GMDS - Deutsche Gesellschaft für Medizinische Informatik,
Biometrie und Epidemiologie e.V.
Industriestraße 154
D-50996 Köln

Tel.: +49 (2236) 3319958
Fax: +49 (2236) 3319959
Email: info@gmds.de
http://www.gmds.de

Vereinsregister: VR 16225 Amtsgericht Köln

Umsatzsteuer-Identifikationsnummer:
27.07.02 DE 182645846

Stellungnahme und Kommentierung der

„Orientierungshilfe Krankenhausinformationssysteme“[1]

Erstellt von der Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“ (DGI)

der

Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)

[1] herausgegeben im März 2014 von den Arbeitskreisen „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Das Originaldokument der OH KIS steht zum Download bei den Datenschutzaufsichtsbehörden des Bundes, der Länder und der Kirchen zur Verfügung, z. B. unter der URL http://www.datenschutz-berlin.de/attachments/771/Orientierungshilfe_Krankenhausinformationssysteme.pdf

Der Text der OH kann unter den gleichen Bedingungen (textlich unveränderte Übernahme, Angabe zu Urheberschaft und Fundstelle des Originaldokuments) verwendet werden.

Inhaltsverzeichnis

Haftungsausschluss / Copyright 1

1 Vorwort 2

2 Zusammenfassung 3

3 Allgemeines 5
3.1 Abgrenzung Datenschutz vs. IT-Sicherheit 6
3.2 Datenschutz bei den im Krankenhaus Beschäftigten 7

4 Formales 8
4.1 Übersicht zur Orientierungshilfe 8
4.2 Die Orientierungshilfe als Prüfkatalog für die Aufsichtsbehörden 8
4.2.1 Anwendungszeitraum 9
4.3 Zielrichtung der AG für die Überarbeitung 9
4.4 Formale Änderungen der Überarbeitung 10
4.4.1 Änderungen im ersten Teil der OH KIS 11
4.4.2 Änderungen im zweiten Teil der OH KIS 11

5 Kommentierung der in der OH KIS aufgeführten Anforderungspunkte 13
5.1 Teil 1: „Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen“ 13
5.1.1 Aufnahme 13
5.1.2 Behandlung 15
5.1.2.1 Zugriffe durch Ärzte 16
5.1.2.2 Zugriffe durch den pflegerischen Stationsdienst 19
5.1.2.3 Zugriffe außerhalb der bettenführenden Fachabteilungen 20
5.1.3 Einschränkung der Zugriffsrechte nach Abschluss des Behandlungsfalls 21
5.1.3.1 Löschung 23
5.1.3.2 Zugriffe für Abrechnung' Controlling' Qualitätssicherung und Ausbildung 23
5.1.3.3 Verarbeitung durch verschiedene Leistungserbringer 26
5.1.4 Technische Administration 28
5.1.5 Besonders schutzwürdige Patientengruppen 29
5.1.6 Zugriffsprotokollierung und Datenschutzkontrolle 30
5.1.7 Auskunftsrechte des Patienten 31
5.2 Teil 2: „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ 33
5.2.1 Rechtliche Einschätzung 33
5.2.2 Kommentar zu den Abschnitten der technischen Anforderungen 35
5.2.2.1 Datenmodell 35
5.2.2.2 Systemfunktionen 39
5.2.2.3 Anwendungsfunktionen 43
5.2.2.4 Rollen- und Berechtigungskonzept 45
5.2.2.5 Datenpräsentation 49
5.2.2.6 Systemzugang 50
5.2.2.7 Protokollierung 51
5.2.2.8 Technischer Betrieb, Administration 57
5.3 Glossar 59
5.3.1 In der OH KIS unerklärte Begrifflichkeiten 59
5.3.2 Begriffe aus Gesetzestexten 61
5.4 Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern 67
5.4.1 Szenario 1: Zulässige Auftragsdatenverarbeitung 67
5.4.2 Szenario 2: Übermittlung zur Erfüllung eines Konsilauftrages 68
5.4.3 Szenario 3: Übermittlung zur Nachbehandlung 69
5.4.4 Szenario 4: Abruf für einen neuen Behandlungsvorgang 69

6 Diskussion 72

7 Abkürzungen 75

Haftungsausschluss / Copyright

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Die Autoren sind keine Juristen. Insofern können und dürfen sie keine rechtsverbindlichen Auskünfte geben. Daher ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen. Eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen für das jeweilige Krankenhaus und die jeweilige Situation anhand der für dieses Krankenhaus geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Grafiken, Tondokumente, Videosequenzen und Texte zu beachten, von ihnen selbst erstellte Grafiken, Tondokumente, Videosequenzen und Texte zu nutzen oder auf lizenzfreie Grafiken, Tondokumente, Videosequenzen und Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt:

Dieses Werk ist unter einer Creative Commons-Lizenz (3.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:

- das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen
- Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anfertigen

Zu den folgenden Bedingungen:

- **Namensnennung**. Sie müssen den Namen des Autors/Rechteinhabers nennen, wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt
- **Keine kommerzielle Nutzung**. Dieses Werk bzw. dieser Inhalt darf nicht für kommerzielle Zwecke verwendet werden.
- **Weitergabe unter gleichen Bedingungen**. Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die daraufhin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

Im Weiteren gilt:

- Im Falle einer Verbreitung müssen Sie anderen die Lizenzbedingungen, unter welche dieses Werk fällt, mitteilen.
- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

http://creativecommons.org/licenses/by-nc-sa/3.0/de/

Köln, 28. März 2014

1 Vorwort

Der in Deutschland gelebte Föderalismus belebt Demokratie und Pluralismus, ermöglicht damit einerseits Anforderungen/Probleme auf Länderebene zu lösen, andererseits wird eine Machtanhäufung durch übergeordnete Instanzen verhindert: Der Föderalismus unterstützt somit eine politische Willensbildung auf mehreren Ebenen.

Die Kehrseite der Medaille besteht darin, dass neben dem Bund auch jedes Bundesland das Recht zur Verabschiedung von Datenschutzgesetzen oder Verordnungen hat. Eine Besonderheit in Deutschland ist, dass der evangelischen und römisch-katholischen Kirche in Deutschland die Verabschiedung eigener Gesetze erlaubt wird, welche für die Institutionen vorrangig vor Bundes- oder Landesgesetzen gelten. In Deutschland gibt es 27 Diözesen der römisch-katholischen Kirche, die alle ein eigenes Datenschutzrecht verabschieden dürfen. Die evangelische Kirche besteht aus einer Gemeinschaft von 20 lutherischen, unierten und reformierten Kirchen in Deutschland, die ebenfalls alle das Recht auf einer eigenen Gesetzgebung besitzen. Erfreulicherweise ähneln sich die Gesetze der Diözesen sehr, sodass die katholische datenschutzrechtliche Gesetzgebung als relativ einheitlich anzusehen ist, Gleiches gilt für die evangelische Kirche.

Die Datenschutzgesetze sind jeweils als Auffanggesetz konzipiert, d. h. dass Regelungen aus dem jeweiligen Datenschutzgesetz nur greifen, wenn keine speziellen Vorschriften existieren. Die Datenschutzgesetze der Länder spezifizieren die Vorgaben des Bundesrechts und gelten so vorrangig. Die Amtskirchen regeln jeweils für ihren Bereich in eigenen Datenschutzanordnungen und spezifizieren so die datenschutzrechtlichen Vorgaben des Bundes und der Länder, sodass diese Anforderungen vorrangig gelten. Dies heißt nicht, dass die anderen Datenschutzgesetze nicht mehr gelten, lediglich die Anforderungen, welche in einem spezialisierten Gesetz differenzierter vorgegeben werden, „überschreiben“ die Anforderungen, alle nicht spezialisierten Forderungen aus dem Gesetz bleiben bestehen.

All dies führt dazu, dass die datenschutzrechtlichen Regelungen in Deutschland alles andere als eindeutig sind. Entsprechend kann auch die von den Arbeitskreisen „Gesundheit und Soziales“ und „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche erstellte „Orientierungshilfe Krankenhausinformationssysteme“ (oft in Kurzform als „OH KIS“ benannt) die bundesweit geltenden Anforderungen nicht alle berücksichtigen, ebenso wenig sind alle Anforderungen, welche die Orientierungshilfe beinhaltet, bundesweit einheitlich durch Gesetze und/oder Verordnungen gefordert.

Der Versuch, bundesweit einheitliche Vorgaben zu einem aus Sicht der Datenschutz-Aufsichtsbehörden des Bundes, der Länder und der Kirchen datenschutzkonformen Einsatz von Krankenhausinformationssystemen zu formulieren, ist ein großer Schritt in die richtige Richtung, sowohl von Herstellern von Informationssystemen wie auch von Betreibern der Systeme. Hersteller von Systemen besitzen jetzt eine Vorgabe, anhand derer sie die Entwicklung ihrer Systeme planen können, und Betreiber müssen bei ihnen Beschäftigten nicht mehr erklären, warum in dem einen Bundesland etwas erlaubt ist, in einem anderen Bundesland aber verboten.

Im Einzelnen besteht sicherlich immer noch Diskussionsbedarf, da Datenschutzfragen häufig auch Abwägungsfragen darstellen, die letztlich aus unterschiedlicher Sicht verschieden beantwortet werden, ohne dass die differierenden Antworten dabei auch notwendigerweise falsch sein müssen.

2 Zusammenfassung

Die GMDS begrüßt den Versuch der Datenschutzaufsichtsbehörden, die Interpretation der datenschutzrechtlichen Anforderungen aus föderaler Sicht auf eine bundeseinheitliche Ebene darzustellen. Die Orientierungshilfe Krankenhausinformationssysteme besteht aus zwei Teilen: Teil 1 wurde „Rechtliche Rahmenbedingungen“ genannt, Teil 2 „Technische Anforderungen“.Teil 1 soll dabei die geltenden datenschutzrechtlichen Rahmenbedingungen aufzeigen, zugleich Vorgaben zur ärztlichen Schweigepflicht darstellen. In Teil 2 der Orientierungshilfe Krankenhausinformationssysteme werden Maßnahmen beschrieben, die der (technischen) Umsetzung der geschilderten datenschutzrechtlichen Anforderungen dienen.

Die Orientierungshilfe Krankenhausinformationssysteme kann keinen Anforderungskatalog für eine datenschutzkonforme Kontrolle durch die Aufsichtsbehörden darstellen, auch wenn dies in der Orientierungshilfe Krankenhausinformationssysteme so beschrieben wurde. Die Datenschutz-Aufsichtsbehörden versuchten die Vorgaben aller Bundesländer in die Orientierungshilfe einzubeziehen und damit stehen in der Orientierungshilfe zwangsläufig einige Anforderungen, die nur auf ein oder mehrere Bundesländer zutreffen, nicht jedoch auf alle Bundesländer. Damit existieren zwangsläufig Anforderungen in der Orientierungshilfe Krankenhausinformationssysteme, welche einer rechtlichen Grundlage für das betreffende Bundesland fehlt. Da eine datenschutzrechtliche Prüfung letztlich aber immer eine Prüfung gegen die zugrunde liegende gesetzliche Norm darstellt, ist die Orientierungshilfe hier als das zu verstehen, was der Name aussagt: als eine Orientierungshilfe.

Die bei der Überarbeitung der Orientierungshilfe Krankenhausinformationssysteme erfolgte Reduktion der von den Datenschutzaufsichtsbehörden im März 2011 aufgestellten Forderungen zeigt, dass damals, als Kommentierungen von Fachgremien bei der ersten Version nicht berücksichtigt wurden, viel entweder falsch formuliert wurde oder aus nicht vorhandenem Wissen um den Workflow bei der Patientenversorgung im Krankenhaus unrichtig gefordert wurde. Aus Sicht der GMDS gibt es immer noch viele Punkte, die überarbeitet oder vereinzelt auch entfernt werden müssten.

Beim Lesen der aktuellen, im März 2014 von den Datenschutzaufsichtsbehörden veröffentlichten zweiten Version der Orientierungshilfe Krankenhausinformationssysteme den Eindruck, dass aus Sicht der Aufsichtsbehörden

- nur Patienten das Recht auf eine informationelle Selbstbestimmung haben und Datenschutz daher nur für diese gelte, nicht aber für die Beschäftigten im Krankenhaus
- Beschäftigte im Krankenhaus grundsätzlich mit dem Vorsatz zur Arbeit gehen, möglichst viele Patientendaten unberechtigterweise zur Kenntnis zu nehmen.

Diesen Eindruck zu erwecken lag sicherlich nicht im Fokus der Ersteller der Orientierungshilfe Krankenhausinformationssysteme. Aber in der Orientierungshilfe Krankenhausinformationssysteme werden des häufigeren Forderungen gestellt, bei denen man sich fragt, ob die Datenschutzaufsichtsbehörden hier eine Abwägung zwischen den wirtschaftlichen Interessen des Krankenhauses und den datenschutzrechtlichen Interessen der Beschäftigten sowie den Belangen eines Patienten vornahmen, oder ob nicht vielmehr die Belange des Patienten als alleiniges Kriterium zur Ableitung der Forderungen der Datenschutzaufsichtsbehörden genutzt wurde. Hier ist sicherlich eine Überarbeitung der Orientierungshilfe Krankenhausinformationssysteme im Sinne einer differenzierteren Betrachtungsweise erforderlich.

Die Erweiterung der Orientierungshilfe Krankenhausinformationssysteme um den Bereich des intersektoralen Datenaustausches, wie er in den Szenarien beschrieben wird, wird von der GMDS ebenfalls befürwortet. In diesem Zusammenhang wäre es wünschenswert, wenn die Aufsichtsbehörden im Anforderungskatalog auch entsprechend auf die intersektorale

Kommunikation eingehen und darstellen, welche Voraussetzungen aus Ihrer Sicht zu erfüllen sind. Insbesondere wäre es erfreulich, wenn die Aufsichtsbehörden für den Datenschutz in diesem Rahmen auch nationale Projekte wie das „IHE-Cookbook“ berücksichtigen und aus datenschutzrechtlicher Sicht kommentieren.

In der Orientierungshilfe Krankenhausinformationssysteme wird nicht immer deutlich, wann sich die Arbeitsgruppe der Datenschutzaufsichtsbehörde mit dem Thema, für das sie eigentlich zuständig ist, beschäftigt, also dem Datenschutz, und wann das Thema IT-Sicherheit angesprochen wird. Die fehlende Abgrenzung zwischen IT-Sicherheit und Datenschutz führt dazu, dass die Arbeitsgruppe mitunter das Ziel der Darstellung der Umsetzung von datenschutzrechtlichen Anforderungen verlässt und sich mit einem Themengebiet befasst, in dem andere Personengruppen vermutlich die bessere Expertise besitzen. Insbesondere, da die Arbeitsgruppe der Datenschutzaufsichtsbehörden zu keinem Zeitpunkt die rechtlichen Grundlagen für die von ihnen gestellten Anforderungen darlegt, wird es häufig zu einem Rätselraten, ob sich die Arbeitsgruppe bei einem bestimmten Punkt mit einem Datenschutz-Thema befasst, oder ob sie ihre Meinung der Umsetzung der IT-Sicherheit darlegt.

Aus Sicht der GMDS muss eine Überarbeitung und Weiterentwicklung der Orientierungshilfe erfolgen, und zwar

- im Sinne der Selbstbestimmung des Patienten
- unter einer stärkeren Berücksichtigung des Wohles des Patienten innerhalb Diagnostik und Behandlung
- im Hinblick auf die Achtung der Persönlichkeitsrechte der Beschäftigten
- in Hinsicht der Darlegung der Rechtsgrundlagen, auf denen die Anforderungen für einen datenschutzkonformen Betrieb eines Krankenhausinformationssystems beruhen.

Für eine erfolgreiche Überarbeitung und Weiterentwicklung müssten aus Sicht der GMDS die Datenschutzaufsichtsbehörden verstärkt auf andere Organisationen zugehen und mit diesen zusammenarbeiten. Derzeit fehlt der Orientierungshilfe Krankenhausinformationssystemen in vielen Fällen die Praxisnähe, die nur durch die Zusammenarbeit der Datenschutzaufsichtsbehörden mit den verschiedenen Organisationen kommen kann. Beispielhaft ohne Anspruch auf Vollzähligkeit seien hier in alphabetischer Reihenfolge genannt:

- Datenschutzfragen: BvD, GDD, GMDS
- Einsatz von Standards: GMDS, HL7-D, IHE-D, Interoperabilitätsforum
- Forschungsfragen: GMDS, TMF
- Krankenhausverwaltung: DKG, GMDS, KH-IT
- Patientenversorgung: Bundesärztekammer, DBfK, GMDS
- Patientenvertretung: BAGP, DAG SHG, vzbv
- Technische Umsetzung: bvitg, GMDS, KH-IT.

Damit die Orientierungshilfe in einer gemeinsamen Anstrengung fit für den Einsatz in der Praxis gemacht wird, ist eine Zusammenarbeit zwischen Datenschutzaufsichtsbehörden und Fachgruppen unabdingbar; das alleinige Vorgehen der Datenschutzaufsichtsbehörden erzeugt ein für die Praxis untaugliches Bürokratiemonster, bei dem zudem die Rechtsgrundlagen für die gestellten Forderungen fragwürdig sind.

3 Allgemeines

Die GMDS begrüßt ausdrücklich den Versuch der Datenschutzaufsichtsbehörden des Bundes, der Länder und der Kirchen, eine für ganz Deutschland geltende Interpretation der für ein Krankenhaus geltenden datenschutzrechtlichen Regelungen zu erstellen. Dies entspricht den Bedürfnissen von Betreibern wie auch von Herstellern von Krankenhausinformationssystemen: bei Betreibern entsteht immer wieder Diskussionsbedarf bei Neueinstellungen, warum Verfahren „x“ im Bundesland 1 genutzt werden darf, in Bundesland 2 jedoch verboten ist und Hersteller müssen haben Kunden in allen Bundesländern, sodass die unterschiedlichen regulativen Normen zu erhöhten Herstellungskosten führen, die letztlich an die Betreiber weitergegeben werden (müssen).

Eine ähnliche Problematik stellt sich im Rahmen der gesetzlichen Krebsregistrierung dar. Auch hier gibt es landesspezifische Regularien, die sich mehr oder weniger stark voneinander unterscheiden. Dies führte dazu, dass die Daten für die epidemiologische Krebsregistrierung nur rudimentär erfasst werden konnten, da die Hersteller derartiger Systeme nicht 16 verschiedene Anforderungen in einem für ein Krankenhaus bezahlbaren Rahmen implementieren konnten. Die Gesellschaft epidemiologischer Krebsregister in Deutschland e.V. (GEKID) ist der Zusammenschluss der gesetzlichen Krebsregister Deutschlands, also der Stellen, welche entsprechend der gesetzlichen Vorgaben für die Krebsregister verantwortlich sind, eine Vereinigung vergleichbar, wie sie die für den Datenschutz verantwortlichen Aufsichtsbehörden mit dem „Düsseldorfer Kreis“ bilden. Die GEKID erstellten einen „Mindestdatensatz“ zur epidemiologischen Krebssicherung, also einen Datensatz der alle Items beinhaltet, welche einerseits für die epidemiologische Krebsregistrierung unverzichtbar ist und andererseits in jedem Bundesland im jeweiligen Landesgesetz enthalten ist.

Gleiches hätte man sich im Rahmen der Ausarbeitung der Orientierungshilfe von den Aufsichtsbehörden für den Datenschutz gewünscht: eine Ausarbeitung, welche einerseits die Anforderungen beinhaltet, welche zur Einhaltung eines datenschutzrechtlichen Betriebs unabdingbar sind, und andererseits in jedem Bundesland ´gefordert werden.

Beim Lesen der Orientierungshilfe gewinnt man jedoch den Eindruck, dass die Aufsichtsbehörden einen Katalog mit den maximal möglichen Forderungen aufstellten. D. h. jede Forderung, die in einem Bundesland erhoben wird, wurde auf alle anderen Bundesländer übertragen. Dabei wurde von den Aufsichtsbehörden anscheinend nicht berücksichtigt, dass

- einige Landesgesetze bis zu 20 Jahre alt sind und die damals aufgestellten datenschutzrechtlichen Anforderungen nicht mehr auf die heutige Patientenversorgung passen,
- einige landesrechtlichen Anforderungen der Bundesgesetzgebung in Hinblick auf der Telematik widersprechen,
- in ländlichen Gebieten andere Voraussetzungen zur Patientenversorgung existieren als in einem Gebiet, in dem eine Großstadt neben der anderen steht.

Forderungen ohne eine gesetzliche Grundlage zu stellen bedeutet, dass sich die Aufsichtsbehörden selbst als gesetzgeberisches Organ präsentieren und zugleich auch noch die Exekutive darstellen - in einem demokratischen Land eigentlich undenkbar. Was die Demokratie anbelangt, sollten sich die Aufsichtsbehörden einmal vor Augen führen, wie die Verteilung bzgl. der Patientenversorgung in Deutschland aussieht. Nachfolgend die Zahlen aus dem Statischen Jahrbuch 2013[2]:

[2] Statistisches Jahrbuch Deutschland und Internationales 2013. Kapitel 4.2.1 Ausgewählte Kennzahlen zu Krankenhäusern, S. 128. Hrsg. Statistisches Bundesamt. ISBN 978-3-8246-1007-5

	Anzahl Krankenhäuser		Anzahl Patienten	
Baden-Württemberg	285	13,9%	2.059.083	11,2%
Bayern	370	18,1%	2.811.503	15,3%
Berlin	79	3,9%	771.418	4,2%
Brandenburg	53	2,6%	544.582	3,0%
Bremen	14	0,7%	200.279	1,1%
Hamburg	47	2,3%	461.221	2,5%
Hessen	174	8,5%	1.299.328	7,1%
Mecklenburg-Vorpommern	39	1,9%	410.150	2,2%
Niedersachsen	197	9,6%	1.615.879	8,8%
Nordrhein-Westfalen	401	19,6%	4.286.435	23,4%
Rheinland-Pfalz	95	4,6%	890.729	4,9%
Saarland	23	1,1%	266.487	1,5%
Sachsen	80	3,9%	986.173	5,4%
Sachsen-Anhalt	49	2,4%	591.354	3,2%
Schleswig-Holstein	94	4,6%	580.808	3,2%
Thüringen	45	2,2%	568.731	3,1%
Bundesgebiet	2045		18.344.160	

Hier muss berechtigterweise gefragt werden, ob beispielsweise Regelungen aus dem Bundesland Berlin, in welchem in weniger als 4% aller in Deutschland existierenden Krankenhäuser knapp 4 % aller Patienten versorgt werden, auf ein Bundesland wie Nordrhein-Westfalen übertragen werden können, in welchem in rund 20% der Krankenhäuser 23 % der Patienten Deutschlands versorgt werden?

Das Vorgehen der Aufsichtsbehörden, die datenschutzrechtlichen Regeln aller Bundesländer zusammen in einem Topf zu geben und daraus die für ganz Deutschland geltende Orientierungshilfe zu „kochen“, ist weder rechtlich erlaubt, noch sinnvoll.

3.1 Abgrenzung Datenschutz vs. IT-Sicherheit

In der Orientierungshilfe Krankenhausinformationssysteme wird nicht immer deutlich, wann sich die Arbeitsgruppe der Datenschutzaufsichtsbehörde mit dem Thema, für das sie eigentlich zuständig ist, beschäftigt, also dem Datenschutz, und wann das Thema IT-Sicherheit angesprochen wird.

Natürlich sind die Themengebiete Datenschutz und IT-Sicherheit eng miteinander verwandt und es gibt viele Bereiche der beiden Sachgebiete, die einander ergänzen. Protokollierung wird beispielsweise sowohl vom Datenschutz als auch von der IT-Sicherheit gefordert, aber bei der Detailtiefe der Protokollierung, der Aufbewahrungsdauer der Protokolldateien und insbesondere bei den Zugriffsmöglichkeiten auf die Protokollinhalte gibt es sehr unterschiedliche Ansichten zwischen Datenschützern und IT-Sicherheitsexperten.

Die fehlende Abgrenzung zwischen IT-Sicherheit und Datenschutz führt dazu, dass die Arbeitsgruppe mitunter das Ziel der Darstellung der Umsetzung von datenschutzrechtlichen Anforderungen verlässt und sich mit einem Themengebiet befasst, in dem andere Personengruppen vermutlich die bessere Expertise besitzen. Insbesondere, da die Arbeitsgruppe der Datenschutzaufsichtsbehörden zu keinem Zeitpunkt die rechtlichen Grundlagen für die von ihnen gestellten Anforderungen darlegt, wird es häufig zu einem Rätselraten, ob sich die Arbeitsgruppe bei einem bestimmten Punkt mit einem Datenschutz-Thema befasst, oder ob sie ihre Meinung der Umsetzung der IT-Sicherheit darlegt.

Damit die Orientierungshilfe Krankenhausinformationssysteme den im Krankenhaus verantwortlichen Führungskräften wirklich eine Orientierungshilfe sein kann, sollten diese Unklarheiten in der aktuellen Version beseitigt werden. D. h.

1. Darlegung der (landes-) rechtlichen Grundlagen für die einzelnen Forderungen,
2. Erklären, wann die Darstellung lediglich die Meinung der Aufsichtsbehörde widerspiegelt und
3. Abgrenzung zwischen Datenschutz und IT-Sicherheit vollziehen.

3.2 Datenschutz bei den im Krankenhaus Beschäftigten

Die Aufsichtsbehörden beschäftigen sich in der Orientierungshilfe ausschließlich mit dem Schutz von Patientendaten. Die Beschäftigten in einem Krankenhaus sind ebenfalls natürliche Personen, welche ein Anrecht auf Datenschutz genießen.

In vielen Punkten wird deren Recht auf die informationelle Selbstbestimmung durch die in der Orientierungshilfe Krankenhausinformationssysteme berührt und auch eingeschränkt (Beispiel Protokollierung), ohne dass die Aufsichtsbehörden an den jeweiligen Stellen hierauf eingehen.

Da die Aufsichtsbehörden jedoch nicht alleine für den Patientendatenschutz zuständig sind, sondern zu den Aufgaben der Datenschutzaufsichtsbehörden die Wahrnehmung der Datenschutzrechte aller Betroffenen gehört, kann und muss man erwarten, dass in der Orientierungshilfe auch die datenschutzrechtlichen Fragen der betroffenen Beschäftigten des Krankenhauses angesprochen und dargelegt werden, insbesondere, wenn Forderungen der Aufsichtsbehörde die informationelle Freiheit der im Krankenhaus Beschäftigten einschränken.

Hier wünscht man sich, dass in der nun vorliegenden überarbeiteten Ausgabe der Orientierungshilfe Krankenhausinformationssysteme etwas mehr Sensibilität und Verantwortungsbewusstsein in Bezug auf die Rechte zur informationellen Selbstbestimmung der im Krankenhaus Beschäftigten gezeigt worden wäre und an Stellen, in denen die Aufsichtsbehörden die Rechte dieser Betroffenen durch die in der Orientierungshilfe aufgestellten Forderungen einschränkt, die entsprechenden (landes-) rechtlichen Normen benennt, welche der verlangten Beschränkung der Datenschutzrechte zu Grunde liegen.

Denn auch für die Beschäftigten gilt, dass eine Datenverarbeitung entweder eine rechtliche Grundlage oder das Einverständnis der jeweils betroffenen (natürlichen) Person bedarf.

4 Formales

4.1 Übersicht zur Orientierungshilfe

Die Orientierungshilfe Krankenhausinformationssysteme besteht aus zwei Teilen: Teil 1 wurde „Rechtliche Rahmenbedingungen“ genannt, Teil 2 „Technische Anforderungen“.

Teil 1 soll dabei die geltenden datenschutzrechtlichen Rahmenbedingungen aufzeigen, zugleich Vorgaben zur ärztlichen Schweigepflicht darstellen[3]. Hierzu muss angemerkt werden, dass die ärztliche Schweigepflicht kein Bestandteil des Datenschutzrechts, sondern des Strafrechts ist und damit auch nicht in den Zuständigkeitsbereich der Datenschutz-Aufsichtsbehörden fällt. (Insbesondere, da Verfehlungen nach §203 StGB ein Antragsdelikt darstellen, d. h. nur auf Antrag des Betroffenen verfolgt werden darf.) Letztlich ist eine vollständige Trennung zwischen Schweigen aus Datenschutzgründen und Schweigen aus Strafrechtsgründen juristisch zwar vollziehbar, im täglichen Leben muss es jedoch zusammen betrachtet werden. Insofern ist es zu begrüßen, dass die Aufsichtsbehörden sich hier des Themas der ärztlichen Schweigepflicht ebenfalls annahmen.

Teil 1 beschreibt dabei in abstrakter Form Vorgänge aus dem Krankenhausalltag und konkretisiert anhand dieser Vorgänge, welche Anforderungen aus Sicht der Datenschutzaufsichtsbehörden erfüllt sein müssen, damit der Vorgang aus datenschutzrechtlicher Sicht durchgeführt werden darf.

In Teil 2 der Orientierungshilfe Krankenhausinformationssysteme werden Maßnahmen beschrieben, die der (technischen) Umsetzung der geschilderten datenschutzrechtlichen Anforderungen dienen. Dabei können die dort beschriebenen Maßnahmen nur als Beispiele angesehen werden, da die Datenschutzgesetze zwar Ziele vorgeben, aber nicht wie die Ziele erreicht werden müssen. Daher müssen die in Teil 2 der Orientierungshilfe genannten Maßnahmen nicht als konkrete Anforderungen, sondern als beispielhafte Möglichkeit(en) der Umsetzung der von den Datenschutz-Aufsichtsbehörden gestellten Anforderungen angesehen werden.

Obwohl als Titel von Teil 1 „Rechtliche Rahmenbedingungen“ gewählt wurde, werden die den Anforderungen zugrunde liegenden Rechtsnormen weder in Teil 1 noch in Teil 2 benannt. Ob die jeweiligen Anforderungen der Datenschutzaufsichtsbehörden daher eine rechtliche Grundlage besitzen oder nur aus Sicht der Datenschutzaufsichtsbehörde eine aus Sicht des Datenschutzes sinnvolle Forderung darstellen, muss daher im jeweiligen Einzelfall entschieden werden. Ein Hinweis zu Interpretationsmöglichkeiten zu den jeweiligen Punkten erfolgt in Kapitel 5.

4.2 Die Orientierungshilfe als Prüfkatalog für die Aufsichtsbehörden

Die Orientierungshilfe Krankenhausinformationssysteme kann keinen Anforderungskatalog für eine datenschutzkonforme Kontrolle durch die Aufsichtsbehörden darstellen, auch wenn dies in der Orientierungshilfe Krankenhausinformationssysteme so beschrieben wurde:

> „Für die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzaufsichtsbehörden (Aufsichts- und Kontrollbehörden) wird das vorliegende Dokument den Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit bilden.“[4]

Die Datenschutz-Aufsichtsbehörden versuchten die Vorgaben aller Bundesländer in die Orientierungshilfe einzubeziehen und damit stehen in der Orientierungshilfe zwangsläufig einige Anforderungen, die nur auf ein oder mehrere Bundesländer zutreffen, nicht jedoch auf

[3] Zitat aus „Begleitpapier zur Orientierungshilfe Krankenhausinformationssysteme“, Seite 1, 2. Absatz

[4] Zitat aus „Begleitpapier zur Orientierungshilfe Krankenhausinformationssysteme“, Seite 1, 3. Absatz

alle Bundesländer. Damit existieren zwangsläufig Anforderungen in der Orientierungshilfe Krankenhausinformationssysteme, welche einer rechtlichen Grundlage für das betreffende Bundesland fehlt. Da eine datenschutzrechtliche Prüfung letztlich aber immer eine Prüfung gegen die zugrunde liegende gesetzliche Norm darstellt, ist die Orientierungshilfe hier als das zu verstehen, was der Name aussagt: als eine Orientierungshilfe.

4.2.1 Anwendungszeitraum

Die Orientierungshilfe gibt an, dass für die Hersteller bzgl. der Anforderungen aus der Orientierungshilfe eine „angemessene Übergangsfrist“[5] notwendig ist, ohne diese Frist zu zu nennen. Somit bleibt unklar, ab wann die Anforderungen an die Hersteller gelten.

Andererseits schreiben die Datenschutzaufsichtsbehörden:

> „Soweit sich die Anforderungen an die Krankenhäuser als Betreiber richten und entweder organisatorische Regelungen beim Einsatz von Krankenhausinformationssystemen betreffen oder mittels vorhandener Informationstechnik umgesetzt werden können, soll die Orientierungshilfe bereits jetzt herangezogen werden.“

Hierbei übersehen die Aufsichtsbehörden, dass nicht alles, was mit IT umgesetzt werden kann, auch einsatzfähig ist.

Beispiel: In vielen Informationssystemen kann die von den Aufsichtsbehörden geforderte Protokollierung umgesetzt werden, indem die Software mittels des Debug-Modus alles aufzeichnet. Damit kann die Anforderung anhand vorhandener Informationstechnik umgesetzt werden. Zugleich wird das Informationssystem jedoch so langsam, dass es faktisch nicht einsetzbar ist.

Einerseits bleibt die Orientierungshilfe bei den Anforderungen an die Hersteller eher verschwommen, da kein zeitlicher Umsetzungszeitraum genannt wird, andererseits wird durch die ungenaue Darstellung bei den Betreibern evtl. ein Einsatz eines Informationssystems gefordert, der letztlich Patientenleben gefährden kann.

Vermutlich haben die Aufsichtsbehörden beides nicht im Sinn gehabt. Seitens der Hersteller wird ein zeitnaher (= z. B. innerhalb der nächsten 2 Jahre) Umsatz der Anforderungen gewünscht, seitens der Betreiber eine sofortige Umsetzung des Machbaren, ohne das Patienten gefährdet werden. Es wäre wünschenswert, wenn dies so auch formuliert wird: die Hersteller hätten Planungssicherheit bzgl. der Releaseplanungen hinsichtlich der Umsetzung der Orientierungshilfe Krankenhausinformationssysteme und die Betreiber wüssten, dass auch bei den Aufsichtsbehörden das Patientenwohl an erster Stelle steht und die machbare Umsetzung immer im Hinblick auf die erfolgreiche Patientenversorgung betrachtet werden muss und nicht allein bzgl. der technischen Machbarkeit.

4.3 Zielrichtung der AG für die Überarbeitung

Ende 2012 beschloss die Arbeitsgruppe bestehend aus Mitgliedern der Arbeitskreise „Gesundheit und Soziales“ sowie „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine „redaktionelle Überarbeitung“[6] der „Orientierungshilfe Krankenhausinformationssysteme“.

Entsprechend der Zielsetzung wurde inhaltlich wenig geändert, vielmehr wurden sprachliche Anpassungen vorgenommen. Beispielsweise wurde der Begriff „Mitarbeiter“ konsequent durch „Beschäftigte“ ersetzt oder auch „Kennzeichen“ durch „Merkmale“.Weiterhin wurden mehrere Anforderungen, welche in der „alten“ OH KIS in einem Aufzählungspunkt vereint

[5] Begleitpapier zur Orientierungshilfe „Krankenhausinformationssysteme“, S. 1, Abs. 4

[6] Zitat aus dem Vorwort zur 2. Fassung der OH KIS

aufgeführt wurden, in der Überarbeitung teilweise in einzelne Punkte gegliedert. Andere Punkte wurden vollständig gestrichen, sodass die Nummerierung in der überarbeiteten Version teilweise von der Nummerierung der ersten Version der OH KIS abweicht.

Die Überarbeitung seitens der Arbeitsgruppe berücksichtigte dabei den „regen Austausch", den die Arbeitsgruppe mit Vertretern der Hersteller und Betreiber führte.

4.4 Formale Änderungen der Überarbeitung

Die Anzahl der aufgeführten Punkte in der OH KIS wurde von 159 auf 151 reduziert:

		OH KIS v01	OH KIS v02
Teil 1		41	48
Teil 2	**Datenmodell**	15	16
	Systemfunktionen	15	19
	Anwendungsfunktionen	16	12
	Rollen- und Berechtigungskonzept	20	18
	Datenpräsentation	4	4
	Nutzungsergonomie / Systemzugang	13	5
	Protokollierung	25	22
	Technischer Betrieb, Administration	10	7
		159	151

Dabei sind die Zählungen zwischen alter und neuer Ausgabe der Orientierungshilfe punktuell verschieden. So kennt die alte Ausgabe der Orientierungshilfe noch Unterpunkte („30a, 30b, ...), die neue Ausgabe jedoch nicht. Weiterhin wurden einzelne Absätze der alten Ausgabe der Orientierungshilfe eigenständige Punkte in der Neufassung der Orientierungshilfe Krankenhausinformationssysteme. Daher ist es die Auflistung einer Übersicht über gelöschte Punkte der alten Orientierungshilfe sowie der neu eingeführten Punkte in der Neufassung der Orientierungshilfe zur Einschätzung der Entwicklung sinnvoll:

		OH KIS v01	OH KIS v02
		Gelöscht	**Neu**
Teil 1		5	8
Teil 2	**Datenmodell**	3	4
	Systemfunktionen	2	4
	Anwendungsfunktionen	7	2
	Rollen- und Berechtigungskonzept	3	1
	Datenpräsentation	0	0
	Nutzungsergonomie / Systemzugang	9	1
	Protokollierung	13	9
	Technischer Betrieb, Administration	4	0
		46	29

4.4.1 Änderungen im ersten Teil der OH KIS

Der erste Teil der Orientierungshilfe richtet sich an die Betreiber, wenngleich Hersteller hier natürlich Hinweise bzgl. Mechanismen finden, die in ihren Systemen implementiert werden sollten.

Im Folgenden wird nicht auf jeden gelöschten Punkt eingegangen, die neu hinzugekommenen Punkte werden in Kapitel 5.1 besprochen. Aber einige gelöschte Punkte, die deutliche Kritik hervorriefen, sollen kurz angesprochen werden.

Einer der am meisten kritisierten Punkte der alten Orientierungshilfe war Punkt 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."

Hierbei stellte niemand die Richtigkeit des ersten Satzes in Frage, der in dieser Form eine der Grundlagen des Datenschutzrechts widerspiegelt. Vielmehr war es der zweite Satz, welcher zu Unverständnis führte. Einerseits wird jeder Patient bei der Erhebung der Daten auf sein Recht hingewiesen, der Verwendung seiner Daten zu widersprechen. D. h. der Patient weiß zum Zeitpunkt seiner Wiederkehr ins Krankenhaus um dieses Recht und muss nicht darauf hingewiesen werden; zudem es für diese Anforderung keine rechtliche Grundlage gibt. Letztlich bleibt es auch zweifelhaft, ob ein erkrankter Mensch zum Zeitpunkt seiner Neuaufnahme auch wirklich frei darüber entscheiden kann. D. h., wenn er vorher, im gesunden Zustand, der Verwendung seiner Daten nicht widersprach, ist kaum damit zu rechnen, dass ein erkrankter Mensch der Verwendung seiner Daten, die evtl. zu seiner Gesundung beitragen können, widerspricht.

Konsequenterweise reagierte die Arbeitsgruppe der Datenschutzaufsichtsbehörden und entfernte diesen Punkt aus der Orientierungshilfe.

Punkt 5 der alten Fassung der Orientierungshilfe erlaubte die Anlegung eines „Basisdatensatzes" auf Grundlage einer Einwilligung eines Patienten. Einerseits wurde der Begriff „Basisdatensatz" von der Arbeitsgruppe der Datenschutzaufsichtsbehörden nicht definiert, andererseits ist es eine Selbstverständlichkeit, dass ein solcher Basisdatensatz mit Einwilligung des Patienten erstellt und genutzt werden darf. Auch dieser Punkt wurde gestrichen.

4.4.2 Änderungen im zweiten Teil der OH KIS

Im zweiten Teil der OH KIS werden Forderungen der Arbeitsgruppe explizit Herstellern (H) und (Betreibern) von Krankenhausinformationssystemen zugewiesen. Dabei unterscheidet die Arbeitsgruppe drei Kategorien: „Weiterhin wird differenziert zwischen zwingenden Anforderungen („muss"), Anforderungen, ohne deren Einhaltung ein datenschutzgerechter Betrieb eines KIS wesentlich erschwert wird („soll"), und Anforderungen, die allgemein einen datenschutzfreundlichen Einsatz unterstützen („sollte"). Bei nicht erfüllten zwingenden Anforderungen an Konfiguration und Nutzung des KIS"[7].

Dabei „profitieren" Hersteller und Betreiber von der Verringerung der Anzahl der explizit aufgelisteten Anforderungen unterschiedlich. Im Folgenden wird summarisch dargestellt, wie sich die „muss"-, „soll"- und „sollte"-Anforderungen verteilen. Bei der Interpretation der

[7] Zitat aus „Begleitpapier zur Orientierungshilfe Krankenhausinformationssysteme", Seite 1, 3. Absatz

[7] Zitat aus der OH KIS, Teil 2, Vorbemerkung Seite 3

Zahlen muss jedoch beachtet werden, dass Betreiber einige Anforderungen nur umsetzen können, wenn zuvor die Hersteller die technischen Voraussetzungen schaffen. Daher erscheint es begreiflich, wenn mehr Anforderungen an Hersteller gerichtet werden als an die Betreiber, auch wenn Letztere letztlich für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich sind.

Dabei veränderten sich die Anforderungen an die Hersteller wie folgt:

Teil 2	Muss		Soll		Sollte	
	v01	v02	v01	v02	v01	v02
Datenmodell	11	11	4	3	1	1
Systemfunktionen	10	9	4	4	2	3
Anwendungsfunktionen	10	4	4	7	3	0
Rollen- und Berechtigungskonzept	15	14	1	0	4	5
Datenpräsentation	2	2	1	1	1	1
Nutzungsergonomie / Systemzugang	7	3	1	0	4	3
Protokollierung	11	11	3	2	3	3
Technischer Betrieb, Administration	4	1	2	1	0	0
	70	55	20	18	18	16

D. h. die Arbeitsgruppe der Datenschutz-Aufsichtsbehörden reduzierte die Anzahl von Anforderungspunkten gegenüber den Herstellern um insgesamt 19 Punkte: 15 „Muss"-Kriterien, 2 „Soll"-Kriterien und 2 „Sollte"-Kriterien. Oder anders ausgedrückt: 17,6% der Forderungen der Arbeitsgruppe gegenüber den Herstellern werden nicht mehr aufgeführt.

Bei den Betreibern veränderte die Arbeitsgruppe den Anforderungskatalog wie folgt:

Teil 2	Muss		Soll		Sollte	
	v01	v02	v01	v02	v01	v02
Datenmodell	9	7	3	3	0	1
Systemfunktionen	8	8	2	3	0	1
Anwendungsfunktionen	2	1	3	7	0	
Rollen- und Berechtigungskonzept	5	6	1	2	4	1
Datenpräsentation	0	0	1	1	0	0
Nutzungsergonomie / Systemzugang	2	1	0	0	2	2
Protokollierung	12	11	2	1	3	2
Technischer Betrieb, Administration	6	3	3	1	1	2
	44	37	15	18	10	9

Bzgl. den Anforderungen gegenüber den Betreibern reduzierte die Arbeitsgruppe also die Gesamtpunktzahl um 5 Forderungen, wobei die „Muss"-Kriterien um 7 Punkte und die „Sollte"-Kriterien um 1 Punkt reduziert wurden, die „Soll"-Kriterien jedoch um 3

Anforderungspunkte erhöht wurden. Oder prozentual ausgedrückt: 7,2% der ursprünglichen Forderungen der Arbeitsgruppe gegenüber den Betreibern finden sich nicht mehr in der Überarbeitung.

5 Kommentierung der in der OH KIS aufgeführten Anforderungspunkte

5.1 Teil 1: „Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen“

5.1.1 Aufnahme

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.

Rechtliche Einschätzung: Zur Legitimierung der oben genannten Forderung wird in der Regel die Vertraulichkeit der Patientendaten zitiert, welche durch die ärztliche Schweigepflicht abgesichert wird. Neben §203 StGB sind hier die Datenschutzbestimmungen des Bundes und der Länder sowie §85 Abs. 2 Satz 3 und 5 SGB X vorrangige Rechtsvorschriften.

Ob eine Aufnahmekraft jedoch in den Geltungsbereich eines Gehilfen im Sinne von §203 Abs. 3 Satz 2 fällt, hängt auch von der Organisationsstruktur eines Krankenhauses ab. Ein Pförtner kann ebenfalls Erfüllungsgehilfe des Arztes sein (vgl. OLG Oldenburg, Beschluss vom 10.06.1982 - 2 Ws 204/82). Dann greifen die oben genannten Vorschriften nicht, wenn die Aufnahmekraft diese Daten dienstlich zur Kenntnis nimmt; die Aufnahmekraft ist dann ein Gehilfe und somit ein Befugter im Sinne der datenschutzrechtlichen Vorschriften.

Kommentierung: Die Forderung der Aufsichtsbehörden ist schon heute in nahezu jedem Krankenhaus in Deutschland umgesetzt. Identifikationsdaten wurden von den Mitarbeitern und Mitarbeiterinnen der Aufsichtsbehörden in ihrer Ausarbeitung nicht definiert. Dementsprechend ist hier ein Interpretationsspielraum gegeben. Bei der Aufnahme im Krankenhaus werden im Zweifelsfall alle Daten verwendet, die eine Identifikation eines Patienten ermöglichen. Dies ist auch notwendig, da nur so evtl. vorhandene Voruntersuchungen, Diagnosen usw. bekannt sind, welche den aktuellen Behandlungsverlauf entscheidend beeinflussen können.

Das Krankenhaus kann - je nach eingesetztem IT-System- die missbräuchliche Verwendung der Suchfunktion entdecken, indem regelmäßig eine Prüfung bzgl. stornierter Fälle erfolgt, ergänzt durch eine Überprüfung der Fälle, die nicht abgerechnet werden.

Allerdings stellt sich die Frage, welcher Missbrauch nachträglich kontrolliert werden soll/muss, wenn die administrative Aufnahmekraft lediglich auf Identifikationsdaten zugreifen darf,

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.

Rechtliche Einschätzung: Die rechtliche Argumentation erfolgt hier analog Ziffer 1, denn auch eine vorbehandelnde Organisationseinheit kann theoretisch medizinische Daten enthüllen, z. B. die Behandlung auf der Station, wo AIDS-Patienten behandelt werden. Entsprechend darf eine administrative Aufnahmekraft keine Möglichkeit zur Kenntnisnahme medizinischer Daten haben, ausgenommen die Aufnahmekraft fungiert als ärztlicher Gehilfe.

Kommentierung: Im heutigen Klinikalltag werden Stationen häufig interdisziplinär belegt, sodass die Angabe einer vorbehandelnden Organisationseinheit nicht als medizinisches Datum anzusehen ist. Der Hinweis auf einen abgeschlossenen Fall beachtet nur Abrechnungsgründe, ohne medizinische Notwendigkeiten zu hinterfragen: Es gibt durchaus Gründe, warum eine administrative Aufnahmekraft wissen muss, warum ein Patient ein Krankenhaus aufsucht (z. B. zentrale Aufnahme, welche den Patienten anschließend zu dezentralen medizinischen Aufnahmen schickt). Zudem ist unter den heutigen Gegebenheiten der Abschluss eines Falles nicht mehr so eindeutig definierbar (z. B. Wiederaufnahme in der oberen Grenzverweildauer).

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

Rechtliche Einschätzung: Entsprechend §254 BGB muss die Aufnahmekraft die Möglichkeit haben, den Patienten auf eine mögliche Gefährdung Dritter, die von ihm ausgeht, warnen können. Gleiches gilt für die in die Behandlung integrierten Personen auf Station oder Ambulanz sowie die künftigen Mitpatienten des zur Aufnahme anstehenden Patienten: auch sie haben ein Recht, vor einer potenziellen Gefährdung geschützt zu werden.

Kommentierung: Die Einschränkung bzgl. Kenntnisnahme von Hinweisen seitens der Aufnahmekraft auf Betrugsversuche/Zahlungsunfähigkeit und multiresistente Keime ist nicht zielführend. Generell muss eine Aufnahmekraft alle Daten zur Kenntnis nehmen, die für eine Aufnahme unabdingbar sind. Welche Daten dies sind, hängt von der Aufgabenstellung entsprechend der organisatorischen Aufstellung innerhalb des Krankenhauses ab. Bei einigen Prominenten ist z. B. die Pseudonymisierung der Aufnahmedaten gewünscht, z. B. aus Gründen des Personenschutzes. Die Aufnahmekraft, welche die realen Personendaten erhebt, muss dementsprechend ggfs. vorhandene Vorbefunde trotz Pseudonymisierung wiederfinden und vorhandene Stammdaten erneuern. Eine Neuaufnahme würde bedeuten, dass ein Zugriff auf bereits vorhandene medizinische Daten nicht möglich ist und unter Umständen das medizinische Risiko der Behandlung deutlich erhöhen.

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.

Rechtliche Einschätzung: Grundsätzlich gilt auch in diesem Fall die datenschutzrechtliche Grundbestimmung, dass Daten nur mit Zustimmung des Betroffenen oder basierend auf einer

rechtlichen Grundlage weitergegebenen werden dürfen. Dies bedeutet, dass der Patient in die Weitergabe seiner Daten durch die Pforte zustimmen muss. In der Regel wird dies im Krankenhausaufnahmevertrag abgebildet; hier entscheidet der Patient, ob er mit der Weitergabe seiner Daten einverstanden ist oder nicht.

Allerdings existieren in verschiedenen Bundesländern Erlaubnistatbestände zur Unterrichtung von Angehörigen bzw. Partnern (z. B. § 11 Abs. 1 Nr. 6 HmbKHG oder §4 Abs. 1 Nr. 4 BremKHDSG).

Kommentierung: Die Möglichkeit, die Anweisung einer Patientin bzw. eines Patienten, dass keine Auskunft bzgl. Anwesenheit im Krankenhaus und/oder Erkrankung an Außenstehende gegeben wird (= „Auskunftssperre"), ist heute in den meisten Krankenhausinformationssystemen umsetzbar, wenngleich nur wenige Patienten diese Möglichkeit nutzen wollen. Die Regel ist, dass die Patienten wollen, dass ihre Angehörigen informiert werden. Häufig werden Mitarbeiter/innen vor einer OP angesprochen und explizit gebeten, dass die Angehörigen schnellstmöglich über den Ausgang informiert werden, damit die Ungewissheit beendet wird. In der juristischen Literatur wird in diesen Situationen bei fehlendem Widerspruch eines Patienten daher von einer konkludenten Einwilligung ausgegangen. Hierbei ist zu bemerken, dass bei einer konkludenten Einwilligung die datenschutzrechtlich geforderte Schriftform nicht eingehalten wird und diese somit einer rechtlichen Nachprüfung nicht standhalten kann.

Staatlichen Behörden muss jedoch ggf. auch ohne Zustimmung des Patienten eine entsprechende Auskunft gegeben werden. Dies muss organisatorisch natürlich nicht notwendigerweise durch die Pforte/Auskunftsperson erfolgen, aber die Auskunftsperson muss wissen, dass bei Auskünften bzgl. zu dieser Patientin/diesem Patienten Ansprechpartner xy verständigt werden muss; ggf. mit dem Hinweis, dass die Pforte/Auskunftsperson zu dieser Patientin/diesem Patienten keine Auskunft geben darf. Ein leeres Suchergebnis wird dieser Aufgabenstellung nicht gerecht und verhindert unter Umständen, dass das Krankenhaus seinen gesetzlichen Verpflichtungen nachkommt.

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.

Rechtliche Einschätzung: Hier gilt das zu Ziffer 1 Gesagte. Entsprechend der Aufgabenstellung, welche aus dem Organisationsablauf im Krankenhaus für die Aufnahmekraft ablesbar ist, muss Zugriff auf die zur Erfüllung der Aufgabe benötigten Daten existieren. Ist die Aufnahmekraft hierbei als ärztlicher Gehilfe anzusehen, darf auch Zugriff auf medizinische Daten existieren.

Kommentierung: -

5.1.2 Behandlung

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

Rechtliche Einschätzung: Die Grundlage dieser Aussage ergibt sich implizit aus der gesetzlichen Forderung, dass nur berechtigte Personen Zugriff auf personenbezogene oder personenbeziehbare Daten bekommen dürfen. Ist eine Person aber berechtigt, muss ihr auch ein Zugriff möglich sein.

Kommentierung: -

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

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

Rechtliche Einschätzung: Die rechtliche Grundlage bildet die gesetzliche Forderung, dass nur berechtigte Personen auf personenbezogene oder personenbeziehbare Daten zugreifen dürfen. Innerhalb einer Organisation muss dementsprechend festgelegt werden, wer welche Aufgaben hat und welche Berechtigungen diese Aufgaben mit sich bringen, z. B. durch ein Berechtigungskonzept. Die Forderung zu einer dokumentierten Zuweisung von Rechtevergaben ergibt sich aus der datenschutzrechtlichen Anforderung, dass einem Betroffenen jederzeit Auskunft erteilt werden muss, wer wann unter welchen Umständen aus welchen Gründen auf welche Daten des Betroffenen Zugriff erhielt.

Kommentierung: Die Umsetzung ist in vielen der derzeit auf dem Markt befindlichen Krankenhausinformationssystemen mitunter nicht möglich. Viele der Systeme basieren auf einer Datenbankstruktur, welche Anfang der 90er Jahre entwickelt wurde, und können Rechte nur abteilungsbezogen vergeben. Die heute übliche abteilungsübergreifende Behandlung ist oftmals kaum abbildbar.

5.1.2.1 Zugriffe durch Ärzte

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.

Rechtliche Einschätzung: Auch bei dieser Aussage ergibt sich die Billigkeit implizit aus der gesetzlichen Forderung, dass nur berechtigte Personen Zugriff auf personenbezogene oder personenbeziehbare Daten bekommen dürfen. Ist eine Person berechtigt, muss ihr ein Zugriff auf die Daten ermöglicht werden.

Kommentierung: Unabhängig vom Behandlungsprozess stehen im Krankenhaus auch andere Aufgaben an, z. B.

- Forschung
- Qualitätssicherung
- Controlling
- MDK

sodass die Erlaubnis für den Zugriff auf die Daten allein an die Behandlung des einzelnen Patienten zu knüpfen für die tägliche Arbeit in einem Krankenhaus zu kurz greift. Die getroffene Aussage ist für die Behandlungssituation zutreffend, stellt somit aber keine abschließende Aussage bzgl. des Zugriffs auf Patientendaten durch Ärzte dar.

10. Erweiterung des Kreises der Zugriffsberechtigten erfolgt auf der Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes (z. B. Zuweisung zu einer weiteren funktionsbezogenen Organisationseinheit, Einbeziehung eines weiteren Arztes bei interdisziplinärer Behandlung, Konsilaufträge) ab dem Zeitpunkt des konkreten Behandlungsauftrags.

Rechtliche Einschätzung: siehe Punkt 9.

Kommentierung: Die Umsetzung in den verschiedenen in Deutschland eingesetzten klinischen Informationssystemen ist unterschiedlich ausgeprägt, sodass die technische Umsetzung in einigen Krankenhäusern nicht möglich ist. Hier müssen dann die technisch erweiterten Zugriffsrechte durch organisatorische Bestimmungen begleitet bzw. Ergänzt wird.

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.

Rechtliche Einschätzung: Die Berechtigung der Aussage des ersten Satzes ergibt sich aus der datenschutzrechtlichen Forderung, dass berechtigte Personen einen Zugriff auf die entsprechenden Daten erhalten dürfen. Bzgl. des zweiten Satzes beruht die Billigkeit der Forderung auf der Tatsache, dass die Behandler der abgebenden Organisationseinheit nicht mehr zum Behandlungskreis des Patienten gehören und somit bzgl. neu angefallener Daten nicht zum berechtigten Personenkreis gehören.

Kommentierung: Der Zugriff auf Patientendaten muss teilweise schon vor dem vollzogenen Wechsel erfolgen, z. B. bei Übergabe aus dem OP. D. h., der Zugriff muss ab dem Zeitpunkt der Planung eines Wechsels einer Organisationseinheit zu einer anderen möglich sein.

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

Rechtliche Einschätzung: Im Falle einer Mitbehandlung ergibt sich die Berechtigung auf den Zugriff der Daten eines Patienten aus der Notwendigkeit, dass die ärztliche Dienstleistung ohne Zugriff auf die dafür benötigten Daten nicht möglich ist. Im Rahmen des Bereitschafts- oder Notdienstes vertritt die anwesende ärztliche Person den regulär behandelnden und benötigt daher Zugriff auf alle Patientendaten. Datenschutzrechtlich ist der Zugriff auf die selbst erhobenen Daten immer erlaubt, da man faktisch „Herr der Daten" ist.

Kommentierung: Die Beschränkung auf den Zugriff der Daten, welche auf Grund eigenerbrachter Leistungen entstanden, ist unzulänglich. Die medizinische Behandlung erfolgt heute im Krankenhaus immer interdisziplinär, sodass der Zugriff auf die Daten, welche beispielsweise konsiliarisch erbracht wurden, erforderlich ist. D. h., der Zugriff auf

beauftragte Leistungen wie beispielsweise Laborergebnisse, Radiologiebefunde muss immer möglich sein.

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.

Rechtliche Einschätzung: Im Falle einer konsiliarischen Mitbehandlung ergibt sich die Berechtigung auf den Zugriff der Daten eines Patienten aus der Notwendigkeit, dass die ärztliche Dienstleistung ohne Zugriff auf die dafür benötigten Daten nicht möglich ist. Daraus folgert jedoch, dass der Konsiliarius keinen „Generalzugriff" auf alle Daten bekommen darf, sondern nur auf die für die Erbringung des Konsils notwendigen Daten.

Eine zeitliche Beschränkung auf die Daten, welche aus den durch den Konsildienst erbrachten Leistungen resultieren, darf nicht erfolgen, da diese Daten zum Konsiliarius gehören. D. h., die Daten gehören zum Konsildienst.

Kommentierung: Konsilanforderungen sind Anforderungen an spezialisierte Dienstleister, welche eine Leistung erbringen, die nur durch die fachliche Kompetenz der Konsildienstleister ermöglicht wird. Ohne die fachliche Kompetenz ist eine Beschränkung der Inhalte, welche der Konsildienstleister einsehen darf, schwierig; ggf. werden dem Konsildienstleister Informationen vorenthalte, welche die Entscheidung maßgeblich beeinflussen würde. Haftungsrechtlich ist dies für das Krankenhaus schwierig umzusetzen, eine Absicherung nur schwer möglich. Daher muss häufig der Konsiliarius entscheiden, welche Daten er für die Erbringung seines Konsildienstes benötigt.

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.

Rechtliche Einschätzung: Wenn ein Grund für einen berechtigten Zugriff gegeben ist, ist damit implizit ein datenschutzrechtlicher Erlaubnistatbestand gegeben („berechtigte Person"). Eine Verpflichtung zur Anzeige eines Hinweises ist rechtlich nicht begründbar. Die Notwendigkeit der Dokumentation des Zugriffs und des entsprechenden Grundes ergibt sich zwingend aus der ärztlichen Dokumentationspflicht, z. B. aus §630f BGB.

Kommentierung: -

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.

Rechtliche Einschätzung: Auch hier gilt wieder der datenschutzrechtliche Umstand, dass berechtigte Personen Zugriff auf die Daten erhalten, für welche die Berechtigung existiert. Selbstverständlich gilt dies für die Patienten, welche ein Belegarzt behandelt.

Kommentierung: In einigen Krankenhäusern führen Belegärzte Konsile in ihrem Fachbereich durch. In diesem Fall benötigen die Beleg-/Konsilärzte Zugriff auf die entsprechenden Daten der Patienten. Des weiteren führen in einigen Häusern Beleg-Ärzte den Bereitschaftsdienst durch. Beispiel: in einer Beleg-HNO-Abteilung operieren drei Beleg-Ärzte ihre HNO-Patienten. Nach 15.00 Uhr ist abwechselnd jeweils einer der 3 Beleg-Ärzte für Notfälle telefonisch erreichbar, sodass jeder HNO-Arzt nicht nur Zugriff auf die Daten „seiner" Patienten benötigt.

Durch die Nutzung der Begrifflichkeit der „beteiligten Mitarbeiter" können weitere Abgrenzungsschwierigkeiten entstehen: Häufig wird eine Beleg-Abteilung von mehreren Belegärzten genutzt, sodass das Personal des Krankenhauses Patienten mehrerer Belegärzte (mit-) behandelt.

Hier muss der Grundsatz gelten, dass eine an der Behandlung eines Patienten beteiligte Person Zugriff auf alle benötigten Daten erhält.

Unabhängig von der direkten Behandlung des Patienten benötigen auch administrative Mitarbeiter (Controlling, Case-Manager, …) Zugriff auf die Patientendaten.

5.1.2.2 Zugriffe durch den pflegerischen Stationsdienst

16. Der Zugriff des Pflegepersonals auf die erforderlichen pflegerischen und medizinischen Daten ist auf die in der eigenen funktionsbezogenen Organisationseinheit (z. B. Station) behandelten Patienten zu begrenzen.

Rechtliche Einschätzung: Auch im pflegerischen Bereich beruht die rechtliche Grundlage auf der gesetzlichen Forderung, dass nur berechtigte Personen auf personenbezogene oder personenbeziehbare Daten zugreifen dürfen. Innerhalb einer Organisation muss aufgrund dessen auch für den pflegerischen Bereich darlegt werden, wer welche Aufgaben hat und welche Berechtigungen diese Aufgaben mit sich bringen. Die Forderung zu einer dokumentierten Zuweisung von Rechtevergaben ergibt sich aus der datenschutzrechtlichen Anforderung, dass einem Betroffenen jederzeit Auskunft erteilt werden muss, wer wann unter welchen Umständen aus welchen Gründen auf welche Daten des Betroffenen Zugriff erhielt.

Kommentierung: -

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.

Rechtliche Einschätzung: Die Befugnis zu einem Zugriff auf personenbezogene oder personenbeziehbare Daten ergibt sich entsprechend den datenschutzrechtlichen Bestimmungen ausschließlich aus der Tatsache, dass es sich bei der zugreifenden Person um eine „berechtiget Person" handelt. Dies kann, muss aber nicht, aus einer zu diesem Zeitpunkt existierenden Dokumentation hervorgehen. Rechtlich unbedenklich ist auch der Datenzugriff einer berechtigten Person, bei welcher der Grund für die Berechtigung erst nach dem Zugriff dokumentiert wird.

Kommentierung: Häufig wird heute in Krankenhäusern mit einem „Mitarbeiter-Pool" gearbeitet, aus welchem im Bedarfsfall Mitarbeiter entnommen und auf den benötigten Arbeitsplätzen verteilt werden. Da Notwendigkeit der Zuteilung häufig auf Zuruf geschehen

muss – z. B. durch Krankheit eines Mitarbeiters, Notfälle – erfolgt eine Dokumentation häufig erst zu einem späteren Zeitpunkt.

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.

Rechtliche Einschätzung: Analog Punkt 12.

Kommentierung: Eine zeitliche Begrenzung des Zugriffs auf die eigenen Daten ist nicht nachvollziehbar und in den Systemen in der Regel auch technisch nicht umgesetzt. Zudem ist aus medizinischen Gründen dies nicht sinnvoll. Beispiel: Patient wird von der Station in den OP verlegt, kommt vom OP in den Aufwachraum und anschließend zurück auf die Station. Station und Aufwachraum brauchen Zugriff auf die Patientendaten, bevor der Patient zu ihnen kommt, insbesondere benötigt die Station Zugriff auf die „neuen" Daten aus OP und Aufwachraum, auch wenn der Patient nicht mehr bei ihnen liegt, um für die Wiederaufnahme alles vorbereiten zu können.

5.1.2.3 Zugriffe außerhalb der bettenführenden Fachabteilungen

19. Beschäftigte des Krankenhauses mit fachrichtungsübergreifender Funktion (z. B. Anästhesie, Physiotherapie, OP-Personal, Diagnostik [z. B. MRT], Pathologie) sollten den Daten-Zugriff entweder durch individuelle Zuweisung oder mit dem/durch den Patientenkontakt erhalten. Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren. Die Differenzierung kann typisiert z. B. nach beauftragter Funktionsstelle, angeforderter Leistung oder Krankheitsbild des Patienten erfolgen. Bei bestimmten Beschäftigten kann ein Zugriff auf sämtliche Daten der jeweiligen Patienten zulässig sein.

Rechtliche Einschätzung: Auch bei Personen, welche in fachübergreifenden Krankenhausbereichen arbeiten, gilt die datenschutzrechtliche Forderung, dass nur berechtigte Personen auf personenbezogene oder personenbeziehbare Daten zugreifen dürfen. Innerhalb einer Organisation daher gerade auch für diesen Bereich, der auf eine verhältnismäßig große Anzahl von Patienten zugreifen muss, festgelegt werden, wer welche Aufgaben zu erfüllen hat und welche Berechtigungen diese Aufgaben mit sich bringen.

Kommentierung: Ist innerhalb eines Krankenhausinformationssystems (im Sinne, wie es im Krankenhaus Verwendung findet, nicht wie die Definition in der OH KIS den Begriff beschreibt) mittels „Order Entry" abbildbar. Das Beauftragungskonzept greift allerdings in der Regel nicht über zwei unterschiedliche Informationssysteme hinweg, sodass in Subsysteme hierüber keine Rechte-Administration erfolgen kann.

20. Der Schreibdienst sollte so organisiert sein, dass der Zugriff durch individuelle Zuweisung zeitlich beschränkt erfolgt. Sofern dies nicht möglich ist, muss zumindest sichergestellt 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.

Rechtliche Einschätzung: Der Laborbereich ist eine der fachübergreifenden Funktionen, so gilt das zu Nr. 21 Gesagte. Hierbei spielt es keine Rolle, ob es sich um ein hauseigenes oder ein externes Labor handelt – entweder ist die zugreifende Person eine berechtigte Person oder nicht. Die Forderung, falls möglich eine Pseudonymisierung zu verwenden, ist eine Grundforderung der Datenschutzgesetze bzgl. Datenvermeidung und Datensparsamkeit, z. B. § 3a BDSG.

Kommentierung: Eine eindeutige Identifikation des Patienten ist immer zwingend erforderlich, da die Informationen einem Patienten unzweifelhaft zugeordnet werden müssen. Bestehen auch nur die geringsten Zweifel, ob die Untersuchungsergebnisse nicht zu dem betreffenden Patienten gehören, sind die Ergebnisse aus medizinischer Sicht zu verwerfen und die Untersuchung zu wiederholen. Bei Rückfragen, wie sie beispielsweise bei mikrobiologischen Untersuchungen die Regel sind, müssen sich Labormediziner und Anforderer über den Patienten unterhalten, klinische Werte wie beispielsweise Kreislaufverhalten, Temperatur und Daten des allgemeinen Wohlbefindens werden dabei ausgetauscht und fließen in den Befund des Labormediziners ein. Hierbei muss der Anforderer ggf. in diversen Informationssystemen Befunde des Patienten abfragen, wobei eine Suche nach informationssystemübergreifenden Pseudonymisierungsnummern nicht möglich ist. Daher ist aus Gründen der Patientensicherheit hier mit Klarnamen zu arbeiten.

5.1.3 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.

Rechtliche Einschätzung: Viele länderspezifischen Datenschutzregelungen erlauben explizit die Nutzung von Patientendaten außerhalb des Behandlungskontextes zu Forschung, Qualitätssicherung und/oder Lehre, sodass eine sich ausschließlich am Behandlungsfall orientierende Sperrung die gesetzlich erlaubte Nutzung einschränken würde. Die datenschutzrechtliche Pflicht unrichtige Daten zu korrigieren, zu löschen oder zu sperren (z. B. § 84 SGB X oder §§20, 35 BDSG) richtet sich danach, ob die Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. D. h. eine Sperrung ist zu fordern, wenn – je nach entsprechendem Landesrecht – die Daten weder für Abrechnungszwecke, noch für Lehre, Forschung oder Qualitätssicherung benötigt werden. Eine automatisierte Sperrung, welche sich nur am Fallabschluss orientiert, ist daher aus rechtlicher Sicht falsch.

Kommentierung: In vielen Fällen endet die Betreuung des Patienten nicht mit der stationären Entlassung. Vielmehr wird der Patient durch Abteilungen wie beispielsweise dem Sozialdienst der Krankenhäuser auch nach der Entlassung betreut. Zudem sollen die Daten entsprechend §291a Abs. 3 SGB V für eine elektronische Patientenakte zur Verfügung stehen, auf die mittels der elektronischen Gesundheitskarte zugegriffen werden kann; bei Sperrung der Daten ist die Intention des Gesetzgebers nicht umsetzbar.

Sofern der in der OH KIS angesprochene eingeschränkte Personenkreis identisch mit dem berechtigten Personenkreis ist, wobei die Berechtigung sich aus der Aufgabenstellung im jeweiligen Krankenhaus ergibt, ist diese Forderung gelebte Praxis in deutschen Krankenhäusern.

Allerdings ist hierbei anzumerken, dass auf gesperrte Daten generell nicht mehr zugegriffen werden kann. Vielmehr müssen die Daten „entsperrt“ und für den Gebrauch explizit wieder freigegeben werden.

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.

Rechtliche Einschätzung: Diese Forderung ist rechtlich nicht begründbar: Entweder handelt es sich um eine berechtigte Person, welche auf die Daten zugreift, oder nicht. Im ersteren Fall ist der Zugriff erlaubt, ohne dass zusätzliche Sicherungsmaßnahmen getroffen werden müssen, im letzteren Fall ist ein Zugriff auf die Daten verboten.

Kommentierung: Die derzeit in Deutschland eingesetzten Informationssysteme bieten nicht die Möglichkeit einer zeitlichen Befristung von Zugriffsrechten, vielmehr wird die Vergabe von Zugriffsrechten über Gruppenzugehörigkeit(en) (ärztlicher Bereich, Controlling, …) und Organisationszugehörigkeit(en) (Station 23, ambulante Abrechnung, …) realisiert.

Eine Buchstabenzugehörigkeit ist für das Casemanagement nicht sinnvoll; hier sollte betrachtet werden, wie viele Patienten ein Casemanager beispielsweise im OP betreut.

Weiterhin ist die Anzahl von Casemanagern im Krankenhaus begrenzt, gerade in kleineren oder mittleren Krankenhäusern gibt es meistens nur 1-2 Casemanager; auch unter diesem Gesichtspunkt ist die Aufteilung der Patienten nicht sinnvoll.

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

Rechtliche Einschätzung: Eine datenschutzrechtliche Forderung kann ohne gesetzliche Grundlage zwar gestellt werden, jedoch besteht keine Pflicht zur Umsetzung.

Kommentierung: Der Punkt sollte gestrichen werden.

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

Rechtliche Einschätzung: Eine gesetzliche Vorgabe bzgl. einer Sperrfrist oder der Einschränkung der Zugriffsrechte existiert nicht, wenngleich eine Zugriffsbeschränkung auf nicht mehr benötigte Daten aus dem Gesetz ableitbar ist. Die Zeitdauer stellt also letztlich eine Interpretation der Arbeitsgruppe der Aufsichtsbehörden dar, die richtig oder falsch sein kann - hier muss individuell entsprechend der landesrechtlichen Gegebenheiten andererseits entsprechend des Patientenwohles entschieden werden.

Kommentierung: Eine Vorgabe des Zeitraums von „unter einem Jahr“ durch die Aufsichtsbehörden ist hier abzulehnen, eine Sperrung kann zu einer Verschlechterung der Patientenbehandlung führen, sogar im Einzelfall das Leben eines Patienten bedrohen.

Die Nutzung von Daten vergangener Behandlungsprozesse liegt bei etwa 80 bis 90 Prozent im Zeitraum der vergangenen 3 Jahre, betrachtet man 5 Jahre, so werden immer noch etwa 60% angefordert. Daher kann nur das Krankenhaus entsprechend den klinischen Anforderungen entsprechend hier organisatorische Regeln treffen und einen Zeitraum festlegen.

Prüfungen durch den MDK-Dienst der Krankenkassen erfolgen auch nach über einem Jahr, ohne dass dies die Ausnahme darstellt. Eine Sperrung würde hier die Abläufe im Krankenhaus behindern.

Auch die nach §137a SGB V gesetzlich vorgeschriebene externe Qualitätssicherung erfordert zum Teil einen Zugriff über einen längeren Zeitraum, z. B. bei Herztransplantation sind es 5 Jahre.

Weiterhin ist vom Gesetzgeber die Nutzung von Daten zu Forschungszwecken ausdrücklich erlaubt, eine von den Aufsichtsbehörden geforderte Sperrung ist daher nicht nachvollziehbar.

Der Punkt sollte daher gestrichen werden.

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.

Rechtliche Einschätzung: Entspricht den gesetzlichen Regelungen.

Kommentierung: Ist gelebte Praxis.

5.1.3.1 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.

Rechtliche Einschätzung: Entsprechend des Prinzips der Datenvermeidung und Datensparsamkeit verlangen die bestehenden Datenschutzgesetze die Löschung von personenbezogenen oder personenbeziehbaren Daten sobald die Daten dies möglich ist (z. B. §84 SGB X, §§20, 35 BDSG).

Kommentierung: Entsprechend der haftungsrechtlichen Vorgaben (§823 BGB, §831 BGB) erlauben die schutzwürdigen Belange der Betroffenen (= Krankenhäuser, Behandler, usw.) erst nach 30 Jahren (§199 BGB) eine Vernichtung.

Weiterhin ist festzustellen, dass die meisten in deutschen Krankenhäusern eingesetzten Informationssysteme derzeit Patientendaten physikalisch nicht löschen können, sondern lediglich eine Darstellungs-/Sichtbeschränkung (= „Sperrung“) eingerichtet werden kann

5.1.3.2 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.

Rechtliche Einschätzung: Die rechtliche Grundlage für jeden Zugriff auf personenbezogene oder personenbeziehbare Daten bildet die Bedingung, dass nur berechtigte Personen Zugriff erhalten. Innerhalb einer Organisation muss daher auch für Funktionskräfte definiert werden, wer welche Aufgaben hat und welche Datenzugriffe diese Aufgaben mit sich bringen, z. B. durch ein Berechtigungskonzept.

Kommentierung: -

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.

Rechtliche Einschätzung: Die Berechtigung für den Zugriff auf personenbezogene oder personenbeziehbare Daten richtet sich ausschließlich nach den Aufgaben, die zu erfüllen sind. D. h., wenn die Daten zur Qualitätssicherung und/oder zum Controlling genutzt werden dürfen und den jeweiligen Personen die entsprechenden Aufgaben zugewiesen wurden, ist ihnen der Zugriff auf die benötigten Daten zu ermöglichen. Eine Einschränkung des Zugriffs erfolgt durch die Aufgabenstellung.

Kommentierung: Die interne medizinische Qualitätskontrolle findet in der Regel durch die erbringende funktionsbezogene Organisationseinheit statt, extern erfolgt die medizinische Qualitätssicherung einerseits im Rahmen der gesetzlichen Qualitätssicherung nach § 137a SGB V, andererseits durch privatwirtschaftlich-orientierte Benchmarking-Dienstleister und medizinische Fachgesellschaften. Bei der Qualitätssicherung nach § 137a SGB V sind die zu übermittelnden Daten vorgeschrieben, auf Grund der gesetzlichen Grundlage ist ein datenschutzrechtlicher Erlaubnistatbestand gegeben. Bei der freiwilligen externen Qualitätssicherung, an der viele Krankenhäuser teilnehmen, werden Patienten identifizierende Daten pseudonymisiert, sodass der Dienstleister Patienten nicht identifizieren kann. Die interne Nutzung von Patientendaten zur Qualitätssicherung ist in allen Bundesländern durch landesspezifische Regelungen erlaubt, Gleiches gilt für die Kirchengesetze, sodass in diesen gesetzlichen Regelungen beschrieben ist, wie die Daten genutzt werden dürfen, eine Pseudonymisierung oder Anonymisierung zur internen Verwendung bei der Qualitätssicherung ist in der Regel nicht vorgeschrieben.

Das betriebswirtschaftliche Controlling erfolgt durch krankenhausinterne Abteilungen der Krankenhausverwaltung statt und wird in der Regel mit aggregierten Daten gearbeitet, sodass eine Identifikation einzelner Patienten nur in Ausnahmefällen erfolgt.

Generell ist der Aussage, dass pseudonymisierte oder anonymisierte Daten wo immer möglich genutzt werden sollen, zuzustimmen.

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.

Rechtliche Einschätzung: Die datenschutzrechtlichen Bestimmungen schreiben eine Anonymisierung, wo nicht möglich eine Pseudonymisierung vor, wann immer Klardaten für den Verwendungszweck nicht zwingend erforderlich sind.

Kommentierung: -

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.

Rechtliche Einschätzung: Dem Prinzip der Datenvermeidung und Datensparsamkeit folgend verlangen die bestehenden Datenschutzgesetze bei der Nutzung von personenbezogenen oder personenbeziehbaren Daten eine Pseudonymisierung oder Anonymisierung, wann immer dies möglich ist (z. B. § 78b SGB X, §3a BDSG). Ist eine Pseudonymisierung oder Anonymisierung nicht möglich, so bieten die meisten Landesgesetze ausdrücklich die

Möglichkeit der Nutzung der Patientendaten zur Qualitätssicherung sowie zur Aus-, Fort- und Weiterbildung:

- §45 Abs. 3 Ziff. 4 LKHG BW: „Patientendaten dürfen auch gespeichert, verändert und genutzt werden … zur Ausbildung, Fortbildung und Weiterbildung von Ärzten und von Angehörigen anderer Berufe des Gesundheitswesens im Krankenhaus, … soweit diese Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen."
- §27 Abs. 4 BayKrG: „Die Krankenhausärzte dürfen Patientendaten nutzen, soweit dies im Rahmen des krankenhausärztlichen Behandlungsverhältnisses, zur Aus-, Fort- und Weiterbildung im Krankenhaus, zu Forschungszwecken im Krankenhaus oder im Forschungsinteresse des Krankenhauses erforderlich ist."
- §24 Abs. 4 Ziff. 2LKG Berlin: „Patientendaten dürfen erhoben, gespeichert, verändert und genutzt werden, soweit … dies zur Aus-, Fort- oder Weiterbildung erforderlich ist und nicht in vertretbarer Weise mit anonymisierten oder pseudonymisierten Daten erreicht werden kann …"
- §28 Abs. 2 Ziff. 3 BbgKHEG: „Patientendaten dürfen auch erhoben, gespeichert, verändert und genutzt werden … zur Ausbildung, Fortbildung und Weiterbildung von Ärztinnen und Ärzten und von Angehörigen anderer Berufe des Gesundheitswesens im Krankenhaus oder in einer vom Krankenhaus genutzten Ausbildungsstätte … soweit diese Zwecke nicht mit anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen."
- §2 Abs. 5 Ziff.4 BremKHDSG: „ Patientendaten dürfen auch gespeichert und genutzt werden … zur Aus-, Fort- und Weiterbildung von Angehörigen eines Heilberufs oder Gesundheitsfachberufs im Krankenhaus, … soweit diese Zwecke nicht mit pseudonymisierten oder anonymisierten Daten erreicht werden können und nicht überwiegende schutzwürdige Interessen des oder der Betroffenen entgegenstehen"
- §10 Abs. 1 Ziff. 8 HmbKHG: „In dem Krankenhaus dürfen Patientendaten genutzt werden, soweit dies erforderlich ist für ... die Aus-, Fort- und Weiterbildung der in dem Krankenhaus tätigen Mitarbeiterinnen und Mitarbeiter, soweit dies mit anonymisierten Daten nicht möglich ist und im Einzelfall überwiegende Interessen der Betroffenen nicht entgegenstehen"
- §34 Abs. 1 Ziff. 3 LKHG M-V: „Patientendaten dürfen für die Zwecke genutzt werden, für die sie nach § 33 Absatz 1 erhoben worden sind. Darüber hinaus dürfen sie nur genutzt werden, soweit dies erforderlich ist für … die im Krankenhaus durchgeführte Aus-, Fort- und Weiterbildung in ärztlichen oder anderen Fachberufen des Gesundheitswesens … soweit der Zweck nicht mit pseudonymisierten oder anonymisierten Daten erreicht werden kann"
- §11 Abs. 2 GDSG NRW: „Für die Qualitätssicherung und die Aus-, Fort- und Weiterbildung im Krankenhaus ist der Zugriff auf Patientendaten nur insoweit zulässig, als diese Zwecke nicht mit anonymisierten Daten erreicht werden können."
- §36 Abs. 2 Ziff. 2 LKG RP: „Patientendaten dürfen nur erhoben, gespeichert oder genutzt werden, soweit … dies zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung oder zur Ausbildung oder Fortbildung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten oder pseudonymisierten Daten erreicht werden kann"
- §13 Abs. 3 Saarländisches Krankenhausgesetz: „…Im Rahmen der Aus-, Weiter- und Fortbildung von Ärztinnen und Ärzten, Zahnärztinnen und Zahnärzten, Apothekerinnen und Apothekern, Psychologischen Psychotherapeutinnen und

Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeutinnen und -therapeuten und Angehörigen der Gesundheitsfachberufe ist zu gewährleisten, dass auf Patientendaten nur insoweit zurückgegriffen wird, als dies für die dem Berufsbild entsprechenden Funktionen erforderlich ist und diese Zwecke nicht mit anonymisierten Daten erreicht werden können …“

- §33 Abs. 2 Ziff. 2 SächsKHG: „Patientendaten dürfen nur erhoben werden, verarbeitet oder sonst genutzt werden, soweit … dies zur Ausbildung oder Fortbildung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist“
- § 27 Abs. 3 Ziff. 2 ThürKHG: „Patientendaten dürfen nur erhoben, gespeichert, verändert oder sonst genutzt werden, soweit … dies zur Ausbildung oder Fortbildung im Krankenhaus erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist“

Kommentierung: -

5.1.3.3 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.

Rechtliche Einschätzung: Es gibt kein Konzernprivileg im Datenschutz, dementsprechend sind die einzelnen Unternehmen eines Konzerns datenschutzrechtlich Fremde. Ein Austausch zwischen diesen Unternehmen kann nur auf Grund eines bestehenden Vertrages zur Auftragsdatenverarbeitung erfolgen, andernfalls erfolgt eine Übermittlung, die entweder die Zustimmung des Betroffenen oder eine gesetzliche Forderung zur Datenübermittlung benötigt.

Kommentierung: -

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.

Rechtliche Einschätzung: Es gibt kein Konzernprivileg im Datenschutz, dementsprechend sind die einzelnen Unternehmen eines Konzerns datenschutzrechtlich Fremde. Ein Austausch zwischen diesen Unternehmen kann nur auf Grund eines bestehenden Vertrages zur Auftragsdatenverarbeitung erfolgen, andernfalls erfolgt eine Übermittlung, die entweder die Zustimmung des Betroffenen oder eine gesetzliche Forderung zur Datenübermittlung benötigt.

Kommentierung: Generell ist die Aussage bzgl. konzernweiten und/oder mandantenübergreifendem Zugriff zuzustimmen. Einrichtungsübergreifende elektronische Fallakten basieren auf einer Einverständniserklärung des Betroffenen, sodass hier eine andere Konstellation vorliegt, die nichts mit der Konzernfragestellung zu tun hat.

Im Rahmen von MVZ sind im Krankenhaus häufig Krankenhausmitarbeiter für das MVZ zuständig, sodass Mitarbeiter/-innen, die sowohl für das MVZ als auch für das Krankenhaus tätig sind, beiden Mandanten zugehörig sind und Zugriff auf alle Mandanten, denen sie zugehörig sind, haben. Dies wurde aber an anderer Stelle der Orientierungshilfe KIS auch schon beschrieben (siehe nächster Punkt).

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

Rechtliche Einschätzung: Ein Mitarbeiter, welcher bei mehreren Mandanten tätig ist, hat die Berechtigung auf Daten, welche er für die Erfüllung seiner Aufgaben benötigt, zuzugreifen. Draus resultierend folgt, dass er natürlich einen mandantenübergreifenden Zugriff auf die Daten erhalten kann. Für Daten, welche nicht personenbezogen oder personenbeziehbar sind, findet das Datenschutzrecht keine Anwendung, dementsprechend dürfen die Daten für jedermann zugänglich sein.

Kommentierung: Siehe Punkt 32

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

Rechtliche Einschätzung: Datenschutzrecht ist nur auf personenbezogene Daten anwendbar. Daher können Datenschutz-Aufsichtsbehörde bzgl. der Verwendung von nicht personenbezogenen Datenbeständen zwar Wünsche äußern, jedoch keine Vorgaben geben.

Kommentierung: Sollte aus der OH KIS entfernt werden.

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.

Rechtliche Einschätzung: Verantwortlich für die Verfügbarkeit von bei Patienten erhobenen Daten ist immer der primäre Datenerheber, dementsprechend ist dieser auch für die gesetzeskonforme Archivierung der Daten verantwortlich. Eine Übernahme von übermittelten Daten (z. B. Röntgenbildern) ist daher aus rechtlicher Sicht nicht gefordert.

Kommentierung: Im Falle, dass der Behandler anhand seiner Dokumentation die Richtigkeit seiner Diagnose oder Therapie nachweisen muss, kann es von Nachteil sein, wenn die übermittelten Daten nicht zur Verfügung stehen (weil diese beispielsweise bei einer Praxisauflösung verschwanden). Daher ist die Übernahme dieser Dokumente ratsam, wenngleich nicht gesetzlich gefordert.

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.

Rechtliche Einschätzung: Hier ist die einzelne Vertragsgestaltung zu betrachten. Wenn es zwischen Krankenhaus und Patient zu keiner vertraglichen Beziehung kommt, dürfen

Mitarbeiter/-innen des Krankenhauses auch keinen Zugriff auf die Daten bekommen. Werden im Krankenhaus hingegen Dienstleistungen für diese Patienten erbracht (z. B. Labor, Küche), so dürfen die dort erhobenen Daten auch im Informationssystem des Krankenhauses gespeichert werden, denn es sind Leistungen, welche Mitarbeiter/-innen des Krankenhauses - ggf. konsiliarisch - erbrachten; das Krankenhaus ist hier „Herr der Daten". Dies ist analog zu im niedergelassenen Bereich erbrachten Leistungen zu sehen: Der Labormediziner speichert die von ihm erhobenen Daten in seinem System. Jede andere Forderung widerspricht den gesetzlichen Forderungen zur ärztlichen Dokumentationspflicht. Natürlich sind diese Daten zu schützen, dass nur berechtigte Personen Zugriff auf diese Daten erhalten dürfen.

Kommentierung: Auch ambulant in Nebentätigkeit behandelte Privatpatienten können Patienten des Krankenhauses sein, die Möglichkeit zur Privatliquidation wird heute nur noch selten an Chefärzte vergeben, vielmehr wird mit leistungsabhängigen Vergütungsanteilen beim Chefarztgehalt gearbeitet.

In dieser absoluten Aussage ist die Darstellung so nicht zutreffend. Der Punkt sollte entweder differenzierter dargestellt werden oder aus der OH KIS entfernt werden.

5.1.4 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.

Rechtliche Einschätzung: Entsprechend den datenschutzrechtlichen Anforderungen (z. B. §78a SGB X oder §9 BDSG) müssen Stellen, welche selbst oder im Auftrag Daten erheben, verarbeiten oder nutzen, technische und organisatorische Maßnahmen einschließlich der Dienstanweisungen treffen, die erforderlich sind, diese Daten zu schützen. Unter Beachtung des Prinzips der der Datenvermeidung und Datensparsamkeit müssen die Zugriffe auf personenbezogene oder personenbeziehbare Daten so stark wie möglich eingeschränkt werden. Eine direkte Aufteilung der Administration der eingesetzten Hardware/Server sowie der entsprechenden Anwendungen ist hieraus allerdings nicht ableitbar.

Kommentierung: Bedingt durch die Anzahl der in der EDV-Abteilung verfügbaren Mitarbeiter /-innen und der Anzahl der eingesetzten IT-Systeme ist eine Rollenteilung in Krankenhäusern in der Regel nicht realisierbar.

Insbesondere unter Berücksichtigung von erforderlichen Bereitschaftsdiensten der EDV-Abteilung ist die geforderte Rollenaufteilung personell von den meisten deutschen Krankenhäusern nicht umsetzbar.

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.

Rechtliche Einschätzung: Entsprechend den datenschutzrechtlichen Bestimmungen (z. B. §§19, 34 BDSG) muss eine Daten verarbeitende Stelle einem Betroffenen auf Antrag Auskunft darüber geben, welche Daten zu seiner Person gespeichert wurden, wem die Daten ggfs. weitergegeben wurden. Eine Weitergabe beinhaltet hierin nicht nur die Übermittlung an Dritte, sondern auch die Nutzung durch verschiedene Personen innerhalb der eigenen

Organisation/Institution. Daher sind Zugriffe auf Daten wie auch der Ausdruck oder der Export von Daten zu protokollieren. Eine revisionssichere Protokollierung ist hingegen nicht gefordert.

Da die Protokolldaten selbst personenbezogene Daten enthalten, sind die Protokolldaten entsprechend den datenschutzrechtlichen Anforderungen (z. B. §78a SGB X oder §9 BDSG) zu schützen. Eine Auswertung der Daten darf daher nur entsprechend vorher festgelegter Regeln erfolgen, die z. B. in einem Protokollierungskonzept festgehalten sein können.

Kommentierung: Ein Remotezugriff auf Arbeitsplatzrechner ist generell mitbestimmungspflichtig, da hierüber potenziell eine Mitarbeiterkontrolle möglich ist. D. h. hier muss eine Betriebsvereinbarung existieren, welche beschreibt, in welcher Form ein Remotezugriff ermöglicht werden darf. Diese Betriebsvereinbarung ist als datenschutzrechtliche Rechtsvorschrift anzusehen, die festlegt, ob Kenntnis und Einwilligung des Nutzers erforderlich ist oder nicht. In Anbetracht der datenschutzrechtlichen Aufgabenstellung des Personal- oder Betriebsrates ist jedoch davon auszugehen, dass eine Betriebsvereinbarung immer Kenntnis und Einwilligung des Nutzers zur Etablierung eines Remotezugriffs fordert.

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

Rechtliche Einschätzung: Eine Fernwartung ist datenschutzrechtlich prinzipiell eine Auftragsdatenverarbeitung (z. B. §80 SGB X, §11 BDSG). Bei einer Auftragsdatenverarbeitung darf der Auftragnehmer nur auf Weisung und entsprechend den Maßgaben des Auftraggebers tätig werden.

Kommentierung: Dies wird von vielen Herstellern verweigert unter dem Hinweis, dass unter diesen Umständen ein störungsfreier Betrieb des eingesetzten Informationssystems nicht möglich ist.

5.1.5 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.

Rechtliche Einschätzung: Krankenhaus-Mitarbeiter/innen, die nicht unmittelbar oder mittelbar (z. B. durch die Abrechnung) an der Behandlung beteiligt sind, gehören nicht zu den berechtigten Personen und dürfen keinen Zugriff auf Daten der betroffenen Person bekommen. Das Interesse von im Krankenhaus angestellten Personen Informationen über Patienten, die man persönlich kennt oder die Personen der öffentlichen Wahrnehmung (= „VIPs“, very important persons) sind, ist überdurchschnittlich hoch. Das Datenschutzniveau ist entsprechend den Anforderungen aus den Datenschutzgesetzen der potenziellen Gefährdung der Daten auszurichten. Gesundheitsdaten gehören per se zu den besonderen Arten, d. h. zu Daten, die besonders schützenswert sind. Den gesetzlichen Anforderungen folgend muss bei Daten von Mitarbeiter/innen oder VIPs der Schutz der Daten vor unberechtigten Zugriffen noch höher liegen als bei den „normalen“ Gesundheitsdaten.

Kommentierung: Bei den heute eingesetzten Informationssystemen ist der Schutz nur über organisatorische Regelungen realisierbar, technische Umsetzungen existieren Stand heute faktisch nicht. Insbesondere besteht die Schwierigkeit, mittels HL7 Pseudonyme an andere Informationssysteme zu kommunizieren, sodass in allen im Krankenhaus eingesetzten Informationssystemen einerseits das Pseudonym einheitlich genutzt wird, sodass die Patientengefährdung durch Einsatz eines Pseudonyms minimiert wird, andererseits die ggf. notwendigen Realdaten des Patienten für die privatärztliche Abrechnung zur Verfügung steht.

Letztlich ist der Schutz dieser Daten daher nur durch eine entsprechende Unternehmenskultur realisierbar.

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.

Rechtliche Einschätzung: siehe Punkt 41.

Kommentierung: siehe Punkt 41.

5.1.6 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.

Rechtliche Einschätzung: Gemäß den datenschutzrechtlichen Bestimmungen (z. B. §§19, 34 BDSG) muss eine Daten verarbeitende Stelle einem Betroffenen auf dessen Antrag hin Auskunft darüber geben, welche Daten zu seiner Person gespeichert wurden, wem die Daten ggfs. weitergegeben wurden. Wie das Krankenhaus als Daten verarbeitende Stelle diese Anforderung umsetzt, ist nicht geregelt. Letztlich kommt hier nur eine Protokollierung in Frage, sei es, dass Menschen die Tätigkeit anderer Menschen protokollieren, sei es, dass Computersysteme die Zugriffe auf personenbezogene oder personenbeziehbare Daten protokollieren. Eine revisionssichere Speicherung der Protokolldaten ist gesetzlich nicht gefordert.

Kommentierung: Eine revisionssichere Protokollierung ist in keinem Informationssystem integriert und wird von keinem Hersteller von Informationssystemen angeboten. Eine revisionssichere Protokollierung erfordert Write-once-Medien und damit sehr kostenintensiv, der Nutzwert wiederum vernachlässigbar, sodass die Kosten-Nutzen-Bewertung eine revisionssichere Protokollierung als nicht wünschenswert bewertet werden muss.

Es gibt keinen einheitlichen Aufbau von Protokolldateien, sodass jeder Hersteller eine eigene Ansicht bzgl. Inhalt und Aufbau der Protokolldaten hat; DIN EN ISO 27789 (Audit-Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2010) hat immer noch den Status einer Vor-Norm und wird faktisch von keinem Hersteller unterstützt.

Daraus resultiert aber auch, dass Art, Umfang und Dauer der Protokollierung häufig vom Hersteller des eingesetzten Informationssystems festgelegt werden. Die geforderte Protokollierung aller lesenden und schreibenden/ändernden Zugriffe kann häufig nur durch die Einstellung eines sogenannten „debug“-Levels erreicht werden, jedoch ist dies mit einem derartigen Performanceverlust verbunden, dass die Anwendung nicht mehr nutzbar ist.

Unter Berücksichtigung der Tatsache, dass die Daten eines Patienten in mehreren Informationssystemen im Krankenhaus gespeichert werden, die Logdateien nicht zentral zusammengeführt werden können, ist eine Übersichtsdarstellung und eine gemeinsame Auswertung über die verschiedenen Protokolldateien ist nicht möglich.

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

Rechtliche Einschätzung: Siege Punkt 43

Kommentierung: -

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.

Rechtliche Einschätzung: Eine Kontrolle der Datenzugriffe aus konkretem Anlass ist unmittelbar aus den Datenschutzgesetzen abzuleiten: Ein konkreter Anlass kann in diesem Zusammenhang nur sein, dass ein Hinweis auf einen unberechtigten Zugriff auf personenbezogene oder personenbeziehbare Daten existiert. Eine anlassunabhängige Kontrolle hingegen ist gesetzlich nicht gefordert; übertragen auf das Wirtschaftsleben würde diese Forderung bedeuten, dass Angestellte in einem Kaufhaus anlassunabhängig auf gestohlene Ware überprüft werden müssen - dies kann im Kaufhaus so geregelt werden, ist aber keine gesetzliche Forderung.

Kommentierung: Eine stichprobenweise anlassunabhängige (Plausibilitäts-)Kontrolle, welche auf eine Person zurückgeführt werden kann, ist auch zur potenziell eine Mitarbeiterkontrolle möglich und damit mitbestimmungspflichtig durch die Personalvertretung. Daher kann diese Kontrolle nicht vom Krankenhaus vorgegeben werden.

Eine Kontrolle aus gegebenem Anlass hingegen ist gesetzlich vorgegeben und muss daher immer erfolgen.

5.1.7 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.

Rechtliche Einschätzung: Leitet sich direkt aus den datenschutzrechtlichen Bestimmungen ab (z. B. §§19, 34 BDSG), ebenso aus §630g BGB.

Kommentierung: Eine Einschränkung auf Grund therapeutischer Bedenken ist möglich (§630g Abs. 1 BGB), dies muss allerdings dokumentiert werden.

Bei der Einsichtnahme durch den Patienten ist es ratsam, wenn eine ärztliche Person anwesend ist, welche dem Patienten spezielle medizinische Begrifflichkeiten oder Zusammenhänge erläutert.

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 Fachabteilung A).

Rechtliche Einschätzung: Leitet sich direkt aus den datenschutzrechtlichen Bestimmungen ab, z. B. §19 Abs. 1 oder §34 Abs. 1BDSG

> *(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über*
> *1.die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,*
> *2.die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und*
> *3.den Zweck der Speicherung.*

Kommentierung: -

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.

Rechtliche Einschätzung: Entsprechend §630g BGB kann ein Patient jederzeit Einsicht in die ihn betreffende Patientenakte verlangen, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder die Rechte Dritter entgegenstehen. Ob eine automatische Verarbeitung möglich ist oder nicht, kann nur anhand des eingesetzten IT-Systems entschieden werden: Ist hier bei einer automatisierten Weitergabe der Daten gewährleistet, sodass Daten Dritter nicht berührt werden (z. B. durch separate Speicherung, die vom Export ausgeschlossen werden kann) oder therapeutische Gründe beachtet werden (z. B. durch Nutzung von Annotationen, die beim Export entsprechend ausgewertet werden), ist auch ein automatisierter Vorgang mit den rechtlichen Anforderungen vereinbar.

Eine „Unkenntlichmachung“ innerhalb der Akte ist entsprechend §630g BGB nur aus therapeutischen oder „sonstigen erheblichen Gründen“ zulässig. Hier ist das Recht auf den Schutz von Informationen von Dritten in der Akte abzuwägen gegen das Recht auf Akteneinsicht entsprechend §630g BGB, wenn keine therapeutische Gründe als Grund für die Unkenntlichmachung vorhanden sind. Regelhaft wird bei dieser Interessenabwägung das Recht des Patienten auf Akteneinsicht wohl überwiegen, wenn man davon ausgeht, dass in einer Patientenakte Dritte nur im Rahmen der Behandlung des Patienten erwähnt werden.

Kommentierung: Für Krankenhäuser besteht die Ungewissheit, wann eine teilweise Unkenntlichmachung gerechtfertigt ist. Im Zweifelsfall wird, insbesondere unter Berücksichtigung des am 27. Februar 2013 in Kraft getretenen Patientenrechtegesetzes, das Krankenhaus dem Patienten vollen Zugriff auf die Akte geben.

5.2 Teil 2: „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“

5.2.1 Rechtliche Einschätzung

Grundsätzlich gibt es keine gesetzlichen Anforderungen an bestimmte technische Umsetzungen hinsichtlich der Forderung personenbezogene oder personenbeziehbare Daten vor unbefugtem Zugriff zu schützen. Patientendaten gehören als Daten, welche die Gesundheit einer Person widerspiegeln, zu den „Besondere Arten“ personenbezogener Daten, ebenso wie Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit oder Sexualleben. Dementsprechend existiert ein hoher Schutzbedarf für Gesundheitsdaten vor. Auch bei dem Schutz dieser Daten muss eine Abwägung der Verhältnismäßigkeit stattfinden: der Schutzbedarf der Gesundheitsdaten liegt auf der einen Waagschale, die für die Umsetzung eines bestimmten Schutzniveaus benötigten Ressourcen (Menschen, organisatorische Anweisungen, technische Hilfsgeräte, Finanzmittel, …) beschweren die zweite Waagschale. Hier muss ein ausgewogenes Verhältnis gefunden werden.

Bzgl. der Umsetzung gibt es Anforderungen, die beispielsweise in der Anlage zu §78a SGB X oder in der Anlage zu §9 BDSG dargestellt sind:

Anlage zu §78a SGB X	Anlage zu §9 BDSG
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),	1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),	2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),	3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),	4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

Anlage zu §78a SGB X	Anlage zu §9 BDSG
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),	5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),	6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),	7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.	8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Wie man sieht, werden hierbei keine expliziten technischen Umsetzungen der geforderten Schutzmaßnahmen genannt, lediglich ein Kommentar wird noch genannt:

> „Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

Daher können keine bundesweiten Anforderungen zu technischen Umsetzungen an den oben genannten Schutzzielen

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Gebot der Datentrennung

erhoben werden, die technischen Umsetzungen sind Aufgabe der datenverarbeitenden Stelle, also des den Patienten betreuenden/behandelnden Krankenhauses.

Einige Landesgesetze gehen jedoch weiter und fordern auch bestimmte Maßnahmen ein. §6 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen fordert unter bestimmten Umständen eine Protokollierung. In §6 Abs. 2 und Abs. 4 LDSG SW heißt es

> „(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(4) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldatenbestände sind ein Jahr zu speichern. Es ist sicherzustellen, dass die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind."

Auch das Landesdatenschutzgesetz Mecklenburg-Vorpommern fordert in §21 Abs. 5 und 6 sowie §22 Abs. 2 und 4 eine Protokollierung, in §22 Abs. 4 wird sogar die Aufbewahrungsdauer der Protokolldateien angegebenen.

In einzelnen Landesgesetzen wird also die Protokollierung ausdrücklich gefordert, aber such dort wird nicht die technische Umsetzung beschrieben. Theoretisch existieren neben technischen Umsetzungen natürlich auch organisatorische Möglichkeiten, z. B. durch die organisatorische Anordnung, dass jeder Datenerhebung, jeder Zugriff und jede Manipulation von Hand erfasst und in Schriftform festgehalten wird. Obschon dies die Anforderung einer Protokollierung erfüllen würde, ist realistischerweise diese Umsetzung nicht möglich, d. h. es kommt nur eine technische Umsetzung in Frage.

Daher kann grundsätzlich festgehalten werden, dass die technische Umsetzung des Schutzes personenbezogener oder personenbeziehbarer Daten ausschließlich bei der verantwortlichen Stelle liegt, die im zweiten Abschnitt der Orientierungshilfe genannten Punkte vielmehr als Beispiele für eine mögliche Umsetzung zu verstehen sind.

5.2.2 Kommentar zu den Abschnitten der technischen Anforderungen

5.2.2.1 Datenmodell

1.1 Jedes PAS, das in einem Umfeld eingesetzt wird, in dem es von mehreren rechtlich selbstständigen Leistungserbringern genutzt werden soll, muss mandantenfähig sein. (Teil I, Tz. 32).

Kommentierung: Dieser Forderung kann man nur zustimmen. Die von der Arbeitsgruppe der Datenschutzaufsichtsbehörden gewählte Bezeichnung „PAS" ist im Umfeld der medizinischen Informatik unüblich und der hier neu definierte Begriff kann zu Missverständnissen im Krankenhaus führen, was letztlich dem eigentlich angestrebten Ziel entgegensteht.

1.2 Verwenden verschiedene Krankenhäuser dieselbe Installation eines PAS, sind darin separate Mandanten einzurichten. Gleiches gilt für die Nutzung derselben Installation eines PAS durch ein Krankenhaus gemeinsam mit einer weiteren rechtlich selbständigen Stelle, insbesondere einem Medizinischen Versorgungszentrum (Teil I, Tz. 32).

Kommentierung: Auch dieser Forderung kann man nur zustimmen. Allerdings sollte vorgesehen werden, dass im Zuge einer gemeinsamen Patientenbehandlung ein gemeinsamer Zugriff auf benötigte Daten erfolgen kann. D. h.D. h., es sind auch mandantenübergreifende „Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen" zu fordern.

1.3 Datenbestände verschiedener Mandanten sind logisch oder physisch so zu trennen, dass Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Für weitere Komponenten eines KIS gilt, soweit relevant, diese Anforderung analog. (Teil I, Tz. 32)

Anforderungen an die Ausgestaltung mandantenfähiger Systeme sind im Übrigen in der Orientierungshilfe zur Mandantenfähigkeit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2012 in der jeweils aktuellen Fassung niedergelegt.

Kommentierung: Die hier beschriebenen Anforderungen bilden die Grundlagen für die Definition des Begriffes „mandantenfähig", daher sollte der Punkt gelöscht und der Begriff im Glossar entsprechend definiert werden.

1.4 Jedes Datenobjekt, das sich auf einen einzelnen Patienten bezieht, ist genau einer Fallakte, in Systemen mit mehreren Mandanten jede Fallakte genau einem Mandanten zuzuordnen (Teil I, Tz. 26, 32). Aus der Fallakte muss sich ergeben, welcher leitende Arzt oder welche Ärzte für die Behandlung zu gegebenem Zeitpunkt die Verantwortung tragen (Teil I, Tz. 9).

Kommentierung: Dieser Forderung ist uneingeschränkt richtig.

1.5 Für Datenobjekte, welche Patienten betreffen, die ambulant in Nebentätigkeit eines privat liquidierenden Arztes oder durch einen Belegarzt behandelt werden, muss das PAS die Möglichkeit bieten, Berechtigungen an diesen Status anknüpfen zu lassen, sofern für den behandelnden Arzt kein eigener Mandant eingerichtet wurde. (Teil I, Tz. 15, 37)

Kommentierung: Diese Forderung ist unklar. Entweder ist es eine privatärztliche Ambulanz, d. h. es existiert ein Behandlungsvertrag zwischen Chefarzt und Patient, nicht aber zwischen Krankenhaus und Patient. Dann ist eine Mandantentrennung erforderlich.

Oder es existiert ein Behandlungsvertrag zwischen Krankenhaus und Patient, wobei der Chefarzt nur einen (Teil-) Betrag privatärztlich abrechnet.

In beiden Fällen ist kein Grund für die geforderte Kennzeichnung gegeben und widerspricht damit der Forderung nach Datensparsamkeit. Zudem bietet die Kennzeichnung die potenzielle Möglichkeit gezielt nach diesen Patienten zu suchen, was dem Sinn der datenschutzrechtlichen Anforderung auch zuwiderläuft.

1.6 Die Fallakte eines Patienten muss Angaben aufnehmen können, welchen funktionsbezogenen Organisationseinheiten ein Patient derzeit zugeordnet ist. Flexible Mehrfachzuordnungen von Patienten zu Ärzten bzw. medizinischen Organisationseinheiten müssen möglich sein (Teil I, Tz. 9). Hierbei soll zwischen Behandlung und Konsil unterschieden werden können (Teil I, Tz. 10 und 13). Ziel ist es, umfassende generelle Zugriffsrechte zu vermeiden und stattdessen die im Rahmen der Behandlung erforderlichen Zugriffe abzubilden (Teil I, Tz. 7).

Kommentierung: Bitte die Anmerkungen zu den Teilziffern 7-11 sowie 16 zum ersten Teil der OH KIS beachten.

1.7 Für jedes patientenbezogene Datenobjekt muss sich unabhängig vom Inhaltstyp bestimmen lassen, wer es wann erstellt und wer es wann wie modifiziert hat (Eingabekontrolle / Revisionsfähigkeit). Werden z. B. aus Haftungsgründen Vidierungen (Freigabenachweise; Teil I, Tz. 10; vgl. auch Tz. 3.9) verwendet, muss sich für jedes hierfür vorgesehene Datum bzw. sachlich zusammenhängenden und gemeinsam zur Anzeige gebrachten Datensatz (Befund, Diagnose) erkennen lassen, ob er vidiert wurde und ggf. durch wen (Eingabekontrolle / Authentizität).

Kommentierung: Die OH KIS hat den Terminus „Datensatz nicht definiert, somit ist unklar, worauf die Forderung hinzielt. Im Vorfeld war des Öfteren vom „Datenobjekt" die Rede,

wobei der Begriff „Datenobjekt“ durch die Verwendung erklärt wurde. Sind hier mit dem Begriff „Datensatz“ wiederum die entsprechenden „Datenobjekte“ gemeint, so ist der Forderung unumstritten zuzustimmen.

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.

Die Betreiber sollen die Einteilung der Daten nach Kategorien nutzen, um den Zugriff von Beschäftigten auf die von ihnen benötigte Datengrundlage zu begrenzen. (Teil I, Tz. 1, 6, 7, 28)

Kommentierung: Datenschutzrechtlich ist diese Forderung nicht abzuleiten. Im medizinischen Umfeld entspricht die geforderte Trennung auch nicht den Aufgaben, d. h. für die Aufgabenerfüllung im Krankenhaus ist diese Forderung eher kontraproduktiv.

Zu den genannten Teilziffern aus dem ersten Teil der OH KIS bitte die dortigen Kommentierungen beachten.

1.9 Für jede Fallakte muss erkennbar sein, ob der Krankenhausaufenthalt beendet und ob der Behandlungsfall administrativ abgeschlossen ist (Teil I, Tz. 22). Fallakten müssen ein Sperrkennzeichen aufnehmen können oder das PAS eine Methode bereitstellen, mit welcher festgestellt werden kann, ob die Fallakte gesperrt ist. (Teil I, Tz. 24).

Kommentierung: Es ist unklar, was hier als „Krankenhausaufenthalt“ bzw. als „administrativer Abschluss des Behandlungsfalls“ definiert wird. Laut Glossar der OH KIS beinhaltet eine Fallakte alle Daten, die zu einem Behandlungsfall gehören. Ein Behandlungsfall wird als medizinischer Behandlungsfall betrachtet, nicht jedoch als Abrechnungsfall.

Ein medizinischer Fall kann nach seinem stationären Aufenthalt über Jahre in einem Krankenhaus ambulant nachbetreut werden, sodass sein „Krankenhausaufenthalt“ erst mit seinem Tod endet. Dementsprechend wird der Behandlungsfall administrativ erst mit dem Tod des Patienten abgeschlossen.

Evtl. ist hierunter aber auch zu verstehen, dass innerhalb eines Behandlungsfalls 1 oder mehrere stationäre Aufenthalte vorkommen können und zu jedem stationären Aufenthalt Aufnahme- und Entlassdatum sowie der Status der Abrechnung (administrativer Teil) festgehalten werden soll.

Der Punkt ist in der vorliegenden Form nicht eindeutig und sollte aus der OH KIS entfernt werden.

1.10 Das PAS muss die Möglichkeit bieten, einen Widerspruch des Patienten gegen die Hinzuziehung von Daten aus einer Vorbehandlung wirksam umzusetzen. (Teil I, Tz. 26).

Kommentierung: Dieser Forderung ist uneingeschränkt richtig.

1.11 Die Fallakte muss ein Kennzeichen aufnehmen können, das festhält, ob für den Patienten eine Auskunftssperre gilt (Teil I, Tz. 4).

Kommentierung: Dieser Forderung ist uneingeschränkt richtig.

1.12 Fallakten sollen bei Bedarf dahingehend gekennzeichnet werden können, dass der Patient Mitarbeiter des behandelnden Krankenhauses ist bzw. dass für die Fallakte ein besonderer Schutzbedarf besteht. Die Struktur des Rollen- und Berechtigungskonzepts soll es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können.

Das Merkmal darf ausschließlich zur Beschränkung der Zugriffsberechtigungen verwendet werden. (Teil I, Tz. 41)

Kommentierung: Wird in der Regel durch eine „VIP"-Regelung umgesetzt, jedoch gilt diese Kennzeichnung nur für das einzelne System. Es existiert keine Schnittstelle, die das Kennzeichen zwischen den Systemen austauscht, sodass in Subsystemen des Krankenhauses wie beispielsweise dem RIS keine Kennzeichnung des Schutzbedarfs vorhanden ist. Daher ist die Umsetzung des Schutzbedarfs technisch noch nicht gelöst.

Auch knüpfen nicht alle IT-Systeme im Krankenhaus, die das VIP-kennzeichen unterstützen, an diesem VIP-Kennzeichen die Möglichkeit einer dedizierten Rechtezuteilung.

1.13 Fallakten müssen bei Bedarf dahingehend gekennzeichnet werden können, dass sie bekannte Personen des öffentlichen Lebens, Personen, die einer besonderen Gefährdung oder einem erhöhten Interesse am Datenzugriff ausgesetzt sind, betreffen, oder dass für die Fallakte ein besonderer Schutzbedarf besteht. Die Struktur des Rollen- und Berechtigungskonzepts muss es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können (Teil I, Tz. 42).

Die Kennzeichen nach dieser Tz. und Tz. 1.12 können in einem Kennzeichen zusammengefasst werden.

Kommentierung: Siehe Kommentierung zu 1.12

1.14 Die unter Tz. 1.11 bis 1.13 genannten Merkmale sollen nicht dazu verwendet werden können, gezielt nach solchen Patienten zu suchen. Soweit eine solche Funktion unverzichtbar ist, ist sie an eine gesonderte funktionelle Rolle zu binden, die nur einem sehr eng begrenzten Personenkreis zugewiesen wird (Teil I, Tz. 7, 41, 42).

Kommentierung: -

1.15 Warnhinweise an nichtmedizinisches Personal sollen nur aus einer abschließend festgelegten Liste ausgewählt werden können und nicht als Freitextfelder gestaltet sein (Teil I, Tz. 3, 7).

Kommentierung: Diese Forderung kann nicht nachvollzogen werden. Bzgl. der Auswertbarkeit ist natürlich ein vorgegebener Wertevorrat zweckmäßig, aber die Frage besteht, warum diese Warnhinweise bzw. deren Verwendung aus datenschutzrechtlichen Gründen ausgewertet werden sollen.

1.16 Wenn Patientendaten für allgemeine Auswertungszwecke, die keinen Patientenbezug erfordern, in eine separate Architekturkomponente übernommen werden (z. B. in ein Data Warehouse), muss eine Anonymisierung erfolgen (Teil I, Tz. 30). Externe Komponenten für Auswertungen, die keinen Patientenbezug erfordern, dürfen nur dann auf den Datenbestand des PAS zugreifen, wenn eine Identifizierung von Patienten anhand der im Zugriff stehenden Daten ausgeschlossen ist (Teil I, Tz. 30, 31, Datensparsamkeit, Zweckbindung).

Kommentierung: Eine Pseudonymisierung ist hier vorzuziehen, da verschiedene Auswertezwecke zwar keine Patientenidentifikation benötigen, jedoch eine zum Teil fallübergreifende Zusammenführung von Daten erfordern.

Stand heute gibt es keine Festlegung, was unter dem Begriff „patientenidentifizierende Daten“ zu verstehen ist. Ohne eine inhaltliche Festlegung ist eine sinnvolle Anwendung der Begrifflichkeit nicht möglich.

Die Krebsregistergesetze der Länder beschreiben zwar die identifizierenden Merkmale, aber letztlich basieren diese Merkmale auf der Auswahl der Daten, welche das Krebsregister erheben darf/soll. Damit ist die Nutzung dieser Definition für ein Krankenhaus nur eingeschränkt möglich.

5.2.2.2 Systemfunktionen

2.1 Die Komponenten eines KIS sollen durch dokumentierte und standardisierte Schnittstellen verknüpft werden. Offene Standards sind zu präferieren (Transparenz).

Kommentierung: -

2.2 Ein PAS sollte es ermöglichen, bei der Übertragung von Daten von einer Komponente in eine andere Referenzen auf Datenobjekte statt der Datenobjekte selbst zu übertragen (Datensparsamkeit). Soweit eine redundante Datenhaltung unvermeidbar ist, müssen Zugriffsbeschränkungen und Löschungen in allen betroffenen Datenbeständen berücksichtigt werden (Teil I, Tz. 22, 27).

Kommentierung: Dass eine Anwendung aus Gründen der Datensparsamkeit Redundanzen vermeiden soll, ist nachvollziehbar. Hersteller von Informationssystemen versuchen auch aus Gründen der Performance in ihrer Datenbankanwendung eine Mehrfachspeicherung zu vermeiden. Die Mehrzahl der in Deutschland eingesetzten administrativen patientenführenden Systeme wurden jedoch nicht „nach einem Guss“ erstellt, sondern bestehen aus Informationssystemen verschiedener Hersteller, die nach und nach von einem Anbieter aufgekauft wurden. Hierdurch bedingt ist die geforderte Vermeidung einer Mehrfachspeicherung nicht erfüllbar, sofern bei einer Datensperrung bzw. -löschung alle Datenobjekte erfasst werden, ist hieran auch nichts auszusetzen; auch bei Informationssystemen muss eine Abwägung zwischen Datenschutzforderung und Umsetzung der Forderung erfolgen, eine vollständige Neuentwicklung der Systeme, welche der Forderung Rechnung tragen könnte, ist nach heutigen Gesichtspunkten nicht bezahlbar.

Solange nur ein System von einem Hersteller betroffen ist, kann eine Sperrung bzw. Löschung in dem System realisiert werden. Es existieren aber keine Schnittstellen, welche eine Sperrung bzw. Löschung von einem System zu einem anderen weiterreicht. Auch sind ggfs. unterschiedliche Aufbewahrungsfristen zu beachten: Ein Arztbrief muss evtl. nur 10 Jahre entsprechend der MBO-A aufbewahrt werden, dennoch können nicht alle Daten zum Patienten gelöscht werden, wenn beispielsweise Aufzeichnungen über die Anwendung von Blutprodukten zur Behandlung von Hämostasestörungen entsprechend § 14 Abs. 3 S. 1 TFG 30 Jahre aufbewahrt werden müssen. Da aber nicht alle Informationen in einem System gespeichert werden, kann ein System nicht entscheiden, wann Datenobjekte zu einem Patienten gelöscht werden können.

2.3 In das KIS sollte ein Single-Sign-On-Dienst integrierbar sein.

Kommentierung: Derzeit existiert kein Standard zur Übermittlung von Anmeldedaten, nur proprietäre Lösungen existieren auf dem Markt. So können Hersteller eines Systems keine übergreifende Lösung anbieten. Die Integration einer proprietären Lösung führt dazu, dass das

Informationssystem wiederum nicht mit Informationssystemen von Herstellern, die eine andere proprietäre Lösung integrierten, kommunizieren kann, ein Single-Sign-On wäre also ebenfalls nicht möglich.

2.4 In einem KIS, in dem Daten für mehrere Mandanten verarbeitet werden, muss auch beim Einsatz eigenständiger Subsysteme eine Parallelführung der Mandanten möglich sein. Dies bedeutet, dass Datenübermittlungen zwischen diesen Subsystemen mandantenbezogen vorgenommen werden. (Teil I, Tz. 32, 33).

Kommentierung: -

2.5: Dieser Punkt fehlt in der OH KIS, es geht nach 2.4 direkt mit 2.6 weiter

2.6 Merkmale nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 sollen in den verschiedenen Komponenten des KIS abgebildet werden können, sofern sie für deren Nutzung nicht offensichtlich irrelevant sind. (Bsp: Eine Tumordokumentation muss keine Angaben über eine Auskunftssperre i. S. v. Teil I, Tz. 4, enthalten.) Für die Merkmale nach Tz. 1.5 und 1.9 ist dies zwingend erforderlich (Teil I, Tz. 7, 37).

Kommentierung: -

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.

Kommentierung: Es existiert kein anerkannter Standard anhand dessen Berechtigungen zwischen verschiedenen Informationssystemen ausgetauscht werden können.

2.8 Das KIS muss über Funktionen verfügen, die es ermöglichen, insgesamt eine Übersicht der zu einem Patienten im KIS gespeicherten Daten zu erzeugen (Teil I, Tz. 43 bis 45 und 47). Diese Funktionen dienen der Datenschutzkontrolle sowie der Beantwortung von Auskunftsersuchen nach § 34 BDSG bzw. den entsprechenden landesrechtlichen Regelungen.

Kommentierung: Der Patient hat das Recht, alle über ihn gespeicherten Daten einzusehen, insofern ist die Forderung vollständig berechtigt. Da die Daten in einem Krankenhaus jedoch in verschiedenen Informationssystemen gespeichert werden, kann eine Übersicht nicht alle gespeicherten Daten anzeigen, höchstens die in dem jeweiligen Informationssystem, gespeicherten Daten. Aber auch diese Funktionalität wird nur von wenigen Informationssystemen bereitgestellt, hier existiert für viel Hersteller noch Optimierungspotenzial für ihre Systeme.

2.9 Es muss möglich sein, zeit- und ereignisgesteuert die Zugriffsberechtigungen für abgeschlossene (1.9) Fallakten oder Teile davon einzuschränken oder sie in ein Archiv auszulagern und sie dem operativen Zugriff zu entziehen. Das PAS muss es erlauben, einzelne Angaben zur zweifelsfreien Identifikation des Patienten festzulegen und ausschließlich diese für eine Suche unter den der Zugriffsbeschränkung unterliegenden Daten vorzuhalten. In den Ergebnissen einer derartigen Suche sollen zunächst ebenfalls nur die identifizierenden Angaben erscheinen. Soweit für bestimmte Aufgaben ein Zugriff auf einen derart identifizierten Behandlungsfall erforderlich ist, sollen die darüber hinausgehenden Daten erst nach dem unter Tz. 4.9 beschriebenen Verfahren bereitgestellt werden (Teil I, Tz. 22, 23).

Kommentierung: -

2.10 Das Krankenhaus muss einen Zeitraum von unter einem Jahr festlegen, nach dem der Zugriff auf abgeschlossene Fallakten gemäß Tz. 2.9 spätestens eingeschränkt wird (Teil I, Tz. 25).

Kommentierung: Eine Vorgabe des Zeitraums von „unter einem Jahr“ durch die Aufsichtsbehörden ist hier abzulehnen, eine Sperrung kann zu einer Verschlechterung der Patientenbehandlung führen, sogar im Einzelfall das Leben eines Patienten bedrohen.

Die Nutzung von Daten vergangener Behandlungsprozesse liegt bei etwa 80 bis 90 Prozent im Zeitraum der vergangenen 3 Jahre, betrachtet man 5 Jahre, so werden immer noch etwa 60% angefordert. Daher kann nur das Krankenhaus entsprechend den klinischen Anforderungen entsprechend hier organisatorische Regeln treffen und einen Zeitraum festlegen.

Prüfungen durch den MDK-Dienst der Krankenkassen erfolgen auch nach über einem Jahr, ohne dass dies die Ausnahme darstellt. Eine Sperrung würde hier die Abläufe im Krankenhaus behindern.

Auch die nach §137a SGB V gesetzlich vorgeschriebene externe Qualitätssicherung erfordert zum Teil einen Zugriff über einen längeren Zeitraum, z. B. bei Herztransplantation sind es 5 Jahre.

2.11 Das PAS muss über Funktionen verfügen, die zusammengenommen sicherstellen, dass nach Ablauf festgelegter Speicherfristen Behandlungsfälle gelöscht werden. Löschung bedeutet in diesem Zusammenhang eine physikalische Löschung. Eine Markierung als „gelöscht“, mit der Folge, dass die Daten lediglich nicht mehr angezeigt werden, ist nicht ausreichend (Teil I, Tz. 27).

Rechtliche Einschätzung: §3 Abs. 4 Ziffer 5 BDSG definiert Löschen als „das Unkenntlichmachen gespeicherter personenbezogener Daten“, die datenschutzrechtlichen Normen sprechen fordern ein Löschen auch ausdrücklich in Hinblick auf diese Definition. Daher ist nicht nachvollziehbar, auf Grund welcher rechtlichen Grundlage die Aufsichtsbehörden hier die Forderung nach einer physikalischen Löschung ableiten.

Kommentierung: Entsprechend den Begrifflichkeiten der Aufsichtsbehörden müsste diese Forderung eigentlich das KIS und nicht das PAS betreffen. Eine automatische Löschung ist abzulehnen, vielmehr ist eine explizite Freigabe zur Löschung notwendig: Im Zweifelsfall kann nur ein Mensch entscheiden, ob die Daten noch gebraucht werden. Sinnvoll ist aber eine Forderung nach einer Liste, in welcher Fälle angezeigt werden, bei denen die Speicherfrist abgelaufen und die vom Informationssystem zum Löschen angeboten werden, sodass ein menschlicher Mitarbeiter die Liste abarbeiten kann.

2.12 Lösch- und Auslagerungsaufträge müssen zwischen den Komponenten eines KIS propagiert werden können. Einzelne Datenbestände (für die womöglich gesonderte Aufbewahrungsfristen gelten) müssen vom Löschvorgang ausgenommen werden können (Teil I, Tz. 27).

Kommentierung: Eine Schnittstelle zwischen den Informationssystemen im Krankenhaus, mittels derer Lösch- und Auslagerungsaufträge kommuniziert werden, liegt in keinem anerkannten Standard vor, lediglich proprietäre Ansätze sind vorhanden.

Zudem müssen die Komponenten eines KIS bei einer Löschung nicht nur unterschiedliche Aufbewahrungsfristen, sondern auch den Kontext der Information beachten.

- Beispiel: Bei einer klinischen Studie werden Studiendaten separat von den Patientendaten aufbewahrt. Entsprechend der Arzneimittelprüfverordnung sind die Unterlangen solange aufzubewahren, solange das Arzneimittel zugelassen ist; die Patientenprüfliste 15 Jahre und die Unterlagen zur Anwendungsbeobachtung 10 Jahre. Beim Löschen von Patientendaten kann es nun passieren, dass die Richtigkeit anderer Daten der Studie nicht mehr gewährleistet ist, was ggfs. gesetzlichen Anforderungen widerspricht.

Haftungsrechtlich ist es ebenfalls problematisch einzelne Daten einer Patientenbehandlung herauszunehmen und zu vernichten, während andere Daten noch aufbewahrt werden (müssen). Die übrig gebliebenen Daten sind im Kontext ggfs. nicht mehr beurteilbar wie beispielsweise die Überprüfung der rechtfertigenden Indikation einer röntgendiagnostischen Maßnahme.

2.13 Das PAS muss über eine Funktion verfügen, die es ermöglicht, einzelne Datenfelder oder Behandlungsfälle zu löschen oder zu sperren (Teil I, Tz. 26).

Sperr- und Löschfunktionen dürfen nur zur Gewährung der Betroffenenrechte und nur von besonders befugten Mitarbeitern eingesetzt werden.

Kommentierung: Auch ist hier statt des Begriffes „PAS“ der Begriff „KIS“ im Sinne der Definition der Aufsichtsbehörden zu wählen. Des weiteren existiert keine standardisierte Schnittstelle zwischen den im Krankenhaus eingesetzten Informationssystemen, mittels derer Lösch- bzw. Sperrinformationen zwischen den Systemen ausgetauscht werden können. Existiert die Löschung bzw. Sperrung jedoch nur in einem System, so stellt sich die Frage, wie dieses System mit Meldungen zum gelöschten/gesperrten Datenobjekt aus anderen Systemen umgehen soll.

2.14 Jede Komponente eines PAS soll eine effiziente Replikation des Datenbestandes in ein Testsystem ermöglichen, das zur Fehlersuche und zum Test von Maßnahmen der Fehlerbehebung dient. Im Zuge der Replikation des Datenbestandes soll es möglich sein, eine Pseudonymisierung etwa durch Ersatz der Identifikationsdaten mit Dummy-Daten durchzuführen. (Datensparsamkeit; Zugriffskontrolle / Vertraulichkeit)

Kommentierung: Diese sicherlich sinnvolle Forderung ist leider nur von den wenigsten Herstellern in einsatzfähiger Form umgesetzt. Auch hier sollte die Forderung auf den Begriff „KIS“ ausgeweitet werden, eine Beschränkung auf PAS erscheint – wenn die Forderung schon erhoben wird - nicht sinnvoll.

2.15 In das KIS muss ein Pseudonymisierungsdienst eingebunden werden, der verwendungszweckspezifisch temporäre Patientenkennzeichen oder Pseudonyme auf der Basis der gespeicherten Identitätsdaten generiert und verwaltet (Teil I, Tz. 30, 31).

Kommentierung: Diese insbesondere auch unter den Gesichtspunkten der Forschung, Qualitätssicherung wie auch der Aus-, Fort- und Weiterbildung sinnvolle Forderung ist leider Stand heute bei den Herstellern nicht verfügbar.

Weiterhin sollte ein Export ausgewählter Patientendaten (entsprechend Konfiguration) unter Nutzung der Pseudonymisierungsfunktion möglich sein. Z. B. zur Übermittlung der Daten an Krankheitsregister.

5.2.2.2.1 Verschlüsselung

2.16 Werden im Zuge des Datenaustauschs zwischen verschiedenen Komponenten des KIS Dienstleistungen externer Provider in Anspruch genommen, muss für eine Transportverschlüsselung gesorgt werden. Die Schlüssel dürfen sich nur in alleiniger Kontrolle des Krankenhauses befinden.

Kommentierung: -

2.17 Speichermedien, welche Daten des KIS aufnehmen und nicht fest installiert sind, müssen verschlüsselt werden (durch Datenträger- oder Dateisystemverschlüsselung). Gleiches gilt für Speichermedien, die sich nicht im alleinigen Zugriff des Krankenhauses befinden. Andere Speichermedien sollen verschlüsselt werden. Die Verschlüsselung mobiler Datenmedien dient dem Schutz der Daten bei Verlust des Mediums, die Verschlüsselung fest installierter Medien dient der Minderung des Risikos unberechtigten Zugriffs auf den Datenträger, auch nach seiner Aussonderung.

Kommentierung: Die Anforderungen aus Satz 1 entsprechen den gesetzlichen Gegebenheiten. Bzgl. Satz 2 gilt dies jedoch nicht uneingeschränkt, vielmehr muss der rechtliche Rahmen des Zugriffs beachtet werden. Findet eine Auftragsdatenverarbeitung statt, so ist eine Verschlüsselung eines Speichermediums, auf welches neben dem Krankenhaus auch der Auftragsdatenverarbeiter Zugriff hat, rechtlich nicht gefordert (obgleich natürlich die Verschlüsselung an sich zum Schutz der Patientendaten unbestritten sinnvoll ist).

Mobile Datenträger, auf denen Patientendaten gespeichert werden müssen verschlüsselt werden, entsprechende datenschutzrechtliche Anforderungen lassen sich aus den Gesetzen ableiten. Hier ist nicht verständlich, warum die Arbeitsgruppe der Aufsichtsbehörden dies nicht fordert, sondern lediglich schreibt „Andere Speichermedien sollen verschlüsselt werden".

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.

Kommentierung: -

2.19 Zur Wahrung der Vertraulichkeit, Integrität und Authentizität der Daten in Protokollen, die zu Zwecken der Datenschutzkontrolle geführt werden, sollten geeignete kryptografische Verfahren nach dem Stand der Technik eingesetzt werden können. Beispiele hierfür sind hybride Verschlüsselungsverfahren, bei denen der Entschlüsselungsschlüssel in einer geschützten Hardware gespeichert wird, und die Nutzung eines Zeitstempeldienstes.

Kommentierung: -

5.2.2.3 Anwendungsfunktionen

3.1 Die Verarbeitungskontexte sollen derart konfigurierbar sein, dass ein Verarbeitungskontext lediglich die Transaktionen zur Verfügung stellt, die zur Ausübung der funktionellen Rollen erforderlich ist, denen er zugeordnet ist. (Teil I, Tz. 7)

Kommentierung: Die Anforderung kann durch ein Berechtigungskonzept abgebildet werden.

3.2 Das Krankenhaus muss in seinem Berechtigungskonzept für jeden Verarbeitungskontext festlegen, welche Funktionen für die Ausübung der mit ihm verbundenen funktionellen Rollen erforderlich sind und bereitgestellt werden. (Teil I, Tz. 1, 7, 28).

Kommentierung: -

3.3 Die Nutzer müssen jederzeit im Rahmen ihrer Aufgaben die Möglichkeit haben, den der anstehenden Arbeitsaufgabe zugeordneten Verarbeitungskontext auszuwählen. Bei einem Wechsel der Verarbeitungskontexte kann ein Bezug der im alten Verarbeitungskontext geöffneten Fallakte (Fall-ID) an den neuen Verarbeitungskontext übergeben werden, sofern gewährleistet ist, dass diese Fallakte im neuen Verarbeitungskontext nur geöffnet wird, soweit sie im Ergebnis einer im neuen Verarbeitungskontext zulässigen Suche oder Abfrage gefunden werden kann.

Kommentierung: Der Anforderung kann eigentlich nur zugestimmt werden, allerdings ist im täglichen Alltag ein Wechsel des Verarbeitungskontextes meist mit einer Neuanmeldung am Informationssystem verbunden, d. h. der „neue“ Benutzer (genauer: das jetzt genutzte Benutzerkonto) hat andere Rollen und damit verbunden andere Rechte, daher wird in einem anderen Kontext gearbeitet. Daher wäre eine „arbeitsfreundlichere“ Implementierung seitens der Hersteller wünschenswert.

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 Patienten in Abhängigkeit von Verarbeitungskontext und Zugriffsberechtigungen nach dem Prinzip der Erforderlichkeit anzupassen. Menüpunkte und Bildschirmmasken, sowie Ergebnislisten müssen in dieser Hinsicht flexibel gestaltet werden können. Das gleiche gilt für allgemeine Übersichtslisten (wie z. B. Stationslisten). (Teil I, Tz. 1, 7, 28)

Kommentierung: Auch diesem Punkt muss man zustimmen, jedoch auch hier sollte „KIS“ statt „PAS“ verwendet werden. Die Abbildung der Anforderungen bzgl. der Konfigurationsmöglichkeiten ist in den heute verfügbaren Informationssystemen kaum anzutreffen, obgleich einige Hersteller an Umsetzungen arbeiten.

3.5 Das PAS muss über eine Funktion verfügen, mit der im Rahmen der Aufnahme eines Patienten eine Kurzübersicht mit den zugelassenen Daten zurückliegender Behandlungsfälle erzeugt werden kann (Teil I, Tz. 1 - 3).

Kommentierung: Der Anforderung ist zuzustimmen, allerdings fehlt seitens der Hersteller mitunter noch die technische Umsetzung.

3.6 Das PAS soll über eine Funktion verfügen, mit der Akten abgeschlossener Behandlungsfälle eines Patienten (oder Teile hiervon) der aktuellen Fallakte mit der Auswirkung zugeordnet werden können, dass die Aufbewahrungsfrist der aktuellen Fallakte sich auf die zugeordneten Daten erstreckt. (Teil I, Tz. 27)

Kommentierung: Der Anforderung ist zuzustimmen, allerdings fehlt seitens der Hersteller mitunter noch die technische Umsetzung.

3.7 Für Sonderzugriffe muss systemseitig die Eingabe einer Begründung gefordert werden können, ggf. auch im Nachhinein. (vgl. Tz. 4.9). (Teil I, Tz. 14)

Kommentierung: Die Forderung steht in Bezug zu der vormals gebrauchten Begrifflichkeit „PAS“. Auch hier sollte der Begriff „KIS“ statt „PAS“ zur Anwendung kommen, ansonsten ist dem Punkt zuzustimmen.

3.8 Ein PAS soll eine Funktion zur Freigabe (Vidierung) eingegebener Daten bieten. Der Umfang der hierbei relevanten Datenkategorien muss konfigurierbar sein. (Authentizität)

Kommentierung: Auch hier sollte der Begriff „KIS“ statt „PAS“ verwendet werden, ansonsten ist dem Punkt zuzustimmen.

3.9 Ein PAS soll es erlauben, Nutzer zur Freigabe bzw. Bestätigung bestimmter Datenobjekte aufzufordern (vgl. Tz. 4.9). (Authentizität)

Kommentierung: Auch hier sollte der Begriff „KIS“ statt „PAS“ verwendet werden, ansonsten ist dem Punkt zuzustimmen.

3.10 Ein Datenexport soll über Schnittstellen möglich sein, die in Abhängigkeit von Verarbeitungszweck und -kontext definiert wurden. (Teil I, Tz. 30, 31)

Kommentierung: Die Forderung steht in Bezug zu der vormals gebrauchten Begrifflichkeit „PAS“. Auch hier sollte der Begriff „KIS“ statt „PAS“ zur Anwendung kommen, ansonsten ist dem Punkt zuzustimmen.

3.11 Es soll möglich sein, bei einem Datenexport automatisiert die Identitätsdaten eines Patienten durch ein Pseudonym zu ersetzen (Teil I, Tz. 30, 31).

Kommentierung: Der Anforderung ist zuzustimmen, allerdings fehlt seitens der Hersteller mitunter noch die technische Umsetzung.

3.12 Die Speicherorte medizinischer Daten sowie die Möglichkeit zum Export von Daten sollen durch Konfiguration beschränkbar sein, z. B. soll die lokale Datenspeicherung auf Arbeitsplatzrechnern unterbunden werden können. (Zugriffs- und Weitergabekontrolle / Vertraulichkeit)

Kommentierung: Dies ist in vielen im Krankenhaus eingesetzten Informationssystemen abgebildet.

5.2.2.4 Rollen- und Berechtigungskonzept

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

- *Zuordnung des Patienten zu Organisationseinheiten (Teil I, Tz. 9)*
- *Dokumentierte ärztliche Anweisungen (u.a. Leistungsanforderungen) und explizite Delegierungen (Teil I, Tz. 10, 13)*
- *Datenkategorie (Teil I, Tz. 1, 7, 28)*
- *Kennzeichen nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 (s. dort)*
- *Ersteller des Datenobjekts / eines Datenobjekts in der Patientenakte (Teil I, Tz. 12, 15, 22)*
- *Impliziter oder explizit erklärter Verarbeitungskontext (Teil I, Tz. 1, 7, 28)*
- *Das Berechtigungskonzept muss es ferner erlauben, Rechte zeitabhängig zu vergeben, und sollte es ermöglichen, Rechte in Abhängigkeit von*

- *dem Ort des Zugreifenden, insbesondere im Verhältnis zum Patienten (Teil I, Tz. 7, 12),*
- *einem Dienst- oder Bereitschaftsplan (Teil I, Tz. 12 und 17), und*
- *dem hinterlegten Behandlungspfad des Patienten (Teil I, Tz. 10)*

zu erteilen (4.8)

Kommentierung: Auch hier sollte eher von „KIS“ als vom „PAS“ gesprochen werden. Die meisten heute im Krankenhaus eingesetzten Informationssysteme bieten diese Funktionalitäten nicht an, insbesondere existiert kein Austausch der Berechtigungen zwischen den eingesetzten Systemen.

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

- *Ärztliche Beschäftigte (Teil I, Tz. 7, 9ff.)*
- *Nicht-ärztliches medizinisches Fachpersonal (z. B. Pflegekräfte) (Teil I, Tz. 16ff., 19ff.)*
- *Verwaltungskräfte (Teil I, Tz. 28 bis 30)*
- *Ausbildungskräfte (Teil I, Tz. 31)*
- *Externe Kräfte (Teil I, Tz. 15, 32)*
- *Technische Administration (Teil I, Tz. 38ff.)*

Kommentierung: Wie die Auswahl der Kategorien von der Arbeitsgruppe der Datenschutzaufsichtsbehörden zustande kommt, ist unklar; eine rechtliche Vorgabe hierzu gibt es nicht. Der grundlegenden Forderung bzgl. der Unterscheidung verschiedener Benutzerkategorien und damit verbundenen Rollen bzw. Berechtigungen muss inhaltlich jedoch zugestimmt werden. Die Auswahl der Kategorien muss jedoch vom jeweiligen Krankenhaus vorgegeben werden: Ein 200-Betten-Krankenhaus hat bzgl. Granularität der Kategorien andere Anforderung als Universitätsklinika.

4.3 Zur Definition von Rechten muss es möglich sein, Organisationseinheiten flexibel und überlappend zu definieren (Teil I, Tz. 9, 10). Beispielsweise überlappen sich die OE „psychiatrischer Konsiliardienst“ und „psychiatrische Fachabteilung“, wo beide bestehen, sodass es möglich sein muss, einen Facharzt beiden OE zuzuordnen.

Kommentierung: Diese sinnvolle Forderung kann Stand heute leider noch nicht in allen Informationssystemen umgesetzt werden. Wo es möglich ist, sollte die Funktionalität genutzt werden.

4.4 Das Krankenhaus muss die Umsetzung des Berechtigungskonzepts dergestalt dokumentieren, dass die Erforderlichkeit des Umfangs erteilter Rechte nachvollzogen werden kann. (Transparenz, Datenschutzkontrolle)

Kommentierung: Der Anforderung ist zuzustimmen.

4.5 Das PAS muss über eine Funktion verfügen, die es erlaubt, die für einzelne Benutzer vergebenen Berechtigungen in einer Übersicht darzustellen. (Transparenz, Datenschutzkontrolle)

Kommentierung: Auch hier sollte statt „PAS“ der Begriff „KIS“ genutzt werden. Der Anforderung ist zuzustimmen, jedoch ist die technische Umsetzung bei vielen im Krankenhaus eingesetzten Informationssystemen noch unzureichend.

4.6 Das PAS muss über eine Funktion verfügen, die es erlaubt, für bestimmte Berechtigungen in einer Übersicht die Benutzer darzustellen, die über diese Berechtigung verfügen. Insbesondere muss es für ein gegebenes Datenobjekt effizient bestimmt werden können, welche Mitarbeiter darauf schreibend oder lesend zugreifen können. (Transparenz, Datenschutzkontrolle)

Kommentierung: Auch hier sollte statt „PAS“ der Begriff „KIS“ genutzt werden. Der Anforderung ist zuzustimmen, jedoch ist die technische Umsetzung bei vielen im Krankenhaus eingesetzten Informationssystemen noch unzureichend.

4.7 Das PAS muss über Funktionen verfügen, mit denen ein Behandlungsfall

a) zur Mitbehandlung einer weiteren funktionsbezogenen Organisationseinheit oder einzelnen Behandlern dauerhaft, befristet oder auftragsbezogen zugewiesen werden kann (Teil I, Tz. 10, 12, 13) und
b) im Rahmen einer Verlegung einer anderen funktionsbezogenen Organisationseinheit dauerhaft zugewiesen werden kann.

Das Rollen- und Berechtigungskonzept muss anknüpfend an die Zuweisung den Zugriff der anderen Organisationseinheit ermöglichen. (Teil I, Tz. 11 und 18)

Kommentierung: Auch hier sollte statt „PAS“ der Begriff „KIS“ genutzt werden. Der Anforderung ist zuzustimmen, jedoch ist die technische Umsetzung bzgl. der geforderten automatischen Anpassung bei vielen im Krankenhaus eingesetzten Informationssystemen nicht vorhanden.

4.8 Rollen und Berechtigungen z. B. für Bereitschaftsdienste oder Vertretungen müssen einer Benutzerkennung einfach und flexibel zugeordnet werden können, um etwaigen wechselnden Aufgabenstellungen Rechnung zu tragen. Hierbei sollten auch zeitliche Muster und Dienstpläne abgebildet werden können (z. B. Rolle Bereitschaftsdienst am Wochenende oder für einen bestimmten Zeitraum; Teil I, Tz. 12 und 17).

Kommentierung: Diese sinnvolle Forderung kann Stand heute leider noch nicht in allen Informationssystemen umgesetzt werden. Wo es möglich ist, sollte die Funktionalität genutzt werden.

4.9 Das Berechtigungskonzept muss die Möglichkeit bieten, Zugriffsbeschränkungen situationsbezogen aufzuheben bzw. Zugriffsrechte zu erweitern. Dies gilt insbesondere für Sonderzugriffe (Teil I, Tz. 14), Zugriffe im Rahmen retrospektiver Prüfungen oder Zugriffe im Rahmen der Qualitätssicherung (Teil I, Tz. 22 und 29).

Dabei ist ein zweistufiges Verfahren vorzusehen, bei dem vor der Ausführung einer Transaktion in einem ersten Schritt

- *eine Begründung für die Erforderlichkeit der Transaktion eingegeben wird (vgl. Tz. 3.9) oder*
- *die Bestätigung durch einen zweiten berechtigten Mitarbeiter erfolgen muss (4-Augen-Prinzip)*

und erst im zweiten Schritt der Zugriff eröffnet wird. Dabei soll die Möglichkeit bestehen, den Zugriff zeitlich zu beschränken (z. B. auf 24 Std.)

Auf die Erweiterung der Zugriffsrechte und die Protokollierung des Zugriffs (vgl. 7.11) soll zuvor hingewiesen werden.

Kommentierung: Ein Krankenhaus muss dem Patienten auf Nachfrage mitteilen können, wer Zugriff auf die Daten erhielt. Hierbei muss im Einzelfall der Zugreifende nachweisen, dass er

berechtigt war. Dies kann durch den Behandlungszusammenhang erfolgen, also z. B. ärztliches oder pflegerisches personal auf der Station, auf welcher der Patient untergebracht war. Erfolgt der Zugriff aber außerhalb derartiger Strukturen, fällt es dem Zugreifenden nach einem gewissen Zeitraum wahrscheinlich schwer, den Grund für den Datenzugriff zu benennen; kann die zugreifende Person den Grund für den Zugriff nicht darlegen, kann u.U. zivilrechtlich gegen die zugreifende Person seitens des Patienten vorgegangen werden. Daher dient die Forderung eigentlich dem Schutz des im Krankenhaus eingesetzten Personals.

Speziell die Forderung, dass erst nach erfolgter Begründung eine Freigabe der Daten erfolgen kann, steht im Widerspruch zum Handlungsgeschehen im Krankenhaus: in einer Notfallsituation kommt es mitunter auf jede Sekunde an, daher muss hier ein Zugriff sofort erfolgen. Eine Forderung bzgl. einer zeitlich nachgelagerten Begründung für den Zugriff ist demgegenüber natürlich statthaft.

Die Umsetzung erzeugt jedoch deutlichen Aufwand und wird daher i.d.R. vom Krankenhauspersonal abgelehnt.

4.10 Zur Authentisierung von Mitarbeitern gegenüber dem KIS sollte ein Zwei-Faktor-Verfahren eingesetzt werden. Das KIS sollte es ermöglichen, Datenzugriffe an die Anwesenheit eines bestimmten Benutzers, nachgewiesen z. B. durch Präsenz eines maschinenlesbaren Mitarbeiterausweises, eines RFID-Tags oder eines vergleichbaren Tokens zu knüpfen (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit).

Kommentierung: Das Krankenhaus muss gewährleisten, dass nur berechtigte Personen auf personenbezogene oder personenbeziehbare Daten zugreifen. Dies kann durch ein Zwei-Faktor-Verfahren geschehen, kann aber auch durch die Kombination Benutzername/Passwort erfolgen.

4.11 Es muss sichergestellt sein, dass es keinem Nutzer möglich ist, durch eine Verknüpfung von Rechten oder einen Wechsel des Verarbeitungskontexts sich über die Summe der ihm erteilten Rechte hinaus zusätzliche Rechte anzueignen. Insbesondere müssen die Zugriffsbeschränkungen auch bei dem Zugriff auf Daten über Patientenlisten und die Suchfunktion beachtet werden (Zugriffskontrolle / Vertraulichkeit).

Kommentierung: -

4.12 Der Umfang der Zugriffsberechtigungen eines Benutzers darf sich allein aus der Gesamtheit der ihm zugeordneten strukturellen und funktionellen Rollen ergeben. (Zugriffskontrolle / Vertraulichkeit)

Kommentierung: Der Anforderung ist zuzustimmen.

4.13 Das Krankenhaus muss strukturelle Rollen so zuschneiden, dass sie sich unabhängig von der konkreten Person an der Stellung in der Krankenhausorganisation ausrichten. Es muss funktionelle Rollen so zuschneiden, dass sie sich unabhängig von einer konkreten Person an einer abgrenzbaren fachlichen Aufgabe und den hiermit in Zusammenhang stehenden Tätigkeiten orientieren (Transparenz).

Kommentierung: Der Anforderung ist zuzustimmen, auch wenn die Formulierung den Inhalt der Anforderung nicht leicht erschließen lässt. Strukturelle Rollen sollen sich grundsätzlich an der Stellung im Krankenhaus, funktionelle Rollen an den Aufgaben orientieren.

4.14 Die Einrichtung von gemeinsam zu nutzenden Benutzerkennungen muss grundsätzlich vermieden werden. In Betracht kommen solche Benutzerkennungen ausnahmsweise z. B. für den Verarbeitungskontext „Pflegekräfte in Stationszimmern" oder im OP-Bereich. Für den Bereich der Administration sind sie unzulässig. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)

Kommentierung: Der Anforderung ist zuzustimmen.

4.15 Die Benutzerverwaltung muss über eine Möglichkeit verfügen, Benutzer dauerhaft oder für einen bestimmten Zeitraum zu sperren bzw. Zugriffsrechte zu entziehen (Zugriffskontrolle / Vertraulichkeit).

Kommentierung: Der Anforderung ist zuzustimmen.

4.16 Die Benutzerverwaltung sollte über eine Schnittstelle zur Personalverwaltung verfügen, die es insbesondere ermöglicht, die Zugriffsberechtigungen von Mitarbeitern automatisiert zu deaktivieren.

Kommentierung: Der Anforderung ist zuzustimmen.

4.17 Die Benutzerverwaltung sollte eine Auswertung danach ermöglichen, für welche Benutzer für einen festgelegten Zeitraum keine Anmeldung mehr erfolgt ist.

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.

Kommentierung: Der Anforderung ist bis auf den letzten Satz zuzustimmen. Missbräuchlich heißt, jemand verwendet etwas entgegen dem erlaubten Zweck. D. h. in diesem Fall jemand darf die Daten für einen bestimmten Zweck nutzen, verwendet sie aber entgegen den erteilten Anweisungen missbräuchlich. Dem kann durch ein Konzept nicht begegnet werden, auch organisatorische Maßnahmen sind bei Missbrauchsfällen nur beschränkt hilfreich.

4.18 Das PAS muss es ermöglichen, dass für die Verfahrensbetreuung und die Berechtigungsverwaltung unterschiedliche Personen mit separaten Benutzerkennungen festgelegt werden können (Teil I, Tz. 38 und Teil II, Tz. 8.1). Die Berechtigungsverwaltung muss bei Bedarf auf mehrere Personen verteilt werden können.

Kommentierung: Der Anforderung ist zuzustimmen.

5.2.2.5 Datenpräsentation

5.1 Das PAS muss es ermöglichen, in Abhängigkeit vom Verarbeitungskontext in den Bildschirmmasken die Anzeige von Teilen der Patientenakte mit oder ohne Darstellung der Identitätsdaten des Patienten zu konfigurieren, z. B. für Schulungszwecke. (Teil I, Tz. 30 und 31).

Kommentierung: Auch hier wäre es zutreffender, von „KIS" zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

5.2 Das PAS soll es ermöglichen, in Abhängigkeit vom Verarbeitungskontext Teile der Patientenakte mit Pseudonymen oder temporären Patientenkennzeichen, die die Identitätsdaten des Patienten ersetzen, darzustellen (Teil I, Tz. 30 und 31).

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

5.3 Das PAS sollte die Oberflächen verschiedener Verarbeitungskontexte klar voneinander optisch (z. B. farblich) unterscheiden, um es den Nutzern zu erleichtern, die ggf. je nach Verarbeitungskontext variierenden Berechtigungen nachzuvollziehen. Dies gilt insbesondere für die Oberfläche des Sonderzugriffs. Hier dient die optische Hervorhebung zusätzlich dazu, den Nutzer aufzufordern, den Zugriff mit erweiterten Rechten nur solange zu nutzen, wie dies erforderlich ist.

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

5.4 Es muss die Möglichkeit bestehen die Angaben nach 1.4 bis 1.6, 1.9 und 1.11 bis 1.13 in Bildschirmmasken zu integrieren, um, wo es erforderlich oder hilfreich ist, den Nutzern einen Hinweis zu geben, im Kontext welchen Mandantens sie operieren, ob für den Patienten eine Auskunftssperre eingerichtet wurde, welcher bzw. welchen Organisationseinheiten ein Patient zugeordnet ist bzw. war, ob die Behandlung und/oder Abrechnung bereits abgeschlossen oder der Patient einer besonders schutzwürdigen Gruppe angehört.

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

5.2.2.6 Systemzugang

6.1 Ein PAS muss einen schnellen Benutzerwechsel ermöglichen (vgl. Tz. 3.2).

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen.

Die Definition von „schnell“ wird von Anwendern und Herstellern unterschiedlich interpretiert, sodass hier im täglichen Betrieb vermutlich keine Übereinstimmung bzgl. der Nutzbarkeit der Funktionalität erzielt wird.

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.

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

6.3 An Arbeitsplätzen des PAS muss eine Bildschirmsperre oder ein Auto-Logout auf Betriebssystem- oder Anwendungsebene eingerichtet sein. Die Zeitdauer bis zur Aktivierung von Sperre oder Logout muss sich an dem Risiko unberechtigten Zugangs zu dem Arbeitsplatz ausrichten. (Zugriffskontrolle / Vertraulichkeit)

Kommentierung: Der Anforderung ist zuzustimmen.

6.4 Wird beim Login (als einer der beiden einzusetzenden Faktoren) ein Token eingesetzt, so sollte nach Login eines Nutzers das Entfernen des Tokens zur Sperrung, das Einführen des Tokens zur Freischaltung der Arbeitsstation, insbesondere nach einem Auto-Logout genutzt werden können.

Kommentierung: Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

6.5 Ein PAS sollte die Speicherung und Wiederaufnahme einer Sitzung an einem anderen Arbeitsplatz innerhalb des Krankenhauses ermöglichen. Zur Wiederaufnahme einer Sitzung an einem anderen Arbeitsplatz muss die gleiche Authentisierung wie bei der Initialisierung der Sitzung vorgesehen werden. (Zugriffs- und Eingabekontrolle / Vertraulichkeit und Revisionsfähigkeit)

Kommentierung: Auch hier wäre es zutreffender, von „KIS“ zu sprechen. Der Anforderung selbst ist zuzustimmen, jedoch wird von vielen Informationssystemen hierzu keine Funktionalität angeboten.

5.2.2.7 Protokollierung

5.2.2.7.1 Allgemeines

Mitunter verlangen Patienten von einem Krankenhaus Namen des sie behandelnden ärztlichen und pflegerischen Personals im Rahmen eines Zivilrechtstreites. Grundlage ist hierfür das datenschutzrechtlich vorhandene Recht auf Auskunft an den betroffenen bzgl.

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Hierbei ist ein Empfänger im Sinne von Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten in der Weise, dass

a) die Daten an den Empfänger weitergegeben werden oder
b) der Empfänger zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

Damit hat der Patient ein Anrecht darauf zu erfahren, welche Person oder welche Personengruppe eine Einsichtnahme in seine Daten möglich war, welche Person oder welche Personengruppe in seine Daten Einsicht nahm.

Der Krankenhausträger ist hier entsprechend der derzeitigen Rechtsprechung zu folgenden Auskünften verpflichtet (OLG Düsseldorf, 30.01.2003 - 8 U 62/02, OLG Frankfurt, 23.09.2004 - 8 U 67/04):

- Namen und Anschrift der ihn operierenden Ärzte, Anschrift ist hier die klinikseitige Anschrift der Operateure
- Ausnahme: der Arzt ist nicht mehr an der Klinik tätig. In diesem Fall kann dem Patienten die Privatanschrift des Arztes genannt werden.

Nicht verpflichtet ist der Krankenhausträger zur Weitergabe folgender Daten an den Patienten:

- Sämtlicher den Patienten behandelnder Ärzte (BGH, 31.10.2000 - VI ZR 198/99)

- Privatanschriften der Operateure.

Um diesen Auskunftsanspruch zu genügen, ist eine Protokollierung der Zugriffe unumgänglich. Unter Protokollierung beim Betrieb von Informations- und Kommunikations-Systemen ist in datenschutzrechtlichem Sinne die Erstellung von manuellen oder automatisierten Aufzeichnungen

- über die tatsächlichen Veränderungen an Hardware-Komponenten (z. B. vorübergehendes Entfernen von Sicherheitselementen) und an der Software (Betriebssystem, systemnahe Software, Anwendungssoftware) sowie
- über Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten

zu verstehen. Elemente einer Protokollierung sind:

- Art der Aktivität,
- Zeitpunkt der Aktivität bzw. des Ereignisses,
- ausführende Person,
- eventuell von der ausführenden Person eingegebene Daten.

Die in der Orientierungshilfe Krankenhausinformationssysteme von den Datenschutzaufsichtsbehörden aufgestellten Forderungen zur Protokollierung gehen teilweise über diesen Auskunftsanspruch hinaus. Hierbei wird als Argument das Urteil des Europäischen Gerichtshof für Menschenrechte aus dem Jahr 2008 (ECHR Application No. 20511/03[8]) im Zusammenhang mit Zugriffen auf medizinische Daten eines Krankenhausinformationssystems herangezogen. In Absatz 44 der Urteilsbegründung[8] wird dargestellt, dass medizinische Daten zu schützen sind, sei es durch ein entsprechendes Berechtigungskonzept oder durch entsprechende Protokollierung („... control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file ..."). Das finnische Krankenhaus löschte alle Protokolldaten, ein am Behandlungskontext orientiertes Berechtigungskonzept existierte ebenfalls nicht. Daher urteilte der ECHR, dass das Krankenhaus seiner Verpflichtung zum Schutz der Daten vor unberechtigten Zugriffen nur unzureichend nachkam. Das Urteil fordert keine Protokollierung aller Zugriffe, sondern es verlangt den Schutz der medizinischen Daten eines Patienten. Natürlich müssen unberechtigte Zugriffe protokolliert werden, so gut es technisch möglich ist (ein „Hacker" hat evtl. die Möglichkeit die Protokolldaten zu manipulieren), da hier das Berechtigungskonzept keine Auskunft geben kann, wer auf die Daten des betroffenen Patienten unberechtigterweise zugriff.

In der Orientierungshilfe fehlt allerdings die Forderung, dass auch der Zugriff auf die Protokollierungsdateien protokolliert werden muss. Weiterhin muss die Protokollierung für die Mitarbeiter transparent erfolgen, d. h. es muss im Handbuch des Systems nachzulesen sein, was protokolliert und was - je nach Konfiguration seitens des Betreibers - evtl. protokolliert wird.

5.2.2.7.2 Punkte der Orientierungshilfe

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.

[8] Right to Privacy Requires Strict Controls, Safeguards and Protection of Health Information. I v Finland. ECHR 20511/03 [Online] 2008 [Zitiert 2014-04-16] Verfügbar unter http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf

Kommentierung: Hierhin gehört auch die Anforderung an die Hersteller, dass die Protokollierungs-Funktionalität die Nutzbarkeit des Systems nicht beeinträchtigen kann.

Weiterhin ist eine Definition der „relevanten Ereignisse“ wünschenswert. Es ist nicht zielführend, wenn jedes Krankenhaus für sich die relevanten Ereignisse definieren (muss), die Prüfung auf Protokollierung dieser Ereignisse im Bundesland hingegen einheitlich durch die Aufsichtsbehörde erfolgt.

7.2 Art und Umfang der Protokollierung, die Verfahrensweisen zur Speicherung, die getroffenen Schutzmaßnahmen, das Vorgehen zur Auswertung der Protokolle sowie die Aufbewahrungsdauer der Protokolldaten sind in einem Protokollierungs- und Auswertungskonzept festzulegen, unter Einbeziehung des behördlichen/betrieblichen Datenschutzbeauftragten und der Mitarbeitervertretung. Die Verpflichtung zur Protokollierung und Auswertung der Protokolle (s. Tz. 7.3ff.) kann jedoch nicht durch Betriebsvereinbarung ausgeschlossen werden.

Kommentierung: Der Anforderung ist bis auf den letzten Satz zuzustimmen. Die Protokollierung ist in dem einen oder anderen Bundesland in der landesdatenschutzgesetzlichen Regelung enthalten (z. B. Berlin), jedoch in den meisten Bundesländern nicht gesetzlich gefordert. Daher besteht bundesweit gesehen keine direkte gesetzliche Pflicht zur Erstellung von Protokolldateien.

Eine Betriebsvereinbarung kann jedoch eine Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG sein, d. h. eine Betriebsvereinbarung kann als Zulässigkeitsvoraussetzungen der Datenverarbeitung einen Tatbestand gegenüber dem Bundesdatenschutzgesetz abweichend regeln und insbesondere auch zugunsten der Arbeitnehmer weiter einschränken (vgl. BAG vom 20.12.1995 AZ 7 ABR 8/95 sowie BAG vom 27.05.1986 AZ I ABR 48/84). Dies ergibt sich bereits aus dem arbeitsrechtlichen Günstigkeitsprinzip. (Wobei die Betriebsvereinbarung BDSG- und grundrechtskonform sein muss.)

Daher kann in der OH KIS nicht prinzipiell eine entsprechende Regelung in einer Betriebsvereinbarung ausschließen.

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.

Kommentierung: Der Begriff „erforderliches Maß“ der Orientierungshilfe ist nicht näher definiert. Daher muss dieser Begriff im Sinne des datenschutzrechtlichen Gebotes der Datenvermeidung und Datensparsamkeit interpretiert werden, d. h. es muss so wenig wie nötig protokolliert werden.

Damit muss das „erforderliche Maß“ vom jeweiligen Krankenhaus individuell definiert werden. Ein Krankenhaus mit einem ausgefeilten Rechtekonzept, welches die Zugriffsmöglichkeiten des Einzelnen einschränkt, muss weniger protokollieren als ein Krankenhaus, welches die Zugriffsrechte sehr weit fasst und einen umfassenden Zugriff auf Patientendaten erlaubt.

Allerdings sollte der Grad der Protokollierung vom jeweiligen Krankenhaus schriftlich in einem Protokollierungskonzept festgehalten werden.

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.

Kommentierung: Siehe Kommentierung Teil 1, Punkt 43.

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.

Kommentierung: Der Anforderung ist zuzustimmen.

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.

Kommentierung: D. h. hier sollen Ereignisse protokolliert werden, die sich nicht direkt in der Datenbank selbst abspielen. Dies ist ohne weitere Vorgaben seitens der Aufsichtsbehörden nicht umsetzbar, da nicht klar wird, was gefordert wird. Auch wäre eine Begründung sowie Beispiele wünschenswert, welche erläutern, warum eine Protokollierung auf Datenbankebene nicht ausreichend ist.

7.7 Vorgesehene Protokollierungen dürfen nicht umgangen werden können.

Kommentierung: Der Anforderung ist zuzustimmen.

7.8 Eine nachträgliche Veränderung von Protokolldaten darf nicht möglich sein.

Kommentierung: Der Anforderung ist zuzustimmen.

7.9 Protokolle sollen so konfigurierbar sein, dass sie keine medizinischen Daten enthalten. (Datensparsamkeit / Vertraulichkeit)

Kommentierung: Der Anforderung ist zuzustimmen.

7.10 Neben der Anmeldung am Verfahren (Login/Logout) müssen die Zugriffe der Nutzer mit zumindest folgenden Angaben protokolliert werden:

- *Zeitpunkt des Zugriffs,*
- *Kennung des jeweiligen Benutzers,*
- *Kennung der jeweiligen Arbeitsstation,*
- *aufgerufene Transaktion (Anzeige/Abfragefunktion, Reportname, Maskenbezeichnung),*
- *betroffene Patienten/Behandlungsfälle*
- *Bei Aufruf einer Suchfunktion muss das Protokoll mindestens enthalten:*
- *verwendete Such- bzw. Abfragekriterien (z. B. Patientennummer, Fallnummer, Name, Geburtsdatum, Wohnort, Diagnose etc.),*

- *Angaben zum Ergebnis der Abfrage (z. B. Zahl der Trefferfälle, Fallnummern, Kennung der angezeigten Bildschirmmaske),*
- *etwaige Folgeaktionen bzw. Navigationsschritte (z. B. Auswahl eines Datensatzes aus einer Trefferliste, Aufruf Bildschirmmasken, Druck, Datenexport).*

Kommentierung: Auch hier kann die Orientierungshilfe nur beispielhaften Charakter zeigen, da die Inhalte einer Protokollierung in dieser Detailtiefe rechtlich nicht fixiert sind.

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.

Kommentierung: Da die Begründung in der Anwendung gespeichert und so jederzeit nachgelesen werden kann, ist eine Speicherung in der Protokollierungsdatei aus folgenden Gründen nicht zu fordern:

1. Eine Speicherung steigert die Unübersichtlichkeit der Protokollierungsdatei.
2. Das Prinzip der Datensparsamkeit gilt auch für Datenschützer.
3. In einer Begründung kann neben dem Patientennamen auch eine medizinische Begründung zum Patienten stehen (was häufig auch der Fall sein wird), sodass hier der Datenschützer Einblick in medizinische Daten zum Patienten bekommt.

Beispiel: „Herr Müller-Lüdenscheid erlitt eine schwere allergische Reaktion auf den Genuss des flambierten Hähnchenschenkels. Daher Notfallzugriff erforderlich."

7.12 Aufgrund der Reichweite technisch-administrativer Funktionen bedarf deren Nutzung einer besonderen Kontrolle. Die Protokollierung von Zugriffen im Rahmen der System- und Verfahrensadministration muss alle Zugriffe erfassen, die Auswirkungen auf Art oder Umfang der Verarbeitung personenbezogener Daten haben (Teil I, Tz. 39)

Kommentierung: Der Anforderung ist zuzustimmen.

7.13 Es muss nachvollziehbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt wurden, insbesondere welche Zugriffe auf personenbezogene Daten hierbei erfolgt sind (Teil I, Tz. 40).

Kommentierung: Der Anforderung ist zuzustimmen.

7.14 Hierzu müssen die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art des Zugriffs) in entsprechenden Protokolldateien festgehalten werden (Teil I, Tz. 40).

Kommentierung: Der Anforderung ist zuzustimmen. Weiterhin muss festgehalten werden, auf welche personenbezogenen Daten ggfs. zugegriffen wurde.

7.15 Die Löschung von Daten ist Teil ändernder Zugriffe. Sie sollte lediglich insoweit protokolliert werden, als für einzelne Daten der Zeitpunkt der Löschung und der jeweilige Benutzer, für Datensätze zusätzlich die jeweilige Fallnummer oder vergleichbare Identifikationsmerkmale festgehalten werden.

Kommentierung: Der Anforderung ist zuzustimmen.

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.

Kommentierung: Der Anforderung ist zuzustimmen.

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.

Kommentierung: Da die Protokolldatei ebenfalls personenbezogene Daten enthält, muss auch der Export der Protokolldatei(en) protokolliert sowie eine Begründung für den Export festgehalten werden.

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.

Kommentierung: Der Anforderung ist zuzustimmen. Der Einblick in die Protokolldaten selbst muss natürlich auch protokolliert werden.

7.19 Zugriffe auf Protokolldaten sollten nur nach dem Vier-Augen-Prinzip und unter Beteiligung eines Datenschutzverantwortlichen erfolgen.

Kommentierung: Der Anforderung ist zuzustimmen.

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.

Kommentierung: Dieser Punkt enthält einerseits einen Generalverdacht gegenüber den in einem Krankenhaus Beschäftigten, welcher mit einem rechtstaatlichen Ansatz nicht vereinbar ist, andererseits widerspricht er den datenschutzrechtlichen Grundgedanken der informationellen Selbstbestimmung, der auch für die im Krankenhaus Beschäftigten gilt.

Eine anlassunabhängige Kontrolle muss immer mit der Mitarbeitervertretung abgesprochen werden und kann ohne rechtliche Grundlage nicht von einer Arbeitsgruppe der Datenschutzaufsichtsbehörden beschlossen werden. Regelmäßige stichprobenartige Auswertungen bedürfen einer Betriebsvereinbarung, welche aber bzgl. des Protokollierungskonzeptes an sich schon notwendig ist; idealerweise wird der hier angesprochene Punkt zwischen Krankenhausleitung und Personalvertretung von vornherein mit geregelt.

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.

Kommentierung: Je nach Größe der Protokolldateien ist eine 12monatige Speicherung nicht durchführbar, eine rechtliche Grundlage hierfür gibt es nicht. Das Krankenhaus muss dem Auskunftsanspruch des Patienten genügen. Kann das Krankenhaus dem Auskunftsanspruch nicht genügen, haftet das Krankenhaus ggfs. hierfür gegenüber dem Patienten. Dieses

Haftungsrisiko und die daraus resultierende Speicherdauer muss das Krankenhaus selbst abschätzen.

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.

Hier ist unklar, was die Arbeitsgruppe als „Verfahrensdokumentation" ansieht. Wahrscheinlich ist hier eine Verfahrensdokumentation im Sinne der GoBS[9] gemeint, die entsprechenden Dokumentationspflichten leiten sich dann aus dem Handelsgesetzbuches (HGB) und der Abgabenordnung (AO) ab.

Die im HGB geforderten aufzubewahrenden Unterlagen sowie deren Aufbewahrungsfristen sind §257 HGB aufgelistet, laut HGB gehören Protokolldaten nicht zu den aufbewahrungspflichtigen Unterlagen. Die aufbewahrungspflichtigen Unterlagen sowie die Aufbewahrungsfristen sind in § 147 AO dargestellt, Protokolldaten sind nach den Vorgaben der AO nicht aufbewahrungspflichtig.

Protokolldaten müssen nicht nach den Regeln der GoBS aufbewahrt werden. Damit dieser Punkt verständlich wird, muss die Arbeitsgruppe definieren, was sie unter Verfahrensdokumentation versteht und auf Grund welcher rechtlichen Grundlage welche Aufbewahrungsfristen gelten.

Alternativ kann der Punkt natürlich auch gestrichen werden: gelten für Protokolldaten gesetzliche Aufbewahrungsdauer, so liegt für die Datenerhebung und -speicherung eine gesetzliche Grundlage vor, ohne dass die Arbeitsgruppe hier Stellung zu beziehen muss. Liegt keine gesetzliche Grundlage vor, kann die Arbeitsgruppe auch keine gesetzliche Grundlage schaffen, d. h. eine Aufbewahrung von Protokolldaten bedürfte der Einwilligung des Betroffenen - zu welchem Zweck sollte dieser Aufwand betrieben werden?

5.2.2.8 Technischer Betrieb, Administration

8.1 Die Administration eines KIS muss in die Bereiche

- *technische Administration der genutzten IT-Komponenten,*
- *Anwendungsadministration / Verfahrensbetreuung und*
- *Berechtigungsverwaltung*

getrennt werden. Die jeweiligen Rollen sollten unterschiedlichen Personen zugewiesen werden (Teil I, Tz. 38).

Kommentierung: Der Anforderung selbst ist zuzustimmen. Allerdings ist die Aufteilung auf drei Personen in den meisten Krankenhäusern aus personellen Gründen nicht umsetzbar, oftmals werden die beschriebenen Funktionen in Personalunion ausgeübt.

8.2 Das Krankenhaus muss sicherstellen, dass eine Fernwartung nur im Einzelfall und mit Einverständnis des Krankenhauses erfolgen kann (Teil I, Tz. 40).

Kommentierung: Siehe Kommentar zu Punkt 40 Teil 1.

[9] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS). [Online] 1995 [Zitiert 2014-04-06] Verfügbar unter http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Betriebspruefung/BMF_Schreiben_Allgemeines/009.html

8.3 Das KIS bzw. die zugrundeliegenden IT-Systeme sollen hierzu über entsprechende Benachrichtigungs- oder Freischaltmöglichkeiten verfügen (Teil I, Tz. 40).

Kommentierung: Der Anforderung ist zuzustimmen.

8.4 Der Wartungsvorgang muss durch das Krankenhaus jederzeit abgebrochen werden können, wobei die Systemkonsistenz zu wahren ist. (Weitergabekontrolle / Vertraulichkeit)

Kommentierung: Bei einem Abbruch des Wartungsvorgangs durch das Krankenhaus muss die Systemintegrität gewährleistet sein, ansonsten muss während der Änderung von systemkritischen Funktionen des Informationssystems der Abbruch von Wartungseingriffen verhindert werden.

Siehe auch Kommentar zu Punkt 40 Teil 1.

8.5 Fernwartungsarbeiten müssen über verschlüsselte Verbindungen und unter separaten, über Identifikations- und Authentisierungsmechanismen geschützten Benutzerkennungen durchgeführt werden. Deren Zugriffsmöglichkeiten müssen auf das für die Durchführung der Wartungsarbeiten erforderliche Maß beschränkt sein; erforderlichenfalls sind mehrere Wartungskennungen einzurichten (Teil I, Tz. 40).

Kommentierung: Der Anforderung ist zuzustimmen.

8.6 Die Übernahme neuer Softwareversionen sollte grundsätzlich nicht im Rahmen der Fernwartung erfolgen. Soweit im Einzelfall unvermeidlich, ist dies zu dokumentieren und die Integrität der übernommenen Software durch geeignete Maßnahmen sicherzustellen (Teil I, Tz.40).

Kommentierung: Hierbei handelt es sich nicht um eine Frage des Datenschutzes. Vielmehr liegt dieser Punkt ausschließlich in den Händen des Krankenhauses.

8.7 Die im Rahmen des Betriebs des KIS notwendigen technischen und organisatorischen Maßnahmen des Datenschutzes sollen auf der Grundlage einer Schutzbedarfs- und Risikoanalyse in einem Datenschutzkonzept und, soweit sie die Informationssicherheit betreffen, auf der Grundlage der IT-Grundschutzstandards 100-1 bis 100-4 des BSI im Informationssicherheitskonzept festgelegt werden.

Kommentierung: Eine Schutzbedarfs- und Risikoanalyse sollte in jedem Krankenhaus durchgeführt werden. Der BSI-Standard ist in vielen Bereichen für ein Krankenhaus nicht zutreffend. Zudem kann in einem Empfehlungsschreiben nicht die Einführung Managementsystems für Informationssicherheit gefordert werden; BSI 100-1 beschäftigt sich genau damit, die Forderung im Empfehlungsschreiben verweist daher genau auf die Einführung eines ISMS.

5.3 Glossar

5.3.1 In der OH KIS unerklärte Begrifflichkeiten

In der Orientierungshilfe KIS werden einige Begriffe immer wieder verwendet, ohne dass eine eindeutige Definition hierfür vorliegt. Nachfolgend wird eine Begriffserklärung für einige immer wieder verwendete Begrifflichkeiten vorgeschlagen.

Begriff	Definition
Datensatz	Ein Datensatz ist eine Gruppe von inhaltlich zusammenhängenden Datenobjekten.
Datenobjekt	**Ein Datenobjekt ist ein Daten beinhaltendes Objekt, welches zusätzlich Attribute und Metadaten beinhaltet. Die Attribute lassen sich nach ihrer Semantik in folgende Kategorien einteilen lassen:** – **Patientenstammdaten,** – **Verwaltungsdaten** – **medizinische und** – **pflegerische Daten.**
Krankheitsfall	Ein Krankheitsfall charakterisiert die Behandlung eines Patienten im Hinblick auf eine bestimmte Erkrankung. Ein Krankheitsfall kann sich über mehrere Abrechnungszeiträume erstrecken, d. h. mehrere Behandlungsfälle beinhalten.
Mandantenfähig	Als mandantenfähig (auch mandantentauglich) wird in der Informationstechnik ein System bezeichnet, welches auf demselben (physikalischen oder virtuellen) Server mehrere Daten verarbeitende Stellen (= „Mandanten“) verwalten kann. Dabei besitzen die Mandanten keinen gegenseitigen Einblick in die zu einem anderen Mandanten gespeicherten Daten oder der zum Mandanten gehörenden Konfiguration des Informationssystems. Ein diesen Anforderungen entsprechendes Informationssystem kann jedoch auch mandantenübergreifende Daten und/oder Objekte beinhalten, sodass zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden muss.
Metadaten	Metadaten sind Daten, welche Informationen über Merkmale anderer Daten enthalten, aber nicht diese Daten selbst. Beispiel: – Status eines (Abrechnungs-) Falls

Begriff	Definition
	– Verantwortlicher Arzt – Ersteller eines Datenobjekts
Organisationseinheit	Sammelbegriff aus der Betriebswirtschaftslehre für durch Zusammenfassung und Zuordnung von (Teil-) Aufgaben zu personalen Aufgabenträgern entstehenden organisatorischen Einheiten. Im Sinne der OH KIS wird ausschließlich die „multipersonale organisatorische Einheit“ betrachtet. Eine Organisationseinheit wird definiert durch - ihre Position innerhalb der Organisation (bezogen auf die anderen Organisationseinheiten) - die Zahl ihrer Stellen - ihre Befugnisse (z. B. Weisungsbefugnisse, Handlungsbefugnisse usw.) - ihre Verantwortlichkeiten (z. B. Umsatzerzielung, Überprüfung von Qualitätsstandards usw.) - ihre Aufgaben (z. B. Verkauf, Produktion usw.) - ihre räumliche Ausdehnung (z. B. Region, Land usw.) - ihre interne Struktur.
Organisationseinheit, funktionsbezogene	Organisationseinheit mit einheitlicher Aufgabe; im medizinischen Umfeld für die Behandlung eines Patienten eingesetzten Personen, welche funktionsunabhängig zu verschiedenen Organisationseinheiten (Stationen, Fachbereichen) eines Krankenhauses gehören können.
Revisionssicherheit	Der Begriff „Revisionssicherheit“ bezieht sich die Anforderungen a. des Handelsgesetzbuches (§§ 239, 257 HGB) b. der Abgabenordnung (§§ 146, 147 AO), c. der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) d. ... d. h., auf praktisch ausnahmslos steuerrechtliche bzw. handelsrechtliche Vorgaben. Andere gesetzlichen Vorgaben werden hierbei nicht beachtet. Die revisionssichere Archivierung ist nur ein Bestandteil der rechtsicheren Archivierung. So beinhaltet eine revisionssichere Archivierung beispielsweise keine datenschutzrechtlichen Vorgaben, z. B. bzgl. des Zugriffs auf die archivierten Daten. Hingegen beinhaltet eine revisions- und rechtssichere Archivierung auch alle rechtlichen

Begriff	Definition
	Anforderungen. Beispiel E-Mail-Archivierung in einem Krankenhaus: Bei einer Terminabstimmung per E-Mail handelt es sich nach dem Bundesdatenschutzgesetz um personenbezogene Daten, die entsprechend BDSG zu löschen sind, sobald die Terminabstimmung erfolgte. So können z. B. alle Mails nach 3 Monaten aus dem Archiv gelöscht werden. Steuerlich relevante Inhalte, wie zum Beispiel Bestellungen bei Lieferanten, müssen 6-10 Jahre aufbewahrt werden. Revisionssicher ist die Archivierung auch dann, wenn alle Mails nach 3 Monaten gelöscht werden. Rechtssicher ist die Archivierung, wenn die Mails revisionssicher entsprechend den verschiedenen gesetzlichen Bestimmungen behandelt werden.
Verfahrensdokumentation	Dokumentation, welche dazu dient, nachweisen zu können, dass die Anforderungen nach GoBS und der Abgabenordnung eingehalten werden.

5.3.2 Begriffe aus Gesetzestexten

Einige Begrifflichkeiten, die in der Orientierungshilfe KIS genutzt werden, sind in verschiedenen Gesetzen definiert, sodass die Begriffsdefinitionen aus den jeweiligen Gesetzen/Verordnungen zur Interpretation der OH KIS verwendet werden müssen. Einiges davon wird in Landesgesetzen definiert, sodass hier nur beispielhaft die Definition aus einem Bundesland (NRW) angegeben werden kann.

Begriff	Definition	Quelle
Arzt	Im jeweiligen Regelungszusammenhang entweder Vertragsarzt, ermächtigter Arzt, angestellter Arzt oder Assistent.	BMV-Ä, §1a Abs. 2
Assistenzarzt	Weiterbildungs- oder Sicherstellungsassistenten gemäß § 32 Abs. 2 Ärzte-ZV; dasselbe gilt für Psychotherapeuten; sie können auch als Ausbildungsassistenten gemäß § 32 Abs. 2 Ärzte-ZV i.V.m. § 8 Abs. 3 PsychThG beschäftigt sein.	BMV-Ä, §1a Abs. 9
Anonymisieren	Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.	BDSG § 3 Abs. 6

Begriff	Definition	Quelle
Aufnahmedatum	Datum, an dem die Behandlungsepisode des aufgenommenen Patienten beginnt.	KHEntgG §8 Abs. 2 i.V. mit Def.-Handbuch 2013 G-DRG
Automatisierte Verarbeitung	Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.	BDSG §3 Abs. 2
Belegarzt	Vertragsarzt mit Versorgungsstatus am Krankenhaus gemäß § 121 Abs. 2 SGB V.	BMV-Ä, §1a Abs. 10
Behandlungsfall (ambulant, MVZ)	Die gesamte von derselben Arztpraxis innerhalb desselben Kalendervierteljahres an demselben Versicherten ambulant zu Lasten derselben Krankenkasse vorgenommene Behandlung gilt jeweils als Behandlungsfall; Behandlungsfälle beziehen sich auf die Rechtsbeziehungen zwischen Kassenärztlichen Vereinigungen und Krankenkassen im Abrechnungswesen.	BMV-Ä, §1a Abs. 28
Behandlungsfall (stationär)	Die Behandlung, die ein Patient von der stationären Aufnahme bis zur Entlassung aus der stationären Behandlung erhält.	KHEntgG §8 Abs. 2 i.V. mit Def.-Handbuch 2013 G-DRG
Behandlungsfall, abgeschlossener	Stationär: aus der stationären Versorgung entlassener Patient Ambulant/MVZ: Quartalsende	
Datenverarbeitung	Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen	DSG NRW,

Begriff	Definition	Quelle
	personenbezogener Daten. Im Einzelnen ist - Erheben (Erhebung) das Beschaffen von Daten über die betroffene Person, - Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung, - Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten, - Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahmebereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft, - Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten, - Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten, - Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten, ungeachtet der dabei angewendeten Verfahren.	§3 Abs. 2
Elektronische Signaturen	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen	SigG, §2 Abs.1
Entlassung	Vorgang, durch den bei einem aufgenommenen Patienten die Behandlungsepisode beendet wird.	KHEntgG §8 Abs. 2 i.V. mit Def.-Handbuch 2013 G-DRG
Identitätsdaten	Identitätsdaten sind: - Familiennamen, Vornamen, Geburtsnamen, frühere Namen und Titel - Geburtstag (Tag im Geburtsmonat), Monat und Jahr der Geburt - Straße und Hausnummer der Wohnanschrift zum Zeitpunkt der Meldung	KRG NRW, §3 Abs 2,3

Begriff	Definition	Quelle
	- Geschlecht - Postleitzahl und Wohnort zum Zeitpunkt der Erkrankung/Meldung - Tag, Monat und Jahr Diagnose - Tag, Monat und Jahr des Todes.	
Löschen	Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.	BDSG, §3 Abs. 4 Nr. 5
Mobile Datenträger	Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger, 1. die an den Betroffenen ausgegeben werden, 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.	BDSG, §3 Abs. 10
Organisatorische Maßnahmen	Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten geeignet sind, 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle), 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle), 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle), 4. zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von	SGB X, Anlage zu § 78a

Begriff	Definition	Quelle
	Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle), 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), 6. zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle), 7. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können. Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.	
Personenbezogene Daten	Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).	BDSG, §3 Abs. 1
Pseudonymisieren	Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.	BDSG §3 Abs. 6a
Psychische Krankheiten	Behandlungsbedürftige Psychosen sowie andere behandlungsbedürftige psychische Störungen und Abhängigkeitserkrankungen von vergleichbarer Schwere.	PsychKG NRW, §1 Abs. 2
Psychotherapeut	Psychotherapeut entspricht der Definition in § 28 Abs. 3 SGB V; danach sind „Psychotherapeuten“ Psychologische Psychotherapeuten und Kinder- und Jugendlichen-Psychotherapeuten. Im jeweiligen Sachzusammenhang kann der Begriff „Psychotherapeut“ Vertragspsychotherapeut, angestellter Psychotherapeut, ermächtigter Psychotherapeut bedeuten.	BMV-Ä, §1a Abs. 3
Sozialdaten	Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden. Betriebs- und	SGB X, §67 Abs. 1

Begriff	Definition	Quelle
	Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.	
Technische und organisatorische Maßnahmen	Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass 1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit), 2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität), 3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit), 4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität), 5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit), 6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz). Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzepts zu ermitteln, zu dessen Bestandteilen die Vorabkontrolle hinsichtlich möglicher Gefahren für das in § 1 geschützte Recht auf informationelle Selbstbestimmung gehört, die vor der Entscheidung über den Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens durchzuführen ist.	DSG NRW, §10 Abs 2/3
Unterlagen	Urkunden, Amtsbücher, Akten, Schriftstücke, amtliche Publikationen, Karteien, Karten, Risse, Pläne, Plakate, Siegel, Bild-, Film- und Tondokumente und alle anderen, auch elektronischen Aufzeichnungen, unabhängig von ihrer Speicherungsform, sowie alle Hilfsmittel und ergänzenden Daten, die für die Erhaltung, das Verständnis dieser Informationen und deren Nutzung notwendig sind.	ArchivG NRW, §2 Abs. 1

5.4 Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern

Obwohl die Orientierungshilfe für sich selbst in Anspruch nimmt, „Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern“[10] zu berücksichtigen, wird in allen in der Orientierungshilfe angesprochenen Szenarien diese Thematik nicht berücksichtigt. Alle Szenarien behandeln die Thematik, wie Daten zwischen einem Krankenhaus und einem externen Versorger ausgetauscht werden, nicht ein Szenario behandelt den Umgang mit den Daten innerhalb eines Krankenhauses. D.h, alle Szenarien beinhalten Aspekte, in welchem es zu einer Offenbarung von Patientengeheimnissen an externe, also außerhalb des Krankenhauses Beschäftigte, kommt. Hier wäre es wünschenswert gewesen, wenn die Datenschutzaufsichtsbehörden mitgeteilt hätten, ob es sich im jeweiligen Fall aus ihrer Sicht um eine befugte oder unbefugte Offenbarung handelt.

5.4.1 Szenario 1: Zulässige Auftragsdatenverarbeitung

Szenario 1a: Gleichwertige Alternativen

Ein von einem Krankenhaus errichtetes MVZ wurde zur vertragsärztlichen Versorgung zugelassen. Das Krankenhaus möchte, um Kosten zu sparen, den Betrieb des Patientenverwaltungssystems von der eigenen IT-Stelle im hauseigenen Rechenzentrum betreiben lassen.

Bei ihrem erstmaligen Besuch erhalten die Patienten die Information über den Betrieb der MVZ-IT durch das Krankenhaus. In der gleichen Stadt sind Vertragsärzte ansässig, die das Leistungsspektrum des MVZ insgesamt abdecken.

Die Patienten erklären im Zuge der Anmeldung schriftlich ihr Einverständnis mit dieser Datenverarbeitung außer Haus.

Szenario 1b: Ersatzverfahren

Im Unterschied zu dem vorigen Szenario sucht Patient P für die Nachbehandlung einer komplizierten Operation, die er am Universitätsklinikum in M hat durchführen lassen einen Spezialisten, der in der Umgebung ausschließlich am MVZ zu finden ist. Das MVZ hat erkannt, dass für einige seiner Patienten die Behandlung am MVZ alternativlos ist und bietet für diejenigen, die das Risiko einer Offenbarung ihrer Daten am Krankenhaus scheuen, ein einfaches papierbasiertes Alternativverfahren für die Führung der Behandlungsakten an. Daher kann sich das MVZ erfolgreich auf die schriftlichen Einverständniserklärungen seiner Patienten stützen, da aufgrund des Alternativverfahrens eine tatsächliche Freiwilligkeit der Einwilligung gewährleistet ist.

Vertragliche, technische und organisatorische Anforderungen

Ein Auftragsdatenverarbeitungsverhältnis (ADV) setzt eine vertragliche Vereinbarung voraus, in dem ein gesetzlich vorgegebener Katalog von Regelungen getroffen werden muss. Unter anderem ist festzuhalten, dass das Krankenhaus die Daten des MVZ nur nach Weisung der Leitung des rechtlich selbständigen MVZ speichern und verarbeiten darf, welche technischen und organisatorischen Maßnahmen das Krankenhaus zum Schutz der Daten des MVZ zu treffen hat, und wie das MVZ die korrekte Ausführung des Auftrags kontrollieren kann.

Zumindest bei großen MVZ liegt es nahe, das im MVZ keine Praxissoftware, sondern ein Modul des Krankenhausinformationssystems zum Einsatz kommt. Zulässig ist dies dann, wenn für das MVZ ein separater Mandant eingerichtet wird. Zu den Anforderungen an die

[10] Begleitpapier zur Orientierungshilfe „Krankenhausinformationssysteme“, Seite 1, Abs. 2

Mandantentrennung vgl. die OH zu diesem Thema, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegeben wurde.

Insbesondere müssen die Zugriffsrechte von Mitarbeitern des MVZ unabhängig von denen des Krankenhauses eingerichtet werden. Dies darf nur nach Weisung der hierzu beauftragten Beschäftigten des MVZ geschehen. Personen, die sowohl vom Krankenhaus als auch vom MVZ beschäftigt werden, müssen zwei verschiedene Benutzerkonten zugeordnet werden.

Jede Angabe zu einem Patienten muss sich eindeutig einem der beiden Mandanten zuordnen lassen, wofür mehrere technische Ausgestaltungsmöglichkeiten denkbar sind. Für einen mandantenübergreifenden Zugriff auf Patientendaten bedarf es stets einer Übermittlungsbefugnis (s.u.). Dies gilt auch für die Stammdaten der Patienten. Vor der gemeinsamen Anzeige von Daten, die aus Krankenhaus und MVZ stammen, ist die Übertragung in den Mandanten, bei dem die nutzende Person angemeldet ist, technisch abzubilden.

Ist vorgesehen, dass Personal des MVZ auch von Geräten des Krankenhauses aus auf Daten von Patienten des MVZ zugreifen soll, muss dies in dem ADV-Vertrag geregelt werden.

Kommentierung: Die Beurteilung der Szenarien 1a und 1 b ist sachlich und rechtlich richtig. Prinzipiell besteht auch die Möglichkeit, dass Patienten der Einsichtnahme in die jeweiligen Daten von MVZ bzw. Krankenhaus zustimmen, insbesondere unter dem Gesichtspunkt, dass ärztliches Personal im MVZ häufig zugleich Beschäftigte des Krankenhauses sind.

5.4.2 Szenario 2: Übermittlung zur Erfüllung eines Konsilauftrages

Szenario 2a: Konsilauftrag an das MVZ

Patient P wird im Krankenhaus behandelt. Der behandelnde Arzt A möchte die fachliche Meinung einer im ambulanten Bereich tätigen Kollegin B einholen. Dies teilt A dem P im Laufe einer Visite mit. Im Nachgang zur Visite wird der Konsilauftrag im Patientenaktensystem (PAS) des Krankenhauses dokumentiert. Dies führt zu einer Übertragung der relevanten Teile der Patientenakte an das MVZ und einer automatisierten Mitteilung an B. Diese nimmt den Konsilauftrag an und sieht die nunmehr freigegebenen Patientendaten ein. Ihr Bericht wird zunächst im AIS gespeichert und dann an das Krankenhaus übertragen, wo er dem A im PAS zur Verfügung steht.

Hätte P der Beauftragung von B widersprochen, so wäre der Konsilauftrag nicht zustande gekommen oder A hätte ihn an die Praxis des Kollegen C gerichtet, sofern P nicht auch gegen dessen Einbeziehung Einwände erhebt.

Szenario 2b: Konsilauftrag an ein Labor des Krankenhauses

Wie im vorigen Szenario erfolgt ein Konsilauftrag, den hier die ambulant tätige Ärztin B mit Wissen von Patientin Q nicht an eine einzelne Person, sondern an ein Speziallabor des Krankenhauses richtet. Der im AIS eingegebene Auftrag wird an das Krankenhaus übertragen, der Befund geht ebenfalls elektronisch den umgekehrten Weg.

Rechtliche, organisatorische und technische Ausgestaltung

Durch den Konsilauftrag kommt ein Vertrag zwischen Beauftragtem und Auftraggeber zustande, der den Rahmen für die Übermittlungen darstellt.

Der Konsilauftrag kann technisch sowohl vom System des Auftraggebers aufgenommen und an den Auftragnehmer über einen sicheren Kanal an den beauftragten Leistungserbringer übertragen werden, als auch direkt von einer Anwendung des Beauftragten entgegengenommen werden, wiederum über einen sicheren Kanal. Bei Anwendung einer Mandantenlösung begründet die Möglichkeit der Übernahme von Konsilen jedoch nicht die

Zulässigkeit des Zugriffs einer Beschäftigten einer Einrichtung auf das PAS bzw. AIS der jeweils anderen.

Kommentierung: Die Beurteilung der Szenarien 2a und 2b ist sachlich und rechtlich richtig.

5.4.3 Szenario 3: Übermittlung zur Nachbehandlung

Szenario 3a: Im Rahmen der ambulanten Behandlung

Patient P wurde im Krankenhaus K operiert. Nach Abschluss seiner stationären Behandlung sucht P zur Nachbehandlung die Ärztin M des krankenhauseigenen MVZ auf. Ärztin M benötigt zur Weiterführung der Behandlung Unterlagen über die Operation im Krankenhaus. Sie informiert P, dass sie die Unterlagen anfordern wird, und nutzt eine Funktion des Arzt-Informationssystems (AIS) des MVZ, um das Krankenhaus über die Weiterbehandlung zu informieren und um Zugang zu der Fallakte des P zu erbitten. Ein hierzu beauftragter Mitarbeiter des Krankenhauses prüft die Anforderung der Unterlagen und überträgt dann die gewünschten Unterlagen aus der Patientenakte des P in einen Zwischenspeicher, aus dem sie automatisiert in das AIS des MVZ übernommen werden. Der Fakt der Übertragung wird ebenso automatisiert in der Patientenakte des P vermerkt.

Die rechtliche Grundlage für diese Übermittlung ergibt sich je nach Landeskrankenhausrecht aus einer konkludenten Einwilligung oder einer gesetzlichen Befugnis.

Szenario 3b: Konkludente Einwilligung im Zuge einer Einweisung

Patient P begibt sich zu seinem Facharzt im MVZ. Der behandelnde Arzt erkennt, dass die ambulante Behandlung nicht zum Ziel führt und weist P in das Krankenhaus ein. P begibt sich in das Krankenhaus. Der dort behandelnde Arzt erkennt, dass er weitergehende Unterlagen aus der ambulanten Behandlung benötigt und ruft bei seinem ihm persönlich bekannten Kollegen im MVZ an. Dieser exportiert die Unterlagen aus dem AIS des MVZ und übermittelt sie elektronisch an das Krankenhaus. Dort werden die Daten in die elektronische Patientenakte des P überführt und stehen in der Folge als Informationsgrundlage für die Behandlung zur Verfügung.

Rechtliche, organisatorische und technische Ausgestaltung

Für eine Übermittlung zwischen Krankenhaus und angeschlossenem MVZ gilt zunächst nichts anderes als für Übermittlungen zwischen dem Krankenhaus und irgendeinem anderen Leistungserbringer: Stützt sich eine Übermittlung auf Aussagen des Empfängers (über das Bestehen eines Behandlungsverhältnisses, über das Vorliegen einer Einwilligung, über das Bestehen einer Notsituation, bei der Gefahr für Leib und Leben des Patienten besteht), so sind diese Aussagen nach Möglichkeit der Umstände zu überprüfen und das Ergebnis zusammen mit der Angabe über die durchgeführte Übermittlung in der Patientenakte zu vermerken. Stellt sich der Anlass der Übermittlung so dringend dar, dass eine Überprüfung im Vorhinein nicht möglich ist, so kann und muss sie im Nachhinein nachgeholt werden.

Einer Übermittlung steht die Bereitstellung zum Abruf gleich. Näheres hierzu siehe in den Erläuterungen zu dem folgenden Szenario.

Kommentierung: Die Beurteilung der Szenarien 3a und 3b ist sachlich und rechtlich richtig.

5.4.4 Szenario 4: Abruf für einen neuen Behandlungsvorgang

Szenario 4a: Einwilligung in die Bereitstellung zum Abruf aus einer einrichtungsübergreifenden Patientenakte

Nach Abschluss seiner Behandlung fragt eine Beschäftigte des Krankenhauses den Patienten P, ob er einverstanden sei, dass Angaben über seine Behandlung in eine einrichtungsübergreifende elektronische Patientenakte eingestellt werden, aus der das Krankenhaus selbst und an einem Behandlungsnetzwerk beteiligte ambulante Einrichtungen Daten abrufen können. P sind alle Leistungserbringer bekannt, die an dem Behandlungsnetzwerk teilnehmen. Derart informiert gibt P seine schriftliche Einwilligung und erhält ein zum Zugriff erforderliches Token/erforderlichen Code.

Als P anderthalb Jahre später im MVZ (das am Behandlungsnetzwerk beteiligt ist) zur Behandlung einer anderen Erkrankung erscheint, erkennt die behandelnde Ärztin, dass sie zur Abschätzung der Risiken eines von ihr in Betracht gezogenen Behandlungsweges die Unterlagen aus der früheren Behandlung im Krankenhaus benötigt. Sie fragt P, ob das Krankenhaus seine Daten zum Abruf bereithalte und führt, nachdem P dies bejaht und das Token/den Code übergibt, den Abruf durch.

Szenario 4b: Gefahr für Leib und Leben

Patient P kommt während eines depressiven Schubes in die Sprechstunde von Neurologin N im MVZ. N ist über den Zustand von P sehr besorgt und möchte die Suizidgefährdung von P mit Hilfe der Unterlagen aus einer früheren Behandlung im Krankenhaus einschätzen. Sie hält P nicht für fähig, eine rationale Entscheidung für oder gegen einen derartigen Datenabruf zu treffen. Sie bittet unter Hinweis auf die Notsituation um Einsicht in die Unterlagen des Krankenhauses. Ein ärztlicher Mitarbeiter des psychiatrischen Fachbereichs des Krankenhauses beurteilt die Erforderlichkeit des Abrufs nach den ihm vorliegenden Unterlagen und lässt dann den Zugriff von N auf die Akten des P freischalten.

Rechtliche, organisatorische und technische Ausgestaltung

Für eine Bereitstellung zum Abruf durch den jeweils anderen Leistungserbringer genügt eine einmalige schriftliche Einwilligung und Schweigepflichtentbindung durch den Patienten, die sich an beide (oder den bestimmten Kreis der) Adressaten richten muss. Der Zweck und die Laufzeit der Einwilligung müssen konkret benannt werden. Je unbestimmter der Zweck, bis hin zur zukünftigen Behandlung noch nicht aufgetretener oder bestimmbarer Erkrankungen, desto enger sollte die Laufzeit gefasst werden. Nicht behandlungsbezogene Einwilligungen (Forschung, Qualitätssicherung) bedürfen in jedem Fall der separaten und expliziten, auf das spezifische Vorhaben oder Verfahren ausgerichteten Einwilligung. Der Patient kann die Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen.

Eine Bereitstellung zum Abruf setzt eine schriftliche Vereinbarung gemäß dem jeweils anwendbaren Bundes- oder Landesdatenschutzrecht voraus. Beispielhaft sei § 10 Bundesdatenschutzgesetz genannt. Auch hier sind die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Dies gilt auch im Falle der ADV, wenn die Maßnahmen nur von einer Seite ausgeführt werden, zum einen für sich selbst und zum anderen für die andere Seite in derem Auftrag.

Zum Abruf bereitgestellte Daten sollten in einen Zwischenspeicher überführt werden. Dies gilt insbesondere dann, wenn der Abruf über Weitverkehrsnetze abgewickelt wird, damit aus diesen kein direkter Durchgriff auf das PAS bzw. das AIS ermöglicht wird. Ein Abruf darf ausschließlich über einen besonders gesicherten verschlüsselten Kanal erfolgen, bei dessen Aufbau sich beide Seiten gegenseitig authentisieren müssen, Die Struktur des Zwischenspeichers muss gewährleisten, dass die Daten eines Patienten bei einem Widerruf der Einwilligung unmittelbar und vollständig gelöscht werden können, ohne die Dokumentation der getätigten Abrufe zu berühren.

Sind Abrufe zwischen zwei Mandanten ein und desselben Systems vorgesehen, so genügt es, die zum Abruf bereitgestellten Daten als solche zu kennzeichnen. Der tatsächliche Abruf

verwirklicht sich durch einen Kopiervorgang aus dem Datenbestand des einen in den Datenbestand des anderen Mandanten.

In beiden Ausgestaltungsformen sind Abrufe wie Übermittlungen in das zu Zwecken der Datenschutzkontrolle geführte Verarbeitungsprotokoll aufzunehmen.

Kommentierung: Die Beurteilung der Szenarien 3a und 3b ist sachlich und rechtlich richtig. Allerdings entspricht die Darstellung der Patientenakte sowie deren Nutzung sehr einfach dargestellt. Hier wäre ein Hinweis auf das IHE-Cookbook[11] sowie der Kommentierung dessen aus Sicht der Datenschutzaufsichtsbehörden wünschenswert.

[11] Aktenbasierte einrichtungsübergreifende Bild- und Befund-Kommunikation [Online] 2013 [Zitiert 2014-04-12] Verfügbar unter http://www.ihe-d.de/index.php/projekte/ihe-d-cookbook

6 Diskussion

Die GMDS begrüßt den Versuch der Datenschutzaufsichtsbehörden, die Interpretation der datenschutzrechtlichen Anforderungen aus föderaler Sicht auf eine bundeseinheitliche Ebene darzustellen.

Die Erweiterung der Orientierungshilfe Krankenhausinformationssysteme um den Bereich des intersektoralen Datenaustausches, wie er in den Szenarien beschrieben wird, ist zu begrüßen. Hier wäre wünschenswert, dass die Aufsichtsbehörden im Anforderungskatalog auch entsprechend auf diesen Bereich eingehen, z. B. indem die Unterstützung verschlüsselter Verbindungen gefordert wird.

Einrichtungsübergreifende Patientenakten werden sowohl in Deutschland wie auch international immer stärker gefordert. Es ist zu begrüßen, dass die Aufsichtsbehörden in ihren Szenarien auch auf diesen Bereich der Patientenversorgung eingehen. Auch hier wäre wünschenswert, wenn die Aufsichtsbehörden ihre Anforderungen gegenüber Betreibern und Herstellern zur Nutzung von Patientenakten darstellen würden. Auch ist wünschenswert, dass die Aufsichtsbehörden nationale Initiativen (Stichwort: IHE-„Cookbook“), die sich mit dem Thema der einrichtungsübergreifenden Patientenakte auseinandersetzen, in ihrer Kommentierung berücksichtigen.

Allerdings gewinnt man beim Lesen den Eindruck, dass aus Sicht der Aufsichtsbehörden für den Datenschutz

1) nur Patienten das Recht auf eine informationelle Selbstbestimmung haben und Datenschutz daher nur für diese gelte, nicht aber für die Beschäftigten im Krankenhaus
2) Beschäftigte im Krankenhaus grundsätzlich mit dem Vorsatz zur Arbeit gehen, möglichst viele Patientendaten unberechtigterweise zur Kenntnis zu nehmen.

Die Orientierungshilfe Krankenhausinformationssysteme stellt mit ihren weitreichenden Vorgaben zur Überwachung der Beschäftigten diese unter einem Generalverdacht. Die geforderte nahtlose Protokollierung und die damit verknüpfte Forderung der Auswertung der Protokollierung geht sogar über die europäische Richtlinie 2006/24/EG zur Vorratsdatenspeicherung hinaus; Letztere erklärte der Europäische Gerichtshof für ungültig[12], jeder kann selbst urteilen, wie vereinbar der von den Datenschutzaufsichtsbehörden geforderte Eingriff in die Grundrechte der Beschäftigten mit dem Grundgesetz ist.

Die Abbildung des Datenschutzrechts in konkrete Maßnahmen bedarf immer einer Abwägung zwischen den den Belangen des Betroffenen und den Interessen der speichernden Stelle oder Dritter, wie es ja auch vom BGH festgestellt wurde[13]. In der Orientierungshilfe Krankenhausinformationssysteme werden des häufigeren Forderungen gestellt, bei denen man sich fragt, ob die Datenschutzaufsichtsbehörden hier eine Abwägung zwischen den wirtschaftlichen Interessen des Krankenhauses und den datenschutzrechtlichen Interessen der Beschäftigten sowie den Belangen eines Patienten vornahmen, oder ob nicht vielmehr die Belange des Patienten als alleiniges Kriterium genutzt zur Ableitung der Forderungen der Datenschutzaufsichtsbehörden wurde.

Die Umsetzung des Datenschutzrechts bedarf unter anderem

[12] Pressemitteilung des Europäischen Gerichtshofes [Online] 2014 [Zitiert 2014-04-16] Verfügbar unter http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf

[13] BGH: Zulässigkeit der Speicherung personenbezogener Daten durch die Schufa. [Online] 2014 [Zitiert 2014-04-16] Verfügbar unter http://dejure.org/dienste/vernetzung/rechtsprechung?Text=III%20ZR%20207%2F82&Suche=III%20ZR%20207%2F82 bzw. http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/WirtschaftUndFinanzenVerkehr/Artikel/151283_SchutzwuerdigeBelangeErfordernAbwaegung.html?nn=408918

- einer Kombination aus Kenntnissen des Datenschutzrechts,
- dem Wissen um das technisch Verfüg- und Einsetzbare im Bereich der Informations- und Kommunikationstechnik,
- einer betriebswirtschaftlichen Grundkompetenz
- dem Bewusstsein über die technische und organisatorische Struktur der Daten verarbeitenden Stelle, also dem Krankenhaus,

wie es der Düsseldorfer Kreis selbst formuliert[14]. In der Orientierungshilfe Krankenhausinformationssysteme kann der Leser den Eindruck gewinnen, dass von diesen Anforderungen zur Interpretation des Datenschutzrechts beim Verfassen der Orientierungshilfe wenig genutzt wurde:

- Die Rechtsgrundlagen für die Anforderungen wurden nicht dargelegt.
- Die Wortwahl der Anforderung deckt sich nicht immer mit dem von den Datenschutzaufsichtsbehörden vorgegebenen Grad der Verbindlichkeit (Beispiel Teil 2, Anforderung 8.6 zweiter Satz: Grad der vorgegebenen Verbindlich keit „sollte“, Wortwahl „ist zu tun“, also muss).
- Die Anforderungen der Orientierungshilfe zeigen, dass bzgl. der vorhandenen Informationssysteme und deren Möglichkeiten bei den Datenschutzaufsichtsbehörden überwiegend ein Unwissen über deren Funktionalität und den Möglichkeiten im praktischen Einsatz vorherrscht.
- Eine Abwägung zwischen den Belangen des Betroffenen und den Belangen der Beschäftigten scheint nicht stattgefunden zu haben.
- Eine Abwägung zwischen den Belangen des Betroffenen und den Interessen der Daten verarbeitenden Stelle scheint nicht stattgefunden zu haben, was letztlich am Vorhandensein der für ein Krankenhaus wichtigen betriebswirtschaftlichen Kenntnissen zweifeln lässt.
- Der Workflow bzgl. Patientenbehandlung in einem Krankenhaus scheint unbekannt zu sein, da mitunter Forderungen gestellt werden, welche das Potential der Patientengefährdung in sich tragen; eine Kenntnis der technischen und organisatorischen Strukturen in einem Krankenhaus scheint damit auch nicht im ausreichendem Maß vorhanden zu sein.

Wünschenswert wäre aus Sicht der GMDS daher:

a) eine Darstellung der Rechtsgrundlagen auf Grund derer welche Anforderung seitens der Datenschutzaufsichtsbehörden gestellt wird,
b) eine Berücksichtigung der Rechte der Beschäftigten auf informationelle Selbstbestimmung, d. h. eine Abwägung zwischen der Wahrscheinlichkeit eines Fehlverhaltens einer/eines Beschäftigten und der generellen Überwachung aller zur Wahrung der Interessen eines Patienten,
c) eine Begrenzung der zwingenden Anforderungen der Orientierungshilfe Krankenhausinformationssysteme auf diejenigen Anforderungen, die für alle Bundesländer gelten,
d) eine Kennzeichnung derjenigen bundeslandspezifischen Anforderungen, die nicht in allen Bundesländern gelten, von den Aufsichtsbehörden im Rahmen von Prüfungen in einzelnen Bundesländern jedoch als zwingende Anforderung betrachtet wird; die Kennzeichnung muss hierbei abbilden, für welches Bundesland es gilt,

[14] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich[Online] 2010 [Zitiert 2014-04-16] Verfügbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Mindestanforderungen_an_Datenschutzbeauftragte/Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf

e) die Berücksichtigung datenschutzrechtlicher Fragen im Bereich der Forschung mit Daten aus der Gesundheitsversorgung (Stichwort: Sekundärnutzung von Routinedaten).

In der derzeitigen Form scheint die Orientierungshilfe Krankenhausinformationssystem eher darauf abzuzielen, dass die Datenschutzaufsichtsbehörden für den Betroffenen - egal ob unter der jeweilige Betroffene ein Patient, ein Beschäftigter im Krankenhaus oder ein Beschäftigter bei einem Auftragsdatenverarbeiter darstellt - entscheiden, was mit seinen Daten geschieht, d. h. den Betroffenen wird letztlich von den Datenschutzaufsichtsbehörden bzgl. seines Rechts auf informationelle Selbstbestimmung entmündigt. Diesen Eindruck zu vermitteln, ist sicherlich nicht das Ziel der Datenschutzaufsichtsbehörden gewesen.

Es muss also eine Weiterentwicklung der Orientierungshilfe erfolgen und zwar

- im Sinne der Selbstbestimmung des Patienten
- unter einer stärkeren Berücksichtigung des Wohles des Patienten innerhalb Diagnostik und Behandlung
- im Hinblick auf die Achtung der Persönlichkeitsrechte der Beschäftigten
- in Hinsicht der Darlegung der Rechtsgrundlagen, auf denen die Anforderungen für einen datenschutzkonformen Betrieb eines Krankenhausinformationssystems beruhen.

Dazu müssten die Datenschutzaufsichtsbehörden aber verstärkt auf andere Organisationen zugehen und mit diesen zusammenarbeiten. Derzeit fehlt der Orientierungshilfe Krankenhausinformationssystemen in vielen Fällen die Praxisnähe, die nur durch die Zusammenarbeit der Datenschutzaufsichtsbehörden mit den verschiedenen Organisationen kommen kann. Beispielhaft ohne Anspruch auf Vollzähligkeit seien hier in alphabetischer Reihenfolge genannt[15]:

- Datenschutzfragen: BvD, GDD, GMDS
- Einsatz von Standards: GMDS, HL7-D, IHE-D, Interoperabilitätsforum
- Forschungsfragen: GMDS, TMF
- Krankenhausverwaltung: DKG, GMDS, KH-IT
- Patientenversorgung: Bundesärztekammer, DBfK, GMDS
- Patientenvertretung: BAGP, DAG SHG, vzbv
- Technische Umsetzung: bvitg, GMDS, KH-IT

Die Orientierungshilfe Krankenhausinformationssysteme ist ein erster wichtiger Schritt in die richtige Richtung: der Betroffene muss selbst entscheiden können und dürfen, was mit seinen Daten geschieht und was nicht geschehen soll. Es ist zu hoffen, dass für die nächste Überarbeitung (Ausgabe Orientierungshilfe Krankenhausinformationssysteme 2016?) die Datenschutzaufsichtsbehörden verstärkt Fachgruppen in den Dialog einbeziehen und deren Kommentierungen auch berücksichtigen, letzteres ist in der Vergangenheit oftmals nicht geschehen.

Damit die Orientierungshilfe in einer gemeinsamen Anstrengung fit für den Einsatz in der Praxis gemacht wird, ist eine Zusammenarbeit zwischen Datenschutzaufsichtsbehörden und Fachgruppen unabdingbar; das alleinige Vorgehen der Datenschutzaufsichtsbehörden erzeugt ein für die Praxis untaugliches Bürokratiemonster, bei dem zudem die Rechtsgrundlagen für die gestellten Forderungen fragwürdig sind.

[15] Vollständige Namensnennung der Organisationen in der Tabelle mit Abkürzungen auf Seite 71

7 Abkürzungen

AG	Arbeitsgruppe
AIS	Arztinformationssystem
AO	Abgabenordnung
ArchivG NRW	Archivgesetz Nordrhein-Westfalen
AZ	Aktenzeichen
BAG	Bundesarbeitsgericht
BAGP	BundesArbeitsGemeinschaft der PatientInnenstellen und -Initiativen
BayKrG	Bayerisches Krankenhausgesetz
BbgKHEG	Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz)
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMV-Ä	Bundesmantelvertrag
BremKHDSG	Bremisches Krankenhausdatenschutzgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
bvitg	Bundesverband Gesundheits-IT e.V.
DAG SHG	Deutsche Arbeitsgemeinschaft Selbsthilfegruppen e.V.
DBfK	Deutscher Berufsverband für Pflegeberufe
DKG	Deutsche Krankenhausgesellschaft e.V.
DRG	Diagnosis Related Groups, =Fallpauschale
DSG	Datenschutzgesetz
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
ECHR	European Court of Human Rights („the Court“)
EDV	Elektronische Datenverarbeitung
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
GDSG NRW	Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen NRW(Gesundheitsdatenschutzgesetz NRW)
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
HL7-D	HL7 Deutschland e.V.
HmbKHG	Hamburgisches Krankenhausgesetz

HmbKHG	Hamburgisches Krankenhausgesetz
IHE-D	IHE Deutschland e. V.
KHEntgG	Gesetz über die Entgelte für voll- und teilstationäre Krankenhausleistungen
KHG	Krankenhausgesetz
KH-IT	Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V.
LKG	Landeskrankenhausgesetz
LKHG	Landeskrankenhausgesetz
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
MDK	Medizinischer Dienst der Krankenkasse
MVZ	Medizinisches Versorgungszentrum
OH KIS	Orientierungshilfe. „Krankenhausinformationssysteme“
OLG	Oberlandesgericht
PsychKG NRW	Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten
PsychThG	Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten (Psychotherapeutengesetz)
SGB	Sozialgesetzbuch
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
StGB	Strafgesetzbuch
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
vzbv	Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.