete Auswertungsmöglichkeiten (siehe bereits oben Tz. 10 und 31).

37. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise eingesehen oder anderweitig verarbeitet hat. Dies betrifft sowohl Zugriffe aus der fachlichen Verfahrensnutzung (einschließlich des Zugriffs auf sog. Patientenübersichten mit Angaben zu der behandelnden Abteilung, Diagnosen etc.) als auch aus der administrativen Bearbeitung. Dabei gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.

38. Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle ist ebenso Aufgabe des Krankenhauses wie eine Kontrolle aus konkretem Anlass (s. Tz. 31). Aufnahmevorgänge, die nicht mit einer abrechnungsfähigen Behandlung in Verbindung stehen, müssen kontrolliert werden.

Einsichts- und Auskunftsrechte der Patientinnen und Patienten

39. Patientinnen und Patienten haben nach Art. 15 DSGVO das Recht, vom Krankenhaus Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten sowie eine Kopie dieser Daten zu erhalten, soweit keine Rechte und Freiheiten anderer Personen oder erhebliche therapeutische Gründe (§ 630 g Abs. 4 S. 3 BGB) entgegenstehen. Der Anspruch umfasst auch die in der Patientenakte gespeicherten Gesundheitsdaten, wie Diagnosen, Befunde, Untersuchungsergebnisse, Angaben zu Behandlungen, Eingriffen, Medikation und sonstige behandlungsbezogene Dokumentationen. Die Auskunft ist vollständig, transparent und in verständlicher Form zu erteilen. Die Auskunft ist unabhängig von der Motivation der Patientin oder des Patienten zu gewähren, also auch dann, wenn die Auskunft beispielsweise der Prüfung eines vermuteten Datenmissbrauchs oder möglicher Behandlungsfehler dienen soll. Die Auskunft nach Art. 15 DSGVO umfasst neben personenbezogenen Daten selbst insbesondere auch Angaben zu den Verarbeitungszwecken, den Kategorien personenbezogener Daten, den Empfängern oder Kategorien von Empfängern, gegenüber denen die Daten offengelegt wurden oder noch offengelegt werden, falls möglich der Speicherdauer, alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, sowie den bestehenden Betroffenenrechten. Die erste Kopie der personenbezogenen ist grundsätzlich unentgeltlich zur Verfügung zu stellen. Wird der Antrag elektronisch gestellt, sind die Informationen grundsätzlich in einem gängigen elektronischen Format bereitzustellen, sofern die betroffene Person nichts Anderes angibt. Bei elektronischer Auskunftserteilung sind nach Art. 12 Abs. 3 Satz 4 DSGVO angemessene technische und organisatorische Sicherungsmaßnahmen zu treffen. Bei einem besonderen berechtigten Interesse, z.B. bei einem konkreten Datenmissbrauchsverdacht, kann das Auskunftsrecht auch Informationen darüber umfassen, wer zu welchem Zeitpunkt welche Daten zur Kenntnis genommen hat. Soweit

lesende Zugriffe zulässigerweise nicht vollständig protokolliert werden, kann es genügen, den Kreis der Personen zu benennen, die die Daten aufgrund ihrer Zugriffsrechte hätten zur Kenntnis nehmen können, z.B. Pflegepersonal der Station X oder Ärztinnen und Ärzte der Fachabteilung A.

40. Neben dem datenschutzrechtlichen Auskunftsanspruch besteht weiterhin das zivilrechtliche Recht auf Einsichtnahme in die Patientenakte nach § 630g BGB sowie ggf. aus Landeskrankenhausgesetzen, falls geregelt. Die Einsicht kann durch unmittelbare Einsichtnahme, durch Zurverfügungstellung einer Abschrift oder durch elektronische Abschrift gewährt werden. Auch nach der zivilrechtlichen Regelung (§ 630g Abs. 1 S. 4 BGB) ist Patientinnen und Patienten die erste Abschrift bzw. Kopie der Behandlungsakte unentgeltlich zur Verfügung zu stellen. Der Anspruch ist beschränkt, soweit erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Anders als das Recht auf Auskunft nach Art. 15 DSGVO können die Rechte aus § 630g Abs. 1 BGB nach dem Tod der Patientin oder des Patienten den Erben zur Wahrnehmung vermögensrechtlicher Interessen und den nächsten Angehörigen bei Geltendmachung immaterieller Interessen zustehen (§ 630g Abs. 3 BGB).

41. Da sowohl bei der datenschutzrechtlichen Auskunft als auch bei dem Einsichtsrecht nach § 630g BGB gegebenenfalls Dritte, z. B. Informationsgeber, Angehörige, Mitpatientinnen und Mitpatienten, vor einer Offenbarung zu schützen sind, kommt ein automatisches Kopieren und Aushändigen der Unterlagen nicht in Betracht. Es bedarf vielmehr der Überprüfung und gegebenenfalls einer teilweisen Unkenntlichmachung durch hierzu besonders beauftragte und geschulte Beschäftigte. Die Berechtigung zur Auskunftserteilung mit Zugriff auf die gesamte Patientenakte muss auf einen möglichst engen Personenkreis beschränkt werden. Eine Ablehnung oder Einschränkung ist zu begründen und nachvollziehbar zu dokumentieren.

Auslagerung des KIS über Cloud-Dienste

42. Die Verarbeitung von Gesundheitsdaten durch Krankenhäuser im Wege von Cloud-Computing-Diensten ist nur nach Maßgabe des § 393 SGB V zulässig. Die im Juli 2024 in Kraft getretene Regelung, die sich nach dem Wortlaut an Leistungserbringer im Sinne des Sozialrechts richtet, erstreckt sich als datenschutzrechtlicher Maßstab auf alle Krankenhäuser im Sinne dieser Orientierungshilfe. Je nach Konstellation und Ausgestaltung sind bei der Nutzung von Cloud-Diensten gesonderte Regelungen zum Beispiel bezüglich der datenschutzrechtlichen Verantwortlichkeiten oder erforderlicher Datentransfers zu treffen.

43. Nach § 393 Abs. 2 SGB V ist die Inanspruchnahme von Cloud-Diensten nur zulässig, wenn die Datenverarbeitung im Inland, in einem Mitgliedstaat der EU oder in einem diesem nach § 35 Absatz 7 SGB I gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 DSGVO vorliegt, in einem Drittstaat stattfindet und die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt.

44. Darüber hinaus müssen nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sein, ein aktuelles C5-Testat der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegen und die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt sein. Seit Juli 2025 muss es sich bei dem vorgelegten C5-Testat um ein Typ-2-Testat handeln. Alternativ dazu können auch andere Testate oder Zertifikate vorgelegt werden, die ein dem C5-Testat vergleichbares oder höheres

Sicherheitsniveau sicherstellen. Darüber hinaus sind bei Nutzung von Cloudressourcen die Anforderungen des C3A-Katalogs des BSI[1] sowie des B3S[2] zu beachten

45. Als angemessene technische und organisatorische Maßnahmen kommen insbesondere der Einsatz von Verschlüsselungstechnologien sowie das sog. Confidential Cloud-Computing in Betracht. Die in diesem Zusammenhang von der DSK 2025 veröffentlichte Entschließung ist zu beachten.[3]

46. Bei der Auswahl von Cloud-Dienste-Anbietern ist auf die Einhaltung der Anforderungen aus den Art. 44 ff. DSGVO zum internationalen Datenverkehr zu achten.

[1]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf?__blob=publicationFile&v=6
[2]https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/
[3]Entschließung Confidential Cloud Computing, verfügbar unter: https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Confidential_Cloud_Computing.pdf