Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen

Synopse der Fassungen 2011 und 2014

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

Neue Fassung		Alte Fassung		Hinweise
Schriftfarbe schwarz	➔keine Änderung erfolgt	Schriftfarbe schwarz	➔ keine Änderung erfolgt	
Schriftfarbe rot	➔neuer Text in neuer Fassung	Schriftfarbe blau	➔ alter Text, bei dem eine Änderung vorgenommen wurde	

Aufnahme

Aufnahme

Administrative Aufnahme

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

1. Die Aufnahmekraft darf bei Eingabe der Identifikationsdaten des neuen Patienten (Suchfunktion) vom System erfahren, ob der Patient schon einmal

1. Die Aufnahmekraft darf bei Eingabe der Identifikationsdaten des neuen Patienten (Suchfunktion) vom System erfahren, ob der Patient schon einmal

in demselben Krankenhaus behandelt wurde. Dies umfasst zunächst nur Identifikationsdaten (Name, Vorname, Patientennummer, etc.). Dabei kann zur klaren Identifizierung die Wild-Card-Funktion (abgekürzte Suche oder Ähnlichkeits-Suche) zugelassen werden (Ausschluss einer Doppelregistrierung derselben Person mit verschiedenen Schreibweisen) und in der Trefferliste neben Identifikationsdaten auch der Zeitraum des letzten stationären Aufenthalts angezeigt werden.	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). Durch nachträgliche Kontrollen muss sichergestellt werden, dass fingierte Aufnahmen von Patienten zum Zweck der Einsicht in Patientendaten aufgedeckt und sanktioniert werden.	Zu nachträglichen Kontrollen siehe Abschnitt Protokollierung
2. Die Offenbarung einer vorbehandelnden funktionsbezogenen Organisationseinheit ist bei der administrativen Aufnahme nur dann zulässig, wenn die Behandlung durch Ärzte dieser Organisationseinheit medizinisch noch nicht abgeschlossen ist. Eine Zugriffsmöglichkeit der administrativen Aufnahmekraft auf medizinische Daten mit Ausnahme der Einweisungsdiagnose ist mangels Erforderlichkeit nicht zulässig.	2. Die Offenbarung einer vorbehandelnden funktionsbezogenen Organisationseinheit ist bei der administrativen Aufnahme nur dann zulässig, wenn in dem Krankenhaus noch nicht abgeschlossene Behandlungsfälle zu dem Patienten geführt werden. Eine Zugriffsmöglichkeit der administrativen Aufnahmekraft auf medizinische Daten mit Ausnahme der Einweisungsdiagnose ist mangels Erforderlichkeit nicht zulässig.	
3. Die Aufnahmekraft darf auch – möglichst standardisierte – Warnhinweise im Datensatz des Patienten zur Kenntnis nehmen, die bereits vor der medizinischen Aufnahme administrative Maßnahmen erfordern. Dies gilt für frühere Betrugsversuche / Zahlungsunfähigkeit von	3. Die Aufnahmekraft darf auch – möglichst standardisierte – Warnhinweise im Datensatz des Patienten zur Kenntnis nehmen, die bereits vor der medizinischen Aufnahme administrative Maßnahmen erfordern. Dies gilt für frühere Betrugsversuche / Zahlungsunfähigkeit von Selbstzahlern und	

Selbstzahlern und für Hinweise auf die Trägerschaft multiresistenter Keime, die umgehend besondere Schutzmaßnahmen erfordern.	für Hinweise auf die Trägerschaft multiresistenter Keime, die umgehend besondere Schutzmaßnahmen erfordern.	
	4. Bei der Aufnahme kann der Patient der Hinzuziehung von Daten aus früheren abgeschlossenen Behandlungsfällen in demselben Krankenhaus ganz oder teilweise widersprechen. Hierauf und auf die mit einer derartigen Beschränkung verbundenen Risiken ist der Patient bereits bei der administrativen Aufnahme in allgemeiner Form (z.B. durch ein Merkblatt) hinzuweisen.	Siehe Nr. 8 und 26 der neuen Fassung
4. Das Krankenhaus muss die Möglichkeit vorsehen, Auskünfte über den Patientenaufenthalt durch die Pforte, andere Auskunftsstellen und das Stationspersonal zu sperren. (Ob diese als Regel einzurichten ist und eine Aufhebung der Einwilligung bedarf, oder ob eine Widerspruchslösung genügt, hängt von den landesgesetzlichen Regelungen ab. Für psychiatrische Patienten ist generell die erste Verfahrensweise zu wählen.) Die Einrichtung einer Auskunftssperre muss zur Folge haben, dass bei der Patientensuche durch Auskunftsstellen kein Treffer angezeigt wird. Bei anderen Stellen – insbesondere auf der jeweiligen Station – muss der Umstand der Auskunftssperre erkennbar werden.	6. Das Krankenhaus muss die Möglichkeit vorsehen, Auskünfte über den Patientenaufenthalt durch die Pforte, andere Auskunftsstellen und das Stationspersonal zu sperren. (Ob diese als Regel einzurichten ist und eine Aufhebung der Einwilligung bedarf, oder ob eine Widerspruchslösung genügt, hängt von den landesgesetzlichen Regelungen ab. Für psychiatrische Patienten ist generell die erste Verfahrensweise zu wählen.) Die Einrichtung einer Auskunftssperre muss zur Folge haben, dass bei der Patientensuche durch die Pforte oder eine andere Auskunftsstelle kein Treffer angezeigt wird.	

5. Die Anlage eines klinischen Basisdatensatzes ist auf Grundlage einer Einwilligung des Patienten möglich. Auf diesen darf bei neuer Vorstellung des Patienten zugegriffen werden.

Medizinische Aufnahme

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

6a. Die medizinische und die administrative Aufnahme können von der gleichen Person abgewickelt werden. Im Zuge der medizinischen Aufnahme ist im erforderlichen Umfang die Kenntnisnahme und Erhebung von medizinischen Daten zulässig.

7. Hat der Patient der Heranziehung von Vorbehandlungsdaten im Rahmen der administrativen Aufnahme widersprochen, ist ein Hinweis im System aufzunehmen, um dem behandelnden Arzt die Möglichkeit zu geben, den Patienten bei der medizinischen Aufnahme auf das potentiell bestehende Risiko einer Fehlbehandlung hinzuweisen und die Gelegenheit zur Rücknahme des Widerspruchs zu geben. Eventuell in begründeten Einzelfällen bestehende Möglichkeiten zur Einschränkung der Haftung des Krankenhauses oder zur Verweigerung der Behandlung ergeben sich aus dem allgemeinen und landesspezifischen Arzt- und Krankenhausrecht.

Siehe Nr. 8 und 26 der neuen Fassung

8. Ist der Patient bei der (Not-)Aufnahme nicht einsichts- oder artikulationsfähig, darf das Krankenhaus grundsätzlich von der mutmaßlichen Einwilligung in die Heranziehung von erforderlichen Vorbehandlungsdaten aus demselben Krankenhaus durch die Behandler ausgehen. Die Tatsache, dass dieser Fall eingetreten ist, muss sich aus dem KIS ergeben.

Siehe Nr. 8 und 26 der neuen Fassung

Behandlung

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

7. Der Zugriff auf die medizinischen und Pflege-Daten ist nach seiner Erforderlichkeit für die persönliche Aufgabenerfüllung der Beschäftigten auszudifferenzieren. Kriterien zur Differenzierung sind zumindest die Stellung der Beschäftigten im Krankenhaus und die ihnen zugewiesenen fachlichen Aufgaben. Der Behandlungsort kann als Indiz für die Übernahme einer Aufgabe dienen. Beispiel sind die einem Bereitschaftsarzt zugewiesenen Stationen, die Anwesenheit eines Chirurgen im OP-Saal, in dem sich der Patient befindet, oder die Anwesenheit einer Pflegekraft auf einer Station, in der er dies tut.

Behandlung

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

10. Der Zugriff auf die medizinischen und Pflege-Daten ist nach seiner Erforderlichkeit für die persönliche Aufgabenerfüllung der Mitarbeiter auszudifferenzieren. Kriterien zur Differenzierung sind zumindest die Stellung eines Mitarbeiters im Krankenhaus und die ihm zugewiesenen fachlichen Aufgaben. Der Behandlungsort kann als Indiz für die Übernahme einer Aufgabe dienen. Beispiel sind die einem Bereitschaftsarzt zugewiesenen Stationen, die Anwesenheit eines Chirurgen im OP-Saal, in dem sich der Patient befindet, oder die Anwesenheit einer Pflegekraft auf einer Station, in der er dies tut.

8. Der Zugriff auf Vorbehandlungsdaten ist nur soweit zulässig, wie das Landeskrankenhausrecht dies gestattet. Ein Widerspruch des Patienten gegen diesen Zugriff ist zu berücksichtigen.

Siehe Nr. 26 der neuen Fassung

Zugriffe durch Ärzte

Soweit im Folgenden auf Ärzte Bezug genommen wird, gelten die Regelungen auch für Psychotherapeuten.

9. Ein Patient ist zu jedem Zeitpunkt seiner Behandlung fachlich oder räumlich einem Arzt oder einer Gruppe von Ärzten zugeordnet. In der Regel darf diese Zuordnung alle Ärzte einer funktionsbezogenen (ggf. interdisziplinär besetzten) Organisationseinheit einschließen, die sich bei der Behandlung des Patienten gegenseitig vertreten. Soweit an der Behandlung eines Patienten Ärzte mehrerer Organisationseinheiten beteiligt sind, kann auch eine entsprechende mehrfache Zuordnung erfolgen. Nach der Zuordnung bestimmen sich die Schranken für den lesenden wie schreibenden Zugriff auf die Daten dieses Patienten.

10. Die Erweiterung des Kreises der Zugriffsberechtigten erfolgt auf der Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes

Zugriffe durch Ärzte

Soweit im Folgenden auf Ärzte Bezug genommen wird, gelten die Regelungen auch für Psychotherapeuten.

11. Ein Patient ist zu jedem Zeitpunkt seiner Behandlung fachlich oder räumlich einem Arzt oder einer Gruppe von Ärzten zugeordnet. In der Regel darf diese Zuordnung alle Ärzte einer funktionsbezogenen Organisationseinheit einschließen, die sich bei der Behandlung des Patienten gegenseitig vertreten. Soweit an der Behandlung eines Patienten Ärzte mehrerer Organisationseinheiten beteiligt sind, kann auch eine entsprechende mehrfache Zuordnung erfolgen. Nach der Zuordnung bestimmen sich die Schranken für den lesenden wie schreibenden Zugriff auf die Daten dieses Patienten.

12. Die Erweiterung des Kreises der Zugriffsberechtigten erfolgt auf der Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes (z.B.

(z.B. Zuweisung zu einer weiteren funktionsbezogenen Organisationseinheit, Einbeziehung eines weiteren Arztes bei interdisziplinärer Behandlung, Konsilaufträge) ab dem Zeitpunkt des konkreten Behandlungsauftrags.

11. Durch Wechsel der Zuordnung des Patienten von einer funktionsbezogenen OE zu einer anderen OE innerhalb des Krankenhauses (Verlegung) erhalten die Behandler der neuen OE erstmals Zugriff auf die Daten des Patienten. Die Ärzte der abgebenden OE können die Zugriffsmöglichkeit auf die Fallakte behalten. Sie dürfen diese Möglichkeit nutzen, soweit dies zur Aufgabenerfüllung (einschließlich der Sicherung der Qualität der eigenen Behandlung) noch erforderlich ist.

12. Für nur zeitweise erweiterte Zugriffserfordernisse (Bereitschaftsdienst nachts oder am Wochenende) sollten notwendige Berechtigungen an „Diensthabende" befristet und nur für ihren Zuständigkeitsbereich zugewiesen werden oder die Anwesenheit vor Ort voraussetzen. Mit dem schreibenden oder nur lesenden Zugriff auf Daten eines Patienten muss die dokumentierte Beteiligung des Arztes an der Behandlung dieses Patienten einhergehen. Ärzte sind darüber hinaus berechtigt, auch nach Ende des Patientenkontakts soweit zur Aufgabenerfüllung (einschließlich der Sicherung der

Zuweisung zu einer weiteren funktionsbezogenen Organisationseinheit, Einbeziehung eines weiteren Arztes bei interdisziplinärer Behandlung, Konsilaufträge) ab dem Zeitpunkt des konkreten Behandlungsauftrags.

13. Durch Wechsel der Zuordnung des Patienten von einer funktionsbezogenen OE zu einer anderen OE innerhalb des Krankenhauses (Verlegung) erhalten die Behandler der neuen OE erstmals Zugriff auf die bisherigen Daten des Patienten. Die Ärzte der abgebenden OE behalten den Zugriff auf die bisherige Behandlungsdokumentation. Auf die „neuen" Daten erhalten die Ärzte der abgebenden OE den Zugriff nur, soweit es zur Aufgabenerfüllung noch erforderlich ist.

14. Für nur zeitweise erweiterte Zugriffserfordernisse (Bereitschaftsdienst nachts oder am Wochenende) sollten notwendige Berechtigungen an „Diensthabende" befristet und nur für ihren Zuständigkeitsbereich zugewiesen werden oder die Anwesenheit vor Ort voraussetzen. Mit dem schreibenden oder nur lesenden Zugriff auf Daten eines Patienten muss die dokumentierte Beteiligung des Arztes an der Behandlung dieses Patienten einhergehen. Ärzte sind darüber hinaus berechtigt, auch nach Ende des Patientenkontakts auf die Dokumentation der eigenen Leistungen und der mit ih-

Qualität der eigenen Behandlung) erforderlich auf die Dokumentation der eigenen Leistungen und der mit ihnen zusammenhängenden medizinischen Daten zuzugreifen.

13. Konsilanforderungen dürfen den Datenzugriff nur in Bezug auf den betroffenen Patienten eröffnen. Die Anforderung kann einzelne Ärzte oder eine Gruppe von spezialisierten Konsiliarärzten berechtigen. Sie ist auf die Daten zu beschränken, die für die Festlegung der Konsiliarleistung erforderlich ist. Der durch die Konsilanforderung eröffnete Datenzugriff ist zu befristen. Konsilärzte sind darüber hinaus berechtigt, auch nach Ende des Patientenkontakts soweit zur Aufgabenerfüllung (einschließlich der Sicherung der Qualität der eigenen Behandlung) erforderlich auf die Dokumentation der eigenen Leistungen und der mit ihnen zusammenhängenden medizinischen Daten zuzugreifen.

nen zusammenhängenden medizinischen Daten zuzugreifen.

15. Konsilanforderungen (ergänzende Mitbehandlung) dürfen den Datenzugriff nur in Bezug auf den betroffenen Patienten eröffnen. Die Anforderung kann an einen einzelnen Arzt persönlich ergehen und damit nur diesen zum Zugriff berechtigen. In diesem Fall ist eine Weitergabe des Konsilauftrages zu ermöglichen. Die Anforderung kann aber auch an eine vorab definierte Gruppe von Konsiliarärzten (z.B. einen internen Konsiliardienst) gerichtet sein. Innerhalb der Konsiliardienstleistenden ist die Gruppe der im Einzelfall Zugriffsbefugten möglichst klein zu halten und nur auf sachliche Notwendigkeiten (Zweitmeinung, Vertretung) zu beschränken. Die Möglichkeit zur Stornierung der Konsilübernahme kann vorgesehen werden. Das Zugriffsrecht auf den Konsiliarbericht selbst bleibt davon unberührt. Der Umfang der zur Verfügung gestellten Daten und die Dauer der Zugriffsberechtigung ist an der Erforderlichkeit für die Konsiliarleistung auszurichten. Das Krankenhaus kann hierzu standardisierte Verfahren vorsehen. Möglichkeiten zur Befristung oder Sperrung des Zugriffs sind vorzusehen.

14. Ein darüber hinaus gehender Sonderzugriff auf Patientendaten außerhalb des differenzierten Berechtigungskonzepts ist in der Regel nicht erforderlich. Sollte er aus besonderen vorübergehenden Gründen doch unabweisbar sein, ist die zugreifende Person durch einen automatisch erscheinenden Hinweis darüber aufzuklären, dass sie außerhalb ihrer Berechtigung zugreift, einen Zugriffsgrund angeben muss und der Zugriff protokolliert und anschließend kontrolliert wird. Die Kontrolle ist hinsichtlich der Methode und der kontrollierenden und auswertenden Personen vorher unter Beteiligung der Beschäftigtenvertretung und der/des betrieblichen bzw. behördlichen Datenschutzbeauftragten festzulegen. Mindestens stichprobenartige Kontrollen durch das Krankenhaus sind erforderlich.

15. Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten. Für die konkret an der Behandlung beteiligten Beschäftigten eines Beleg-Krankenhauses gelten die Tz. 6 ff.

Zugriffe durch den pflegerischen Stationsdienst

16. Der Zugriff des Pflegepersonals auf die erforderlichen pflegerischen und medizinischen Daten ist

16. Ein darüber hinaus gehender Notzugriff auf Patientendaten außerhalb des differenzierten Berechtigungskonzepts ist in der Regel nicht erforderlich. Sollte er aus besonderen vorübergehenden Gründen doch unabweisbar sein, ist die zugreifende Person durch einen automatisch erscheinenden Hinweis darüber aufzuklären, dass sie außerhalb ihrer Berechtigung zugreift, einen Zugriffsgrund angeben muss und der Zugriff protokolliert und anschließend kontrolliert wird. Die Kontrolle ist hinsichtlich der Methode und der kontrollierenden und auswertenden Personen vorher unter Beteiligung der Beschäftigtenvertretung und der/des betrieblichen bzw. behördlichen Datenschutzbeauftragten festzulegen. Mindestens stichprobenartige Kontrollen durch das Krankenhaus sind erforderlich.

17. Belegärzte erhalten nur Zugriff auf die Daten ihrer Patienten. Für die konkret an der Behandlung beteiligten Mitarbeiter eines Beleg-Krankenhauses gelten die Ziff.10 ff.

Zugriffe durch Pflegepersonal

18. Der Zugriff des Pflegepersonals auf die erforderlichen pflegerischen und medizinischen Daten ist

auf die in der eigenen funktionsbezogenen Organisationseinheit (z.B. Station) behandelten Patienten zu begrenzen.

17. Die Berechtigung ergibt sich bei wechselnder Zuordnung zu Organisationseinheiten (Springer) aus der dokumentierten Zuweisung zu einer OE durch die zuständige Stelle, ggf. in Verbindung mit der Anwesenheit der Pflegekraft vor Ort.

18. Durch die Anordnung der Verlegung des Patienten in eine andere OE erhalten die Pflegekräfte der „neuen" OE erstmals Zugriff auf die bisherigen Daten des Patienten. Die Pflegekräfte der abgebenden OE behalten ihre Zugriffsberechtigung nur für einen festzulegenden, eng begrenzten Zeitraum zum Abschluss der Dokumentation.

Zugriffe außerhalb der bettenführenden Fachabteilungen

19. Beschäftigte des Krankenhauses mit fachrichtungsübergreifender Funktion (z.B. Anästhesie, Physiotherapie, OP-Personal, Diagnostik [z.B. MRT], Pathologie) sollten den Daten-Zugriff entweder durch individuelle Zuweisung oder mit dem/durch den

auf die in der eigenen funktionsbezogenen Organisationseinheit (z.B. Station) behandelten Patienten zu begrenzen.

19. Die Berechtigung ergibt sich bei wechselnder Zuordnung zu Organisationseinheiten (Springer) aus der dokumentierten Zuweisung zu einer OE durch die Pflegeleitung, ggf in Verbindung mit der Anwesenheit der Pflegekraft vor Ort.

20. Durch die Anordnung der Verlegung des Patienten in eine andere OE erhalten die Pflegekräfte der „neuen" OE erstmals Zugriff auf die bisherigen Daten des Patienten. Die Pflegekräfte der abgebenden OE behalten ihre Zugriffsberechtigung nur für einen festzulegenden, eng begrenzten Zeitraum zum Abschluss der Dokumentation. Sie erhalten keinen Zugriff auf die „neuen" Daten.

Fachübergreifende Zugriffe

21. Krankenhausmitarbeiter/ innen mit fachrichtungsübergreifender Funktion (z.B. Anästhesie, Physiotherapie, OP-Personal, Diagnostik [z.B. MRT], Pathologie) sollten den Daten-Zugriff entweder durch individuelle Zuweisung oder mit dem/durch den

Patientenkontakt erhalten. Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren. Die Differenzierung kann typisiert z.B. nach beauftragter Funktionsstelle, angeforderter Leistung oder Krankheitsbild des Patienten erfolgen. Bei bestimmten Beschäftigten kann ein Zugriff auf sämtliche Daten der jeweiligen Patienten zulässig sein.

20. Der Schreibdienst sollte so organisiert sein, dass der Zugriff durch individuelle Zuweisung zeitlich beschränkt erfolgt. Sofern dies nicht möglich ist, muss zumindest sichergesellt sein, dass die einzelnen Schreibkräfte jeweils nur einer bestimmten Funktionseinheit mit entsprechenden Zugriffsrechten zugeordnet sind.

21. Das (Zentral-)Labor bzw. deren diensthabende / handelnde Beschäftigte dürfen mit der Leistungsanforderung nur einen Zugriff auf die für die Befundung erforderlichen Daten des im Auftrag benannten betroffenen Patienten erhalten.

Patientenkontakt erhalten. Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren. Die Differenzierung kann typisiert z.B. nach beauftragter Funktionsstelle, angeforderter Leistung oder Krankheitsbild des Patienten erfolgen. Bei bestimmten Mitarbeitern kann ein Zugriff auf sämtliche Daten zulässig sein.

22. Das (Zentral-)Labor bzw. deren diensthabende / handelnde Mitarbeiter/innen darf mit der Leistungsanforderung nur einen Zugriff auf die für die Befundung erforderlichen Daten des im Auftrag benannten betroffenen Patienten erhalten. Bei einem hauseigenen Zentrallabor, das nicht versichertenbezogen selbst abrechnen muss, ist eine Bearbeitung wünschenswert, bei der die Identitätsdaten der Patienten im Regelfall durch medizinisch-technische Assistenten und andere nichtärztliche Mitarbeiter nicht zur Kenntnis genommen werden können.

Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls

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

Nach der Behandlung

23. Nach Abschluss des Behandlungsfalles – d.h. nach Abwicklung der medizinischen und verwaltungsmäßigen Routinevorgänge – (oder nach Verlegung in ein anderes Krankenhaus) ist die elektronische Patientenakte im Sinne der jeweils geltenden rechtlichen Regelungen zu sperren. Dies kann auch im Zuge einer Überführung in ein Patientendokumentationsarchiv geschehen. Notwendig ist es, für die Sperrung eine feste Frist nach Entlassung des Patienten festzulegen. Diese Frist ist abhängig von den jeweiligen organisatorischen Abläufen im Krankenhaus (Fallabschluss durch medizinisches Controlling / Abrechnung / Qualitätssicherung). Von der Sperrung ausgenommen sind lediglich die zum Auffinden der gesperrten Patientendaten erforderlichen Identifikationsdaten.

Siehe auch Nr. 24 und 25 der neuen Fassung

24. Auf gesperrte Daten darf nur ein eingeschränkter Personenkreis Zugriff erhalten, um festgelegte Aufgaben erfüllen zu können (Zugriff durch ehemals behandelnde Ärzte; Auskünfte an MDK, externe Ärzte oder Patienten; Qualitätssicherung u.a.). Die zum Zugriff berechtigen Personen können unter Beachtung der bestehenden gesetzlichen Vorgaben die Berechtigung im Einzelfall delegieren. Der Zugriff ist auf diejenigen Daten zu

Siehe auch Nr. 24 und 25 der neuen Fassung

beschränken, die zur jeweiligen Aufgabenerfüllung regelmäßig erforderlich sind. Die Zugriffsberechtigungen für diese Zwecke sollten nach der Erfahrung (Zeitspanne für Rückfragen) zeitlich begrenzt werden. Die Patientensuche in gesperrten Daten ist nur nach wenigen vorgegebenen Kennzeichen (z. B. Name, Entlassungsdatum) zu ermöglichen.

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

24. Diese Zugriffsbeschränkung hat als technisch-organisatorische Maßnahme unabhängig davon zu erfolgen, ob und wann nach datenschutzrechtlichen Vorschriften eine Sperrung der Daten vorzunehmen ist.

25. Das Krankenhaus hat eine angemessene Frist (nicht länger als ein Jahr) nach Abschluss des Behandlungsfalls entsprechend den jeweiligen organisatorischen Abläufen im Krankenhaus festzulegen, in-

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

nerhalb derer die Einschränkung der Zugriffsmöglichkeiten spätestens zu erfolgen hat.

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

Siehe auch Nr. 8 der neuen Fassung

Löschung

27. Patientendaten sind in Krankenhausinformationssystemen zu löschen, wenn sie zur Durchführung des Behandlungsvertrags nicht mehr erforderlich sind, vorgeschriebene Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

26. Patientendaten sind in Krankenhausinformationssystemen zu löschen, wenn sie zur Durchführung des Behandlungsvertrags nicht mehr erforderlich sind, vorgeschriebene Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Zugriffe für Abrechnung, Controlling, Qualitätssicherung und Ausbildung

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

Zugriffe durch Funktionskräfte

27. Die Krankenhausverwaltung / Abrechnungsabteilung darf nur Zugriff auf die für sie erforderlichen Patientendaten (Stammdaten, Diagnosen, Leistungen usw.) haben, nicht aber auf nicht erforderliche, weitergehende medizinische Befunde / Doku-

	mente bildgebender Verfahren.	
29. Soweit zur internen Qualitätssicherung oder beim Controlling der Zugriff durch die an der Qualitätssicherung oder dem Controlling beteiligten Beschäftigten auf alle Daten eines Patienten zugelassen werden muss, ist durch Zuständigkeits- und Funktionsaufteilungen, zeitliche Beschränkungen oder sonstige geeignete technisch-organisatorische Maßnahmen ein ständiger Vollzugriff auf alle Daten aller Krankenhauspatienten zu vermeiden.	28. Soweit zur internen Qualitätssicherung oder beim Controlling der Zugriff durch die an der Qualitätssicherung oder dem Controlling beteiligten Mitarbeiter auf alle Daten eines Patienten zugelassen werden muss, ist durch Zuständigkeits- und Funktionsaufteilungen und zeitliche Beschränkungen ein ständiger Vollzugriff auf alle Daten aller Krankenhauspatienten zu vermeiden. Soweit möglich ist eine Verwendung vorzusehen, bei der die Identitätsdaten des Patienten nicht zur Kenntnis genommen werden können.	Siehe auch Nr. 30 der neuen Fassung
	Sonstige Zugriffe	
30. Soweit nicht erforderlich (z. B. für das Geschäftsprozessmanagement, das strategische Controlling und die betriebswirtschaftliche Steuerung des Krankenhauses) ist eine Verwendung vorzusehen, bei der die Identitätsdaten des Patienten nicht zur Kenntnis genommen werden können.		
31. Soweit Patientendaten zur Aus- oder Fortbildung außerhalb eines Behandlungskontexts benötigt werden, sind diese in geeigneter Weise zu anonymisieren, soweit nicht landesspezifische Bestimmungen abweichende Regelungen enthalten.	29. Soweit Patientendaten zur Aus- oder Fortbildung außerhalb eines Behandlungskontexts benötigt werden, sind diese in geeigneter Weise zu anonymisieren, soweit nicht landesspezifische Bestimmungen abweichende Regelungen enthalten.	

Verarbeitung durch verschiedene Leistungserbringer

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

30. Patienten, die in anderen Krankenhäusern oder Unternehmen des Konzerns, dem das Krankenhaus angehört, (z.B. in GmbHs wie Medizinische Versorgungszentren) behandelt werden, werden dadurch nicht zugleich Patienten des Krankenhauses. Sie dürfen daher nur in den Patientenbestand des jeweiligen Krankenhauses bzw. Unternehmens aufgenommen werden. Ein gemeinsames (Krankenhaus und andere Stelle bzw. anderes Krankenhaus umfassendes) KIS ist wenn überhaupt, dann nur bei Trennung der Datenbestände in verschiedene Mandanten möglich. Einrichtungs- und insbesondere mandantenübergreifende Zugriffe stellen datenschutzrechtlich Übermittlungen dar, deren Zulässigkeit sich nach Arzt- und Datenschutzrecht richtet.

Siehe auch Nr. 33 der neuen Fassung

33. Einrichtungs- und insbesondere mandantenübergreifende Zugriffe stellen datenschutzrechtlich Übermittlungen dar, deren Zulässigkeit sich nach Arzt- und Datenschutzrecht richtet. Beispiele für die zulässige Ausgestaltung derartiger Übermittlungen sind in einem Szenarienkatalog ausgeführt, der ergänzend zu der vorliegenden Orientierungshilfe von der federführenden Unterarbeitsgruppe bereitgestellt wird.

Siehe auch Nr. 30 der alten Fassung

34. Eine Person kann mehreren Mandanten als Mitarbeiter zugeordnet werden. Greift eine solche Person im Zuge ihrer Tätigkeit für einen Mandanten auf Daten zu, die diesem Mandanten bereits zugeordnet sind, dann liegt keine Übermittlung vor, so dass die Mandantenzuordnung der Daten unverändert zu bleiben hat, gleich von wo der Zugriff erfolgte.

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

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

37. Ambulant in Nebentätigkeit behandelte Privatpatienten sind grundsätzlich nicht Patienten des Krankenhauses, sondern der insoweit berechtigten Ärzte. Für Behandlungsakten von ambulant in Nebentätigkeit behandelten Privatpatienten hat der Arzt die alleinige datenschutzrechtliche Verantwortung.

30a. Eine Person kann mehreren Mandanten als Mitarbeiter zugeordnet werden. Greift eine solche Person im Zuge ihrer Tätigkeit für einen Mandanten auf Daten zu, die diesem Mandanten bereits zugeordnet sind, dann liegt keine Übermittlung vor, so dass die Mandantenzuordnung der Daten unverändert zu bleiben hat, gleich von wo der Zugriff erfolgte. Neben mandantenbezogenen Datenbeständen kann ein KIS einzelne nicht personenbezogene Datenbestände vorhalten, auf die von allen Mandanten aus zugegriffen werden kann.

30b. 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.

36. Ambulant in Nebentätigkeit behandelte Privatpatienten sind grundsätzlich nicht Patienten des Krankenhauses, sondern der insoweit berechtigten Ärzte. Ihre Behandlungsdaten dürfen anderen Mitarbeiter/innen des Krankenhauses nicht standardmäßig, sondern nur insoweit und nur so lange zugänglich sein, als sie in die Behandlung einbezogen

werden (z.B. Labor). Soweit die Daten dieser Patienten im KIS verarbeitet werden sollen, sind sie getrennt von den übrigen Daten zu halten. Die Zugriffsberechtigungen für diesen Datenbestand sind getrennt von den anderen Zugriffsberechtigungen im KIS zu verwalten.

Technische Administration

38. Durch technische und administrative Rollenteilung (z. B. Systemadministration und Administration der einzelnen Anwendungen) ist ein missbräuchlicher Datenzugriff zu erschweren. Die Zugriffsrechte und Eingriffsebenen der Administratoren sind entsprechend ihren spezifischen Aufgaben zu begrenzen.

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

40. Bei einer (Fern-)Wartung durch Dritte/Externe sind

Technische Administration

31. Durch technische und administrative Rollenteilung (z. B. Systemadministration und Administration der einzelnen Anwendungen) ist ein missbräuchlicher Datenzugriff zu erschweren. Die Zugriffsrechte und Eingriffsebenen der Administratoren sind entsprechend ihren spezifischen Aufgaben zu begrenzen.

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

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

41. Beschäftigte des Krankenhauses als Patienten müssen davor geschützt werden, dass Kolleginnen und Kollegen von ihrem Aufenthalt erfahren (können), die nicht unmittelbar an der Behandlung beteiligt sind. Soweit dies nicht bereits durch die oben beschriebenen Maßnahmen erreicht wird, kommt (zusätzlich) u.U. eine Aufnahme unter fiktivem Namen in Betracht. Die Zuordnung von fiktivem zu tatsächlichem Namen ist geschützt und nur einem eng begrenzten Personenkreis zugänglich aufzubewahren.

42. Für Patienten, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, gilt grundsätzlich dasselbe. Die Festlegung trifft die Klinikleitung auf Antrag des Patienten.

besondere Maßnahmen erforderlich, damit die Wartung nur mit Wissen und Wollen des Krankenhauses im zugelassenen Umfang stattfinden kann.

Besonders schutzwürdige Patientengruppen

34. Krankenhaus-Mitarbeiter/innen als Patienten müssen davor geschützt werden, dass Kolleginnen und Kollegen von ihrem Aufenthalt erfahren (können), die nicht unmittelbar an der Behandlung beteiligt sind. Soweit dies nicht bereits durch die oben beschriebenen Maßnahmen erreicht wird, kommt (zusätzlich) u.U. eine Aufnahme unter fiktivem Namen in Betracht. Die Zuordnung von fiktivem zu tatsächlichem Namen ist geschützt und nur einem eng begrenzten Personenkreis zugänglich aufzubewahren.

35. Für Patienten, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, gilt grundsätzlich dasselbe. Die Festlegung trifft die Klinikleitung.

36. Ambulant in Nebentätigkeit behandelte Privatpatienten sind grundsätzlich nicht Patienten des Krankenhauses, sondern der insoweit berechtigten

Siehe Nr. 33 der neuen Fassung

Ärzte. Ihre Behandlungsdaten dürfen anderen Mitarbeiter/innen des Krankenhauses nicht standardmäßig, sondern nur insoweit und nur so lange zugänglich sein, als sie in die Behandlung einbezogen werden (z.B. Labor). Soweit die Daten dieser Patienten im KIS verarbeitet werden sollen, sind sie getrennt von den übrigen Daten zu halten. Die Zugriffsberechtigungen für diesen Datenbestand sind getrennt von den anderen Zugriffsberechtigungen im KIS zu verwalten.

Zugriffsprotokollierung und Datenschutzkontrolle

43. Aufgrund von Art und Umfang der in einem Krankenhausinformationssystem verarbeiteten medizinischen und administrativen Daten bedarf es für eine datenschutzgerechte Gestaltung einer angemessenen Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Grundlage hierfür ist eine aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe sowie geeignete Auswertungsmöglichkeiten.

44. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat. Dies betrifft sowohl Zugriffe aus der fachlichen Verfahrensnutzung (einschließlich des Zugriffs auf

Zugriffsprotokollierung und Datenschutzkontrolle

37. Aufgrund von Art und Umfang der in einem Klinikinformationssystem verarbeiteten medizinischen und administrativen Daten bedarf es für eine datenschutzgerechte Gestaltung einer angemessenen Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Grundlage hierfür ist eine aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe sowie geeignete Auswertungsmöglichkeiten.

Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet oder genutzt hat. Dies betrifft sowohl Zugriffe aus der fachlichen Verfahrensnutzung (einschließlich des Zugriffs auf

sog. Patientenübersichten mit Angaben zu der behandelnden Abteilung, Diagnosen etc.) als auch aus der administrativen Betreuung. Dabei gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.	sog. Patientenübersichten mit Angaben zu der behandelnden Abteilung, Diagnosen etc.) als auch aus der administrativen Betreuung. Dabei gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken.
45. Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle ist ebenso Aufgabe des Krankenhauses wie eine Kontrolle aus konkretem Anlass (s.Tz. 40). Aufnahmevorgänge, die nicht mit einer abrechnungsfähigen Behandlung in Verbindung stehen, müssen kontrolliert werden.	38. Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle ist ebenso Aufgabe des Krankenhauses wie eine Kontrolle aus konkretem Anlass (s.Ziff.39).

Auskunftsrechte des Patienten

46. Der Patient muss die Möglichkeit erhalten, Auskunft über und Einsicht in alle zu seiner Person gespeicherten Daten zu bekommen, soweit keine erheblichen therapeutischen Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Hierzu gehören auch die nach einer Behandlung archivierten Daten sowie die Empfänger von übermittelten Daten. Auch psychiatrische und psychotherapeutische Patienten haben grundsätzlich einen gesetzlichen Auskunftsanspruch. Die Auskunft und Einsicht kann je nach Wunsch des Patienten auch durch einen Ausdruck oder in elektronischer Form erfolgen.

47. Bei einem besonderen berechtigten Interesse, z.B. bei einem Datenmissbrauchsverdacht, umfasst das Auskunftsrecht auch die Information, wer zu welchem Zeitpunkt welche Daten zur Kenntnis genommen hat. Werden die lesenden Zugriffe zulässigerweise (vgl- Teil II, Tz. 7.5) nicht vollständig protokolliert, genügt es, den Kreis der Personen zu benennen, welche die Daten auf Grund ihrer Zugriffsrechte hätten zur Kenntnis nehmen können (z.B. Pflegepersonal der Station X, Ärzte der Fachabteillung A).

Auskunftsrechte des Patienten

39. Der Patient muss die Möglichkeit erhalten, Auskunft über und Einsicht in alle zu seiner Person gespeicherten Daten zu bekommen. Hierzu gehören auch die nach einer Behandlung archivierten Daten sowie die Empfänger von übermittelten Daten. Auch psychiatrische und psychotherapeutische Patienten haben grundsätzlich einen gesetzlichen Auskunftsanspruch. Die Auskunft und Einsicht kann auch durch einen Ausdruck oder die Übergabe eines Datenträgers (CD, USB-Stick) erfolgen.

Siehe Formulierungen in § 630 g BGB (Patientenrechtegesetz)

40. Das Auskunftsrecht umfasst auch die Information darüber, wer zu welchem Zeitpunkt welche Daten zur Kenntnis genommen hat. Werden unter Voraussetzung der Einhaltung der in Ziff. 1 bis 33 niedergelegten Grundsätze die lesenden Zugriffe nicht vollständig protokolliert, genügt es, den Kreis der Personen zu benennen, welche die Daten auf Grund ihrer Zugriffsrechte hätten zur Kenntnis nehmen können (z.B. Pflegepersonal der Station XY, Ärzte der Fachabteilung XY).

48. Da bei der Auskunft gegebenenfalls Dritte (z.B. Informationsgeber; Angehörige) vor einer Offenbarung zu schützen sind, kommt ein automatisches Kopieren und Aushändigen nicht in Betracht. Es bedarf vielmehr der Überprüfung und ggf. einer teilweisen Unkenntlichmachung durch hierzu besonders beauftragte und geschulte Beschäftigte. Die Berechtigung zur Auskunftserteilung mit Zugriff auf die gesamte Patientenakte muss auf einen möglichst engen Personenkreis beschränkt werden.

41. Da bei der Auskunft gegebenenfalls Dritte (z.B. Informationsgeber; Angehörige) vor einer Offenbarung zu schützen sind, kommt ein automatisches Kopieren und Aushändigen nicht in Betracht. Es bedarf vielmehr der Überprüfung und ggf. einer teilweisen Unkenntlichmachung durch hierzu besonders beauftragte und geschulte Mitarbeiter. Die Berechtigung zur Auskunftserteilung mit Zugriff auf die gesamte Patientenakte muss auf einen möglichst engen Personenkreis beschränkt werden.