

Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern



Datenschutz

im Krankenhaus

Stand: Januar 2003
Herausgeber: Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin
19053 Schwerin
Telefon: (03 85) 5 94 94-0
Telefax: (03 85) 5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: <http://www.lfd.m-v.de>

Inhalt

Grundlagen

Einleitung	4
Ärztliche Schweigepflicht	5
Offenbarung aufgrund der Patienteneinwilligung	6
Offenbarung aufgrund von Rechtsvorschriften	8
Offenbarungsbefugnis	8
Offenbarungspflicht	10
Dokumentation	10

Landeskrankenhausgesetz Mecklenburg-Vorpommern – LKHG M-V

Geltungsbereich	11
§ 14 Anwendungsbereich und Begriffsbestimmungen	13
§ 15 Erheben und Speichern von Daten	15
§ 16 Nutzen und Übermitteln von Daten im Krankenhaus	20
§ 17 Übermitteln an Stellen außerhalb des Krankenhauses	24
§ 18 Auskunft und Akteneinsicht	32
§ 19 Löschung und Sperrung von Daten	33
§ 20 Datenverarbeitung für Forschungszwecke	37
§ 21 Datenverarbeitung im Auftrag	42
§ 20 DSGVO M-V Behördlicher Datenschutzbeauftragter	47

Einzelprobleme beim Datenschutz im Krankenhaus

Prüfungen des Medizinischen Dienstes der Krankenversicherung (MDK)	56
Gesetzliche Grundlagen	56
Zuständigkeit des MDK	56
Begutachtung nach § 275 SGB V	56
Begutachtung nach § 276 Abs. 4 SGB V	59
Begutachtung nach § 17a KHG	60
Übermittlung der gutachterlichen Stellungnahme	61
Datenübermittlung innerhalb des Krankenhauses	61

Psychischkrankengesetz Mecklenburg-Vorpommern – PsychKG M-V

§ 43 Personenbezogene Daten	62
§ 44 Bekanntgabe und Begründung von Anordnungen, Akteneinsicht	64

Dienstanweisung zum Datenschutz im Krankenhaus

Vorbemerkung	65
Gliederung	66
Allgemeines	67
Einleitung	67
Rechtliche Grundlagen	67
Schweigepflicht, Datengeheimnis	68
Patientendatenschutz im Einzelnen	68
Erheben und Speichern von Daten (§ 15 LKHG M-V)	68

Nutzen und Übermitteln von Daten im Krankenhaus (§ 16 Abs. 1, 4 LKHG M-V)	68
Grundsätze der Datenübermittlung	69
Übermittlung innerhalb des Krankenhauses (§ 16 Abs. 3 LKHG M-V)	70
Übermittlung an Stellen außerhalb des Krankenhauses (§ 17 LKHG M-V)	71
Datenverarbeitung nach Abschluss der Behandlung (§ 19 LKHG M-V)	73
Datenverarbeitung für Forschungszwecke (§ 20 LKHG M-V)	73
Datenverarbeitung im Auftrag (§ 21 LKHG M-V)	74
Beschlagnahmeschutz	74
Rechte des Betroffenen (§ 18 LKHG M-V)	74
Datenschutzbeauftragter des Krankenhauses (§ 20 DSG M-V)	74
Anhang	
Datenschutzbehörden in Mecklenburg-Vorpommern	75
Muster einer Bestellung zum behördlichen Datenschutzbeauftragten	77
Orientierungshilfe „Forderung an Wartung und Fernwartung“	79
Weiterführende Informationen und Literatur	82
Abkürzungsverzeichnis	83
Stichwortverzeichnis	84

Grundlagen

Einleitung

Das Datenschutzrecht hat sich seit Beginn der siebziger Jahre im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten kontinuierlich entwickelt und umfasst alle Bereiche des gesellschaftlichen Lebens. Vorrangige Aufgabe des Datenschutzes ist es, das **Recht auf informationelle Selbstbestimmung** der Bürgerinnen und Bürger zu gewährleisten, das heißt die Befugnis jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Dieses Recht basiert auf dem **Persönlichkeitsrecht** des Artikels 2 in Verbindung mit dem Schutz der Menschenwürde in Artikel 1 Grundgesetz und ist durch das Bundesverfassungsgericht im so genannten Volkszählungsurteil von 1983 formuliert und vom Landesgesetzgeber in § 1 des Landesdatenschutzgesetzes Mecklenburg-Vorpommern verankert worden. Nicht der abstrakte Schutz von Daten ist folglich das Ziel, sondern die Wahrung eines wesentlichen Rechts jedes Einzelnen.

Mit personenbezogenen Daten darf nur unter einem **Erlaubnisvorbehalt** umgegangen werden, das heißt, die personenbezogene Datenverarbeitung ist nur „ausnahmsweise“ erlaubt, und zwar dann, wenn ein Datenschutzgesetz oder eine andere Rechtsvorschrift dies vorsieht oder der betroffene Bürger darin eingewilligt hat. In der Verfassung unseres Bundeslandes ist das Recht auf Schutz der personenbezogenen Daten in Artikel 6 geregelt.

Neben dem Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG M-V), das für die öffentlichen Stellen des Landes gilt, gibt es eine Vielzahl bereichsspezifischer Regelungen. Dadurch ist es nicht immer leicht, die geltenden Datenschutzvorschriften zu überblicken. Auch bei der Verarbeitung von Patientendaten innerhalb eines Krankenhauses sind nicht nur die Vorschriften des Landeskrankenhausgesetzes für das Land Mecklenburg-Vorpommern (LKHG M-V), sondern in Abhängigkeit von der zu erfüllenden Aufgabe weitere gesetzliche Vorschriften zu beachten.

Datenschutzrechtliche Regelungen zielen darauf, den Umgang mit personenbezogenen Daten in der Weise vorzuschreiben, dass sie nicht missbräuchlich verwendet werden. Die sachgerechte Verarbeitung dieser Daten ist durch angemessene **technische und organisatorische Maßnahmen** sicherzustellen. Weiterhin wird geregelt, welche Rechte der Betroffene hat, wie die Einhaltung der Vorschriften kontrolliert wird und wie Verstöße geahndet werden können.

Während man vor der Einführung des Datenschutzrechts das Persönlichkeitsrecht eines Betroffenen durch Geheimhaltungsvorschriften wahren konnte, beispielsweise durch die **Schweigepflicht der Ärzte** und ärztlichen Helfer oder durch das Post-, Brief- und Fernmeldegeheimnis, ist durch die automatisierte Datenverarbeitung und durch neue Informations- und Kommunikationstechnologien das Risiko der Verletzung des Persönlichkeitsrechts gestiegen. Datenschutzrechtliche Vorschriften sollen dieses Risiko für den Betroffenen in Grenzen halten. Dabei gelten die „konventionellen“ Geheimhaltungsvorschriften weiterhin, und sie sind darüber hinaus durch das Datengeheimnis ergänzt worden.

Bei der Anwendung datenschutzrechtlicher Vorschriften ist zu beachten, dass Regelungen in Spezialgesetzen, wie dem LKHG M-V, den Regelungen in den allgemeinen Datenschutzgesetzen, wie dem DSG M-V oder dem Bundesdatenschutzgesetz (BDSG), vorgehen. Diese allgemeinen Gesetze bezeichnet man daher als Auffanggesetze.

Das LKHG M-V regelt speziell die Verarbeitung von Patientendaten im Krankenhaus. Es verweist aber auch auf das DSGVO M-V, welches mit Ausnahme einiger Vorschriften neben dem LKHG M-V ebenfalls anzuwenden ist. An dieser Stelle sei darauf hingewiesen, dass das DSGVO M-V in der Regel nur für öffentliche Stellen des Landes gilt.

Im privatrechtlichen Bereich kommt das BDSG zur Anwendung. Zu der damit verbundenen Problematik der unterschiedlichen datenschutzrechtlichen Kontrollzuständigkeiten siehe zum Geltungsbereich des LKHG M-V, Seite 12.

Ärztliche Schweigepflicht

Warum müssen Patientendaten besonders geschützt werden, und welche Folgen kann eine Offenbarung dieser Daten für einen betroffenen Patienten haben?

Angaben über die gesundheitliche Disposition eines Menschen gehören zu seinen intimsten Daten. Werden diese Daten unzulässigerweise einem Dritten bekannt, so kann das nicht nur zur Schädigung des Ansehens des betroffenen Patienten und zu seiner gesellschaftlichen Ausgrenzung führen, sondern unter Umständen auch zu einer existenziellen Bedrohung für ihn werden, beispielsweise dass er seine Arbeit verliert, obwohl er weiterhin arbeits- und leistungsfähig ist, und dergleichen mehr.

Diese Gefahr für einen Betroffenen hat bereits Hippokrates vor mehr als zweitausend Jahren erkannt und seine Schüler unter anderem schwören lassen: „Was ich in meiner Praxis sehe und höre und außerhalb dieser im Verkehr mit Menschen erfahre, was niemals anderen Menschen mitgeteilt werden darf, darüber werde ich schweigen in der Überzeugung, dass man solche Dinge stets geheim halten muss“. Der Inhalt des hippokratischen Eides hat Eingang in die Berufsordnungen der Ärzte gefunden. Ärzte müssen ein in der Berufsordnung enthaltenes Gelöbnis ablegen und sich unter anderem dazu verpflichten „alle ... anvertrauten Geheimnisse auch über den Tod des Patienten hinaus zu wahren“. Im Übrigen gilt die **Schweigepflicht** in gleicher Weise unter Ärzten, § 9 Abs. 4 BOÄ M-V. Soll ein weiterer Arzt in die Behandlung eines Patienten einbezogen werden, so ist dafür die **Einwilligung** des Patienten erforderlich. Es wird davon ausgegangen, dass eine konkludente Einwilligung in einem solchen Fall ausreichend ist – der behandelnde Arzt muss also dem Patienten erklären, dass ein weiterer Arzt in die Behandlung einbezogen werden muss, und sollte die Gründe dafür darlegen. Wenn ein Patient der Hinzuziehung eines anderen Arztes nicht widerspricht, so ist von seiner Einwilligung auszugehen. Damit ist dann auch die Weitergabe der für diese Behandlung erforderlichen Daten zulässig. Der erstbehandelnde Arzt muss allerdings noch abwägen, welche Daten der hinzugezogene Arzt benötigt.

In einem Krankenhaus lässt sich die Schweigepflicht kaum auf einen bestimmten Arzt beziehen, da regelmäßig mehrere Ärzte an der Behandlung beteiligt sind. Hier ist diese Grenze durch die Behandlung innerhalb der **Fachabteilung** gegeben. Sofern also eine weitere Fachabteilung oder gar ein anderes Krankenhaus in die Behandlung einbezogen werden soll, ist der Patient darüber aufzuklären, und erst nach seiner Zustimmung dürfen die für diese Behandlung erforderlichen Daten übermittelt werden.

Die Verletzung der ärztlichen Schweigepflicht ist durch § 203 Abs. 1 sowie 3 bis 5 StGB strafbewehrt. Der hohe Stellenwert der ärztlichen Schweigepflicht kommt auch darin zum Ausdruck, dass dem Arzt in Straf- oder Zivilprozessen ein **Zeugnisverweigerungsrecht** zusteht, er also auch vor Gericht in diesen Fällen Verschwiegenheit wahren kann, § 53

Abs. 1 Nr. 3 StPO und § 383 Abs. 1 Nr. 6 ZPO. Das Zeugnisverweigerungsrecht des Arztes wurde schließlich auch durch ein ausdrückliches **Beschlagnahmeverbot** ergänzt, § 97 StPO. Damit ist es den Strafverfolgungsbehörden verwehrt, die im Besitz eines Arztes befindlichen Krankengeschichten, Untersuchungsbefunde oder andere Unterlagen mit Angaben über einen Patienten zu beschlagnahmen. Für Gegenstände in Krankenhäusern besteht eine Spezialregelung in § 97 Abs. 2 Satz 2 StPO, da sich die Unterlagen regelmäßig nicht in Gewahrsam des einzelnen Arztes befinden: „Der Beschlagnahme unterliegen auch nicht Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Ärzte, Zahnärzte, Apotheker und Hebammen erstreckt, wenn sie im Gewahrsam einer Krankenanstalt sind,“

Für Patientendaten/-unterlagen außerhalb eines Krankenhauses, wenn das Krankenhaus also keinen Gewahrsam an den Unterlagen mehr hat, besteht kein Schutz vor Beschlagnahme.

Und dennoch gibt es auch Fälle, in denen trotz Gewahrsams an den Patientenunterlagen eine Beschlagnahme zulässig sein kann. In § 97 Abs. 2 Satz 3 StPO heißt es dazu: „Die Beschränkungen der Beschlagnahme gelten nicht, wenn die zur Verweigerung des Zeugnisses Berechtigten einer Teilnahme oder einer Begünstigung, Strafvereitelung oder Hehleri verdächtig sind oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren“. So ist beispielsweise in einem Fall die **Durchsuchungsanordnung** und die darauf folgende **Beschlagnahme von Patientenakten** bei niedergelassenen Ärzten im Rahmen eines Ermittlungsverfahrens wegen des Verdachts des Ausstellens unrichtiger Gesundheitszeugnisse und des Verstoßes gegen das Ausländergesetz für zulässig erachtet worden (Berliner Verfassungsgerichtshof vom 28.06.2001 – 100/00). Eine solche Konstellation des § 97 Abs. 2 Satz 3 StPO wäre auch bei Unterlagen denkbar, die vom Krankenhaus erstellt und aufbewahrt werden.

Richten sich dagegen die Ermittlungen gegen den Patienten, und hat dieser seinen Arzt von der Schweigepflicht entbunden, so entfällt hierdurch das Beschlagnahmeverbot bei dem Arzt, der ja sonst nach § 53 Abs. 1 Nr. 3 StPO das Zeugnis verweigern dürfte. Mit der Entbindung von der Schweigepflicht ist der Arzt auf Anfrage der Ermittlungsbehörden dann auch zur Herausgabe der sich in seinem Gewahrsam befindlichen Gegenstände gemäß § 95 StPO verpflichtet.

Schließlich ist auch das vertrauliche Gespräch zwischen Arzt und Patient von der akustischen Raumüberwachung zum Zweck der Strafverfolgung (großer Lauschangriff) ausgenommen, § 100d Abs. 3 StPO. Dieses Ergebnis ist allerdings erst durch massive Intervention der Öffentlichkeit gegen den ursprünglichen Gesetzentwurf entstanden. Im Bereich der Gefahrenabwehr ist die Raumüberwachung unter engen Voraussetzungen nach § 33 Abs. 6 SOG M-V allerdings zulässig.

Offenbarung aufgrund der Patienteneinwilligung

Ein Arzt oder ein Krankenhaus darf das Geheimnis preisgeben, wenn der Betroffene eingewilligt hat oder wenn eine Rechtsvorschrift dies ausdrücklich vorsieht.

Voraussetzung für eine **Einwilligung** oder Erklärung zur Entbindung von der Schweigepflicht ist, dass der einwilligende Patient die Tragweite seines Entschlusses erkennen kann. Der Patient muss die Einwilligung für einen bestimmten Zweck geben. Eine Generalein-

willigung in der Art, dass der Patient den Arzt von der Schweigepflicht entbindet, ohne den Zweck und damit eine Grenze für die Einwilligung vorzugeben, ist nicht zulässig. Beispiel: „Ich entbinde meinen Arzt von seiner Schweigepflicht.“

Die Datenübermittlung auch medizinischer Daten an Sozialversicherungsträger ist gesetzlich geregelt, überwiegend im Sozialgesetzbuch. In Einzelfällen, insbesondere bei Sozialleistungen, die auf Antrag gewährt werden, benötigen Sozialversicherungsträger häufig Patientendaten auf der Basis einer **Schweigepflichtentbindungserklärung**. In solchen Fällen ist es ausreichend, wenn der Sozialversicherungsträger dem Krankenhaus oder dem Arzt mitteilt, dass für einen bestimmten Zweck Patientendaten benötigt werden und dass eine solche Erklärung vorliegt. Es ist nicht notwendig, dass das Krankenhaus oder der Arzt eine Kopie davon erhalten, da der Sozialversicherungsträger die Verantwortung für richtige Angaben (Schweigepflichtentbindungserklärung liegt vor) in seinem Gesuch trägt. Wenn allerdings eine Kopie zur eigenen Absicherung gewünscht wird, so kann sie nicht verwehrt werden.

Liegt einem Arzt ein solches **Ersuchen** vor, so muss er in jedem Fall prüfen, welche Daten er übermittelt. Der Arzt trägt die Verantwortung dafür, dass es nur die **erforderlichen Daten** sind; beispielsweise ist die Übermittlung der vollständigen Krankengeschichte in der Regel nicht erforderlich.

Nicht in jedem Fall ist eine schriftliche Schweigepflichtentbindungserklärung notwendig. Bittet ein Patient den Arzt um eine Untersuchung und um das Ausfüllen eines Erhebungsbogens über seinen Gesundheitszustand für den Abschluss einer Lebensversicherung, so gibt er damit zu erkennen, dass der Arzt diese Daten an die Versicherung weitergeben darf. Zu beachten ist dabei, dass diese Daten nicht einem Dritten, zum Beispiel einem Sozialversicherungsträger, offenbart werden dürfen, es sei denn, es liegt eine ausdrückliche Einwilligung für diesen Zweck vor.

Einer gesonderten Schweigepflichtentbindung bedarf es auch in den Fällen nicht, in denen sich ein Patient bei der zuständigen Stelle, beispielsweise bei der Ärztekammer, über die Behandlung seines Arztes beschwert. Mit der erhobenen **Beschwerde** begründet der Patient nicht nur die Pflicht der zuständigen Stelle, eine sachliche Prüfung und die Erteilung eines schriftlichen Bescheides vorzunehmen. Er gibt mit seiner Beschwerde auch den Umfang sowohl der Schweigepflichtentbindung als auch der Prüfung vor. Der Wunsch des Patienten, einen bestimmten, von ihm dargelegten Sachverhalt prüfen zu lassen, beinhaltet gleichzeitig eine, wenn nicht ausdrücklich, dann aber doch konkludent erklärte, tatbestandsausschließende Schweigepflichtentbindung des von der Beschwerde betroffenen Arztes gegenüber den die Beschwerde bearbeitenden Stellen. Der Patient braucht daher nach Eingang der Beschwerde nicht noch extra aufgefordert zu werden, den von der Beschwerde betroffenen Arzt von seiner Schweigepflicht zu entbinden.

Eine über den von der Beschwerde vorgegebenen Rahmen hinausgehende **Geheimnisoffenbarung** durch den Arzt oder eine darüber hinausgehende Sachprüfung durch die zuständige Stelle wären von der Beschwerde nicht mehr gedeckt. So muss der sich beschwerende Patient den wesentlichen Inhalt seiner Beschwerde mitteilen. Nur so können der betroffene Arzt und die bearbeitende Stelle erkennen, auf welches Verhalten oder welche Behandlung des Arztes und welchen Prüfumfang sich die Beschwerde bezieht. Beschwerft sich beispielsweise ein Patient über eine Terminvergabe, ist zur Prüfung der Beschwerde die Mitteilung der Diagnose und der Behandlung grundsätzlich nicht zulässig. Anders in den Fällen, in denen die Terminvergabe mit der gesundheitlichen Disposition unmittelbar

zusammenhängt. Zum Beispiel, wenn der Patient trotz offensichtlich schlechten Gesundheitszustandes nicht behandelt und auf einen späteren Zeitpunkt verwiesen wird.

Offenbarung aufgrund von Rechtsvorschriften

Offenbarungsbefugnis

Im Rahmen des Vertragsverhältnisses zwischen Arzt/Krankenhaus und Patient gibt es viele Rechtsvorschriften zur Datenübermittlung. Auf die für den Krankenhausbereich speziell geltenden wird bei der Erläuterung des LKHG M-V näher eingegangen.

Ein Arzt kann im Einzelfall gemäß § 34 StGB der Geheimniswahrung unterliegende Tatsachen Dritten mitteilen, wenn dadurch eine **Gefahr** für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut abgewendet werden kann. Er handelt dann nicht rechtswidrig und kann für die Preisgabe des ihm anvertrauten Geheimnisses nicht bestraft werden. Vor einer solchen Offenbarung ist in jedem Fall abzuwägen, ob das damit zu schützende Interesse das beeinträchtigte Interesse an der Geheimhaltung erheblich überwiegt. Beispielsweise wäre es gegebenenfalls zulässig, die Verkehrsbehörde darüber zu informieren, dass ein Patient aufgrund seiner Krankheit kein Fahrzeug mehr führen kann und bei Teilnahme am Straßenverkehr sich und andere gefährden würde. Voraussetzung ist jedoch, dass der Arzt zuvor versucht hat, den Patienten davon zu überzeugen, von sich aus seinen Führerschein abzugeben und kein Fahrzeug mehr zu führen. Falls das Zureden des Arztes erfolglos bleibt, sollte er dem Patienten mitteilen, dass er in diesem Fall die Verkehrsbehörde benachrichtigt – die Information des Patienten ist zwar gesetzlich nicht vorgeschrieben, trägt aber zur Transparenz bei. Teilt der Arzt seine Bedenken nicht der Verkehrsbehörde mit, entstehen für ihn daraus keine straf- oder zivilrechtlichen Vorwürfe, wenn er den Patienten entsprechend über eine etwaige Fahruntauglichkeit aufgeklärt und aufgefordert hat, selbst entsprechende Schritte einzuleiten.

Unter Umständen ist ein Arzt sogar verpflichtet, seine ärztliche Schweigepflicht zu brechen. In einem Fall ist ein Arzt wegen unterlassener Hilfeleistung verurteilt worden, weil er es unterließ, die Eltern eines **minderjährigen** Mädchens über ihre Risikoschwangerschaft aufzuklären. Das junge Mädchen folgte nicht dem Rat des Arztes, ins Krankenhaus zu gehen, und verstarb an den Komplikationen der **Schwangerschaft**. Die Richter waren der Auffassung, dass in dieser Situation der Arzt hätte tätig werden und die Eltern informieren müssen. Nur so hätte das Mädchen gerettet werden können (Bundesgerichtshof – 1 StR 413/82).

Ein weiteres Beispiel: **HIV-Infizierte**. Diese Personen brauchen die Verschwiegenheit des Arztes in stärkstem Maße. Jedoch ist ein frühzeitiges Mitwissen Dritter, wenn für diese die Gefahr der Infektion gegeben ist, wichtig für deren Schutz. Deshalb sollte der Arzt dem Infizierten dringend raten, sich diesen gefährdeten Dritten zu offenbaren, und er sollte ihm dabei auch helfen. Unterrichtet der Infizierte die Personen nicht, so kann sich der Arzt nach **Abwägung** des Geheimhaltungsinteresses mit den Rechtsgütern Leben und Gesundheit des oder der Dritten auf den **rechtfertigenden Notstand** berufen und beispielsweise gefährdete Personen warnen oder die HIV-infizierte uneinsichtige Prostituierte der Behörde anzeigen. In diesem Zusammenhang ist zu erwähnen, dass bereits die Infizierung eines Dritten durch den ungeschützten Geschlechtsverkehr eines HIV-Infizierten, der von seiner Infektion Kenntnis hat, strafrechtlich verfolgt werden kann, § 223 StGB.

Ein Arzt ist an die Schweigepflicht nicht gebunden, wenn die Vertrauenssphäre zwischen dem Arzt und dem Patienten beispielsweise für Straftaten zu Lasten des Arztes oder die Nichtzahlung des ärztlichen Honorars missbraucht wird. Hier muss das Interesse des Patienten an der Geheimhaltung hinter dem Anspruch des Arztes auf Wahrnehmung eigener Interessen zurücktreten. Der Arzt wäre anderenfalls wegen seiner Verschwiegenheitspflicht praktisch rechtlos, während sich der betroffene Patient hinter dem Schweigegebot des Arztes „verstecken“ könnte, obwohl er selbst den Interessenkonflikt veranlasst hat.

Ein weiteres Beispiel ist die Simulation einer Krankheit. Auch hier besteht kein Schweigegebot bei so genannten Krankenhauswanderern, die sich Unterkunft und Verpflegung im Krankenhaus erschleichen. Dies bedeutet jedoch nicht, dass das Krankenhaus eine Liste mit Namen solcher Personen führen darf, um bereits bei der Aufnahme wirtschaftlichen Schaden zu vermeiden. Diese „Warnmeldung“ dürfte auch praktisch bedeutungslos sein, da es sich bei der Aufnahme des „Patienten“ durchaus um einen Notfall handeln und das Krankenhaus dann die Behandlung nicht ablehnen kann. Eine gründliche Aufnahmeuntersuchung in bestimmten Aufnahmesituationen sowie ein gesundes Misstrauen dürften besser geeignet sein, einen wirtschaftlichen Schaden zu vermeiden. Wird bei der Aufnahme festgestellt, dass der Patient simuliert, ist eine Anzeige wegen Betrugsversuchs zulässig. Der Arzt darf beispielsweise auf Nachfrage der Strafverfolgungsbehörde auch mitteilen, dass ein Patient eine Krankheit simuliert hat, um eine Übernachtung zu erschleichen.

Aufgrund des hohen Stellenwertes des Persönlichkeitsschutzes in der Rechtsordnung muss der Arzt immer prüfen, in welchem Umfang er Daten offenbart. Dabei unterliegt schon der Umstand, dass jemand einen Arzt oder ein Krankenhaus aufsucht, wie auch die Anschrift des Patienten dem Geheimnisschutz.

Die Schweigepflicht gilt auch über den **Tod des Betroffenen** hinaus, § 203 Abs. 4 StGB. Erben oder Hinterbliebene sind nicht berechtigt, einen Arzt von der Schweigepflicht zu entbinden; die Schweigepflicht kann nur durch Entbindung seitens des Geheimhaltungsberechtigten, also regelmäßig des Patienten, gelöst werden. Der Arzt muss nach dem Tod eines Patienten seine Entscheidung, ob er Daten oder Informationen weitergibt, die seiner Schweigepflicht unterliegen, vom tatsächlichen – soweit er bekannt ist – sonst vom mutmaßlichen Willen des Verstorbenen abhängig machen. Der Arzt hat bei seiner gewissenhaften Prüfung, ob Anhaltspunkte dafür bestehen, dass der Verstorbene die ganze oder teilweise Offenlegung der Krankenunterlagen gegenüber seinen Hinterbliebenen beziehungsweise Erben mutmaßlich missbilligt haben würde, einen **Ermessensspielraum**. Bei der Erforschung des mutmaßlichen Willens des verstorbenen Patienten wird auch das Anliegen der die Einsicht begehrenden Personen eine entscheidende Rolle spielen, zum Beispiel Geltendmachung von Ansprüchen, Wahrung nachwirkender Persönlichkeitsbelange des Verstorbenen. Die Entscheidung kann der Arzt jedoch nur alleine treffen, weil er für die Entscheidung durch eine dritte Stelle zwangsläufig das Geheimnis erst preisgeben müsste, was ja gerade nur im Ausnahmefall geschehen soll.

Beispiele:

Ein Kind eines Verstorbenen möchte die Todesursache beziehungsweise die Ursache für eine Krankheit seiner Mutter oder seines Vaters wissen, weil es selbst an einer Krankheit leidet und eine erbliche Disposition vermutet. Dieses berechtigte Interesse erfordert jedoch keine Durchbrechung der ärztlichen Schweigepflicht. Hier könnte das Kind seine Krankheit dem Arzt mitteilen und ihn bitten zu prüfen, ob sie im Zusammenhang mit dem Tod oder einer Erkrankung des Elternteils steht, oder das Kind lässt sich vom Arzt des verstor-

benen Elternteils danach untersuchen, ob dessen Todesursache auch Ursache seiner Krankheit sein kann.

Mitunter sind Angaben zur Todesursache oder einer früheren Erkrankung von Bedeutung, wenn der Verstorbene eine Lebensversicherung abgeschlossen hatte und die Erben die Versicherungsleistung nur erhalten können, wenn der Versicherung besondere Umstände des Todes mitgeteilt werden. Auch bei einer solchen Konstellation muss der Arzt nicht immer die Todesursache mitteilen, mitunter kann beispielsweise eine Bestätigung ausreichend sein, dass eine natürliche Todesursache vorliegt. Im Übrigen muss die Versicherung auch mitteilen, welche Angaben konkret erforderlich sind. Wenn der Versicherungsvertrag bestimmte Leistungsausschlüsse enthält, so kann der Arzt aufgrund dieser Ausschlüsse entscheiden, welche Daten er mitteilt beziehungsweise wie weit er Tatsachen offenbart.

Wenn Angehörige die näheren Todesumstände ihres Verwandten wissen wollen, weil sie vermuten, dass ein Behandlungsfehler des Arztes zum Tod geführt hat und insoweit den hierfür Verantwortlichen seiner Strafe zuführen wollen, so kann der Arzt die entsprechende Auskunft oder die Einsicht in Behandlungsunterlagen mit Hinweis auf seine Schweigepflicht nicht verweigern.

Offenbarungspflicht

Die gesetzlich geregelten **Offenbarungspflichten** reichen nur soweit, wie der Gesetzeszweck es jeweils erfordert. Üblicherweise sind die zu offenbarenden Daten im Gesetz genannt. Weitere Daten dürfen dann nicht übermittelt werden.

Das Strafgesetzbuch enthält Anzeigepflichten zur Verbrechensverhinderung, die mit Einschränkungen auch für Ärzte gelten. Nach § 139 StGB wird ein Arzt nicht bestraft, wenn er eine Anzeige der geplanten Straftat seines Patienten unterlässt, sich aber ernsthaft bemüht hat, die Tat zu verhindern. Davon ausgenommen sind Mord und Totschlag, Völkermord, erpresserischer Menschenraub, Geiselnahme oder ein Angriff auf den Luftverkehr durch eine terroristische Vereinigung – solche Taten muss der Arzt immer anzeigen, wenn sie ihm in seiner Eigenschaft als Arzt bekannt geworden sind.

Meldegebote bestehen für Ärzte und in Krankenhäusern für den leitenden Arzt beziehungsweise den leitenden Abteilungsarzt für die in § 6 ff. IfSG bezeichneten Krankheiten. Anzeigepflichten und damit Offenbarungsgebote regelt ebenfalls das Personenstandsgesetz (PStG). Danach sind die Leiter von öffentlichen Krankenanstalten verpflichtet, Geburten und Todesfälle anzuzeigen, §§ 18, 34 PStG. Insoweit sind sie von der Schweigepflicht entbunden.

Der Landtag von Mecklenburg-Vorpommern hat 1998 ein Gesetz zur Ausführung des Krebsregistergesetzes beschlossen, das ein Meldegebot für Krebserkrankungen an das Krebsregister der fünf neuen Bundesländer und Berlins enthält. Im Krebsregister selbst werden die Daten pseudonymisiert gespeichert; ein etwaiger **Widerspruch** des Patienten gegen die Meldung an das Krebsregister ist unbeachtlich, § 2 Abs. 2 KrebsRAG MV.

Dokumentation

Neben der Pflicht zur Verschwiegenheit sind die Ärzte zur **Dokumentation** ihrer Behandlung verpflichtet. Die Dokumentationspflicht für Ärzte in Mecklenburg-Vorpommern ist in § 32 Nr. 5 HeilBerG M-V sowie in § 10 BOÄ M-V geregelt. Bei der Aufbewahrung und

Verwendung der Dokumentation sind **technische und organisatorische Maßnahmen** gemäß §§ 21, 22 DSGVO M-V für öffentliche Stellen beziehungsweise § 9 BDSG für nicht-öffentliche Stellen (z. B. niedergelassene Ärzte) zu beachten.

Die ärztliche Dokumentation ist in einer für den Fachmann hinreichend klaren Form abzufassen, es ist daher nicht notwendig, dass ein Laie sie ohne weiteres verstehen kann. Wesentliche Bestandteile der Dokumentation sind unter anderem: Anamnese, Diagnostik, Funktionsbefunde, Medikation, ärztliche Anordnungen zur Pflege, Operationsmethode, Lagerung auf dem OP-Tisch, Wechsel des Operateurs bei einem Eingriff, Maßnahmen der Intensivmedizin, Anfängerkontrolle bei Eingriff und Pflege, therapeutische Maßnahmen und deren Ergebnis, Sektionsergebnisse, Apparateinsatz, Nachbehandlung, Hinweis auf Gefahrenlagen und Vorbeugungen, Hinweise im Rahmen der therapeutischen Aufklärung zur Selbstbestimmung, Ratschläge zur Inanspruchnahme eines Spezialisten, Verweigerungen und Beschwerden des Patienten.

Landeskrankenhausesgesetz Mecklenburg-Vorpommern – LKHG M-V

Geltungsbereich

Gemäß § 2 Abs. 1 LKHG M-V gilt das Gesetz für alle Krankenhäuser im Land Mecklenburg-Vorpommern, die der allgemeinen stationären Versorgung dienen, soweit nichts anderes bestimmt ist. Einzelne Bereiche des LKHG M-V sind zwar für bestimmte Krankenhäuser, zum Beispiel Universitätskliniken, ausgenommen, jedoch gelten die datenschutzrechtlichen Bestimmungen des Dritten Abschnittes des LKHG M-V ausnahmslos auch für diese Krankenhäuser.

In allen Fragen des Patientendatenschutzes ist in erster Linie das LKHG M-V anzuwenden. Ergänzend gelten gemäß § 14 Abs. 2 LKHG M-V mit einigen Ausnahmen auch die Vorschriften des DSGVO M-V. Der Gesetzeshinweis auf die ergänzenden Vorschriften des DSGVO M-V weist jedoch eine Besonderheit auf:

Das Landesdatenschutzgesetz gilt gemäß § 2 DSGVO M-V für öffentliche Stellen des Landes, beispielsweise für Behörden und öffentlich-rechtliche Einrichtungen des Landes, der Landkreise und der Gemeinden. Als Krankenhausträger sind in der Regel freigemeinnützige, kommunale oder private Träger und das Land vorgesehen, § 1 Abs. 3 LKHG M-V. Diese Aufzählung macht deutlich, dass ein Krankenhaus nicht in jedem Fall in einer öffentlich-rechtlichen Trägerschaft geführt werden muss. Ist eine privat-rechtliche Trägerschaft gegeben, so findet das Landesdatenschutzgesetz keine Anwendung; für diesen Datenschutzbereich gilt vielmehr das Bundesdatenschutzgesetz. Die entsprechende Kontrollzuständigkeit obliegt in diesen Fällen nicht dem Landesbeauftragten für den Datenschutz, sondern der Datenschutzaufsichtsbehörde im Innenministerium des Landes. Hinzu kommt, dass für Krankenhäuser in kirchlicher Trägerschaft das jeweilige kirchliche Datenschutzrecht gilt; die Kontrollzuständigkeit liegt bei den kirchlichen Datenschutzbeauftragten.

Die datenschutzrechtliche Dreiteilung zwischen den öffentlichen, privaten und kirchlichen Stellen im Land und die damit verbundenen unterschiedlichen Kontrollkompetenzen hat der Gesetzgeber schlichtweg übersehen, als er den Verweis auf das LKHG M-V ergänzende Vorschriften ausschließlich auf das Landesdatenschutzgesetz beschränkte. Tatsächlich

genießen aber nicht nur die in öffentlich-rechtlichen Krankenhäusern behandelten Patienten einen über das LKHG M-V hinausgehenden Datenschutz. Für die Patienten von privaten und kirchlichen Krankenhäusern gelten die allgemeinen Datenschutzvorschriften des BDSG beziehungsweise des Kirchenrechts in entsprechender Weise, ohne dass ein Gesetzesverweis im LKHG M-V deren Anwendbarkeit regelt. Auch wenn sich dies nicht ausdrücklich aus dem LKHG M-V ergibt: Wegen der Gesetzssystematik, die das Verhältnis der speziellen, vorrangigen zu den allgemeinen, nachrangigen Regelungen bestimmt, finden in dem jeweiligen Bereich die allgemeinen Datenschutzvorschriften entsprechende Anwendung.

Entscheidend ist damit für die Beantwortung der Frage, welche allgemeinen Datenschutzvorschriften als Ergänzung zum LKHG M-V Anwendung finden, die **Rechtsform** desjenigen Trägers, der das Krankenhaus führt. Danach lässt sich dann auch feststellen, wer für die datenschutzrechtlichen Kontrollen und Beratungen zuständig ist.

Für **öffentlich-rechtliche Unternehmen** im Sinne des Landesdatenschutzgesetzes, die am Wettbewerb teilnehmen, gelten bei der Verarbeitung personenbezogener Daten die Vorschriften des BDSG und nur einige wenige des DSG M-V. Dies ist in § 2 Abs. 5 DSG M-V bestimmt. Für den Bereich der Krankenhäuser hat der Landesgesetzgeber dies jedoch ausdrücklich ausgeschlossen, indem er in § 14 Abs. 2 Satz 2 LKHG M-V regelte, dass § 2 Abs. 5 DSG M-V und damit das BDSG auf Krankenhäuser in Mecklenburg-Vorpommern keine Anwendung findet. Insoweit gelten auch für diese öffentlich-rechtlichen, am Wettbewerb teilnehmenden Krankenhäuser die nach § 14 Abs. 2 Satz 1 LKHG M-V zu berücksichtigenden Vorschriften des DSG M-V.

Mit der subsidiären Anwendung des DSG M-V unterliegt das Krankenhauspersonal im öffentlichen Bereich auch dem **Datengeheimnis** nach § 6 DSG M-V. Alle Beschäftigten, die Zugang zu Patientendaten haben, sind bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Sie dürfen mit diesen Daten nur zum Zweck der rechtmäßigen Erfüllung ihrer Aufgaben umgehen. Gleiches gilt für Beschäftigte eines Krankenhauses in privat-rechtlicher Trägerschaft: § 5 BDSG regelt das Datengeheimnis für diesen Bereich entsprechend.

Nach dem DSG M-V sind die öffentlich-rechtlichen Krankenhäuser verpflichtet, bei **automatisierter Verarbeitung** der Patientendaten für jedes der von ihnen eingesetzten Datenverarbeitungsverfahren ein Verzeichnis anzulegen und auf dem neuesten Stand zu halten, § 18 DSG M-V. Auf Anforderung sind diese Verzeichnisse dem Landesbeauftragten für den Datenschutz M-V zu übermitteln. In vollem Umfang hat ein Krankenhaus auch die erforderlichen **technischen und organisatorischen Maßnahmen** vorzusehen, um die Einhaltung der Datenschutzvorschriften sicherzustellen und die Rechte der Betroffenen zu gewährleisten, §§ 21, 22 DSG M-V. Ähnliches gilt nach dem BDSG auch im privaten Bereich, jedoch mit einigen Besonderheiten, §§ 4d, 4e, 9 BDSG.

Jeder in einem öffentlich-rechtlich geführten Krankenhaus behandelte Patient kann sich nach dem DSG M-V an den Landesbeauftragten für den Datenschutz wenden, wenn er annimmt, bei der Verarbeitung seiner Patientendaten in seinen Rechten verletzt worden zu sein, § 26 DSG M-V. Der Landesdatenschutzbeauftragte kann Verstöße gegen datenschutzrechtliche Bestimmungen oder nicht ausreichende technische oder organisatorische Maßnahmen zum Patientendatenschutz beanstanden und die Beseitigung von Mängeln fordern, § 32 DSG M-V.

Entsteht bei unzulässiger oder unrichtiger automatisierter Verarbeitung der Patientendaten ein Schaden, so ist das Krankenhaus zum **Schadensersatz** verpflichtet, § 27 DSGVO M-V. Im privat-rechtlichen Datenschutzbereich können sich die betroffenen Patienten gemäß § 38 BDSG mit ihren Sorgen und Fragen zu der Verarbeitung ihrer Daten im Krankenhaus an das Innenministerium Mecklenburg-Vorpommern als zuständige Datenschutzaufsichtsbehörde wenden. Ein Schadensersatzanspruch besteht für diese Patienten selbstverständlich auch im Bereich des BDSG, § 7 BDSG.

§ 14 Anwendungsbereich und Begriffsbestimmungen

§ 14 Abs. 1 LKHG M-V

Im Krankenhaus verarbeitete Patientendaten unterliegen unabhängig von der Art ihrer Verarbeitung dem Datenschutz. Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten eines Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.

Nach Satz 1 ist das **Recht auf informationelle Selbstbestimmung** nicht davon abhängig, wie die Patientendaten verarbeitet werden: Ob also automatisiert oder nicht automatisiert – sie unterliegen in jedem Fall datenschutzrechtlichen Bestimmungen. Es ist auch unerheblich, ob die Daten als Bildaufzeichnungen oder als maschinell erstellte Diagramme oder nach anderen Verfahren gespeichert sind.

Der im Datenschutzrecht sonst übliche Begriff der „personenbezogenen Daten“ wird in diesem Bereich durch Satz 2 eingegrenzt und durch Satz 3 erweitert. Die Eingrenzung kommt durch die Verwendung des Begriffs „**Patientendaten**“ zum Ausdruck. Es muss sich folglich um eine Person handeln, die sich als Patient im Krankenhaus aufhält, damit die Bestimmungen dieses Gesetzes anwendbar sind. Der Umstand, dass jemand einen Arzt oder ein Krankenhaus als Patient aufgesucht hat, fällt ebenso wie Name, Anschrift und Telefonnummer eines Patienten grundsätzlich auch unter den Geheimnisschutz des § 203 StGB.

Die Erweiterung des Begriffs „Patientendaten“ wird dadurch deutlich, dass nicht nur die personenbezogenen Daten des Betroffenen (Patienten) dazugehören, sondern auch die **Daten von Dritten**, wenn sie eine bestimmte Beziehung zum Patienten haben, zum Beispiel Name, Anschrift oder Telefonnummer eines Angehörigen oder einer Bezugsperson. Diese Daten unterliegen den datenschutzrechtlichen Vorschriften und somit auch dem § 42 DSGVO M-V, der die unbefugte Verarbeitung der geschützten Daten unter Strafe stellt. Jedoch unterliegen die Daten des Angehörigen beziehungsweise der Bezugsperson nicht automatisch der Schweigepflicht des § 203 Abs. 1 StGB. Das wäre nur dann der Fall, wenn sie als Geheimnis zu qualifizieren wären, beispielsweise wenn es sich hierbei auch um Daten über gesundheitliche Verhältnisse handelt.

Daten von Dritten, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden, sind ebenfalls Patientendaten; zum Beispiel Daten einer Person, die die Krankheit beim Patienten ausgelöst hat (wie Träger von Krankheitserregern). Weil es sich hier um Daten über gesundheitliche Verhältnisse des Dritten handelt, unterliegen sie darüber hinaus auch der ärztlichen Schweigepflicht.

Ähnlich der Definition der personenbezogenen Daten handelt es sich nach Satz 2 nur dann um **Patientendaten**, wenn Einzelangaben einem bestimmten oder einem bestimmbar Patienten zugeordnet werden können. Sind Daten mit dem Namen eines Patienten verbunden, so ist dieser Patient bestimmt, mithin sind dies Patientendaten. Sind Einzelangaben beispielsweise mit einer Patientennummer (oder Krankenversicherungsnummer u. dgl.) verbunden, so ist der Patient hierüber bestimmbar, und es handelt sich ebenfalls um Patientendaten.

Die Abgrenzung zwischen Patientendaten und Daten, die nicht Patientendaten sind, bereitet in der Praxis häufig Schwierigkeiten, vor allem wenn man bedenkt, dass bei bestimmten Konstellationen und oberflächlichem Aufbau einer Statistik schon aus **aggregierten Daten** auf Personen geschlossen werden kann. Erstellt beispielsweise ein Krankenhaus eine **Statistik**, in der unter anderem das Geburtsjahr eines 100-jährigen Patienten mit weiteren Daten über seine Gesundheit angegeben ist, ist es möglich, den Patienten zu bestimmen, insbesondere dann, wenn bereits Daten über ihn veröffentlicht wurden, wie Gratulation zum 100. Geburtstag in der Regionalpresse. Gerade bei statistischen Daten ist deshalb besonderer Wert darauf zu legen, dass einzelne Patienten nicht bestimmbar sind. Am einfachsten wird das dadurch erreicht, dass in einer Merkmalsklasse eine genügend große Anzahl von Fällen – mindestens drei – enthalten ist. In unserem Fall könnte der 100-jährige Patient in einer Merkmalsklasse aufgenommen werden, die alle Patienten enthält, die älter als 80 Jahre sind – vorausgesetzt, dass in dieser Klasse mehr als drei Patienten enthalten sind. Möglich wäre es auch, nicht das Geburtsjahr für Statistiken zu verwenden, sondern Geburtsjahrgänge zum Beispiel in Zehn-Jahres-Stufen zusammenzufassen.

Bei der weiteren Betrachtung der Patientendaten ist es sinnvoll, wenn man sie in **medizinische Daten** und in **Verwaltungsdaten** gliedert, da hiernach die wesentlichen **Zugangs- und Zugriffsbeschränkungen** ausgerichtet werden müssen. Sicherlich lässt sich diese Trennung nicht durchgängig realisieren – es wird auch immer Überschneidungen geben – der Schutz der Patientendaten wird aber so der jeweiligen Aufgabenerfüllung besser angepasst und sinnvoll gewährleistet. Des Weiteren ist zu berücksichtigen, dass die **medizinische Dokumentation** eine ganz andere Zielstellung hat, als diejenige der Verwaltungstätigkeit. Die medizinische Dokumentation dient im Wesentlichen der Darstellung und Aufbewahrung von Angaben zur Anamnese, zu den Befunden, zur Diagnose und zu den Behandlungsmaßnahmen, während die von der Verwaltung benötigten Patientendaten zum Beispiel für **Abrechnungszwecke** mit der Krankenversicherung oder der sozialen oder seelsorgerischen Betreuung erforderlich sind.

§ 14 Abs. 2 LKHG M-V

Ergänzend zu den Vorschriften dieses Gesetzes über die Verarbeitung von Patientendaten gelten die Vorschriften des Landesdatenschutzgesetzes vom 28. März 2002 (GVOBl. M-V S. 154) mit der Ausnahme des § 25 Abs. 3 des Landesdatenschutzgesetzes und mit der Maßgabe, dass an die Stelle der §§ 4 und 7 Abs. 1 bis 4, der §§ 8 bis 10, des § 13 Abs. 2 bis 5 und der §§ 14, 15, 24 und 34 des Landesdatenschutzgesetzes die Vorschriften dieses Gesetzes treten. § 2 Abs. 5 des Landesdatenschutzgesetzes findet auf Krankenhäuser keine Anwendung.

Der Patientendatenschutz ist im LKHG M-V nicht abschließend geregelt. Aus diesem Grund weist Absatz 2 darauf hin, dass für die Verarbeitung von Patientendaten die Vorschriften des DSGVO M-V mit den dort genannten Ausnahmen gelten. Diese Ausnahmen sind damit begründet, dass es für diese Regelungen im LKHG M-V spezialgesetzliche Normen

gibt und die Vorschriften des DSG M-V insoweit ergänzende Funktionen haben. Die folgende Übersicht stellt den Zusammenhang zwischen den ausgenommenen Regelungen des DSG M-V und den dafür anzuwendenden spezialgesetzlichen Regelungen dar:

Bei Patientendaten nichtgeltende Regelungen des Datenschutzgesetzes M-V	Spezialgesetzliche Regelungen des Krankenhausgesetzes M-V
§ 4 Verarbeitung von personenbezogenen Daten im Auftrag	§ 21 Datenverarbeitung im Auftrag
§ 7 Absätze 1 bis 4 Grundsatz	§ 15 Abs. 1 Erforderlichkeit, Erlaubnisvorbehalt, Einwilligung (letzter Halbsatz)
§ 8 Einwilligung	§ 15 Abs. 2 Einwilligung
§ 9 Erheben	§ 15 Abs. 1 Nummern 1 bis 3 Erheben für bestimmte Aufgaben
§ 10 Nutzen	§ 16 Abs. 1 Nutzen und Übermitteln von Daten im Krankenhaus
§ 13 Absätze 2 bis 5 Berichtigen, Sperren, Löschen	§ 19 Löschung und Sperrung von Daten
§ 14 Übermittlung an Stellen innerhalb des öffentlichen Bereichs	§ 16 Absätze 2 und 3 Übermittlung innerhalb des Krankenhauses
§ 15 Übermittlung an inländische nicht-öffentliche Stellen	§ 17 Übermittlung an Stellen außerhalb des Krankenhauses
§ 24 Auskunft, Akteneinsicht	§ 18 Auskunft und Akteneinsicht
§ 34 Wissenschaftliche Forschung	§ 20 Datenverarbeitung für Forschungszwecke

In Satz 2 ist normiert, dass § 2 Abs. 5 DSG M-V auf Krankenhäuser keine Anwendung findet. Diese Norm enthält besondere Bestimmungen für **öffentlich-rechtliche Unternehmen**, die am Wettbewerb teilnehmen. Für diese Unternehmen gelten nur bestimmte Normen des DSG M-V und ergänzend die Regelungen für nicht-öffentliche Stellen des BDSG. Obwohl öffentlich-rechtlich geführte Krankenhäuser auch öffentlich-rechtliche Wettbewerbsunternehmen sind, sind diese Einschränkung des DSG M-V und der genannte Teil des BDSG wegen § 14 Abs. 2 LKHG M-V nicht anzuwenden.

Der Verweis in § 14 Abs. 2 LKHG M-V auf das DSG M-V deckt jedoch nur den Bereich ab, in dem es um die Datenverarbeitung in einem Krankenhaus eines öffentlich-rechtlichen Trägers geht. Wie bereits ausgeführt, ist das Landesdatenschutzgesetz für den nicht speziell im LKHG M-V geregelten Datenschutzteil nur auf öffentlich-rechtliche Stellen des Landes anwendbar. Hinsichtlich der privatrechtlich geführten Krankenhäuser gilt das Bundesdatenschutzgesetz und somit beispielsweise §§ 4f, 4g, 5, 9, 35 Abs. 1 BDSG. Siehe zur gesamten Problematik Seite 12.

§ 15 Erheben und Speichern von Daten

§ 15 Abs. 1 LKHG M-V

Patientendaten dürfen nur erhoben und gespeichert werden, soweit dies erforderlich ist

1. zur Erfüllung des mit dem Patienten oder zu seinen Gunsten abgeschlossenen Behandlungsvertrages, einschließlich der Erfüllung der ärztlichen Dokumentationspflicht und der Pflegedokumentation,
2. zur sozialen und seelsorgerischen Betreuung des Patienten nach § 11, wenn eine Einwilligung wegen offenkundiger Hilflosigkeit oder mangelnder Einsichtsfähigkeit nicht eingeholt werden kann und der mutmaßliche Wille des Patienten nicht entgegensteht,
3. zur Leistungsabrechnung und Abwicklung von Ansprüchen, die mit der Behandlung im Zusammenhang stehen,

oder soweit dieses Gesetz oder eine andere Rechtsvorschrift dies vorschreibt oder erlaubt oder der Patient im Einzelfall eingewilligt hat.

In Absatz 1 werden die Grundsätze beim **Erheben** und **Speichern** als besondere Formen des Verarbeitens genannt. Patientendaten dürfen nur erhoben und gespeichert werden, wenn und soweit dies für einen **bestimmten Zweck** erforderlich ist (**Erforderlichkeit, Zweckbindungsgebot**). Bei den Patientendaten, die dem medizinischen Bereich zuzuordnen sind, hängt die Einschätzung, ob sie zur Behandlung erforderlich sind, im Wesentlichen vom behandelnden Arzt ab. Die Daten müssen jedoch grundsätzlich mit der aktuellen Behandlung in einem Zusammenhang stehen. Beispielsweise kann eine umfassende Familienanamnese dann erforderlich sein, wenn die Diagnostik oder die Therapie von erblichen Dispositionen beeinflusst wird. Hingegen dürfte es aus medizinischer Sicht an einer Erforderlichkeit der Datenerhebung fehlen, wenn bei einem Krankenhausaufenthalt wegen einer Meniskusoperation Daten über Erkrankungen in der Familie erhoben werden oder solche, die eine lange zurückliegende Fraktur eines Fingers betreffen, die normal und ohne Komplikationen verheilt ist.

Es gibt aber auch Patientendaten, bei denen die Erforderlichkeit des Erhebens durch Rechtsvorschrift festgeschrieben ist. Beispielsweise müssen bestimmte Daten eines in der gesetzlichen **Krankenkasse** versicherten Patienten an die Krankenkasse übermittelt werden (§ 301 SGB V). Sofern diese Daten nicht bereits im Zusammenhang mit der Behandlung erhoben wurden, ist dies zum Zweck der gesetzlich vorgeschriebenen (erforderlichen) Übermittlung nachzuholen.

Die wesentlichen Zwecke, für die Daten – soweit erforderlich – erhoben werden dürfen, sind in den Nummern 1 bis 3 genannt.

Gemäß **Nummer 1** dürfen Patientendaten zur Erfüllung des **Behandlungsvertrages** erhoben werden. Dazu gehören im weiteren Sinne alle mit der Behandlung zusammenhängenden Daten, wobei der Vertrag selbst in der Regel nur wenige enthält. Es ist eine Berufspflicht eines Arztes bzw. seiner Gehilfen, die ärztliche Behandlung und Pflege zu dokumentieren. Für die Behandlung und Dokumentation müssen Patientendaten erhoben und gespeichert werden (siehe Seite 11).

In der Gesetzesbegründung wird darauf verwiesen, dass **Behandlung** in diesem Sinne auch Aufnahmediagnostik, Konsiliararztstätigkeit sowie die Begutachtung ist, soweit nicht andere gesetzliche Vorschriften gelten. Es ist allerdings fraglich, ob diese sehr weitgehende Definition medizinrechtlich und datenschutzrechtlich haltbar ist. Beispielsweise muss ein Arzt den Patienten über die Behandlung aufklären, dies trifft auch für die Hinzuziehung

eines Konsiliars zu. Der Patient hat jedoch ein **Widerspruchsrecht** und kann auch eine Behandlung ablehnen. Wenn der Patient die Hinzuziehung eines Konsiliars ablehnt, darf der behandelnde Arzt auch keine Patientendaten an diesen Arzt übermitteln. Ist der Patient hingegen über die weiteren Maßnahmen informiert worden, und hat er diesen nicht widersprochen, so bedarf es keiner zusätzlichen und förmlichen Einwilligung zur Datenübermittlung (konkludente Einwilligung).

Nummer 2 nennt als weitere Aufgaben, für die Daten erhoben und gespeichert werden dürfen, die **soziale und die seelsorgerische Betreuung** des Patienten. Diese Datenerhebung ist aber von der Einwilligung des Patienten beziehungsweise von seinem mutmaßlichen Willen abhängig. Im Grunde genommen ist zur Erfüllung der Aufgabe nur die Angabe eines Datums erforderlich, und zwar für den Zweck der seelsorgerischen Betreuung, ob und welcher Religionsgemeinschaft der Patient angehört. Alle weiteren hierfür möglicherweise erforderlichen Daten liegen dem Krankenhaus ohnehin vor (z. B. Name, Adresse, Aufenthaltsort im Krankenhaus und – soweit erforderlich – das Alter). An die Einwilligung zur Datenerhebung und -speicherung für diesen Zweck sind allerdings keine hohen formalen Anforderungen zu stellen. Da es im Falle der Hilflosigkeit des Patienten als ausreichend erachtet wird, insbesondere die Speicherung vom mutmaßlichen Willen abhängig zu machen, sollte die Erhebung auf freiwilliger Basis erfolgen. Der Zweck der Erhebung muss dem Patienten wie bei jeder anderen Datenerhebung erläutert werden (z. B. § 9 Abs. 3 DSGVO M-V). Die reine Abfrage der Religionsgemeinschaft würde den datenschutzrechtlichen Normen nicht entsprechen. So sind die Patienten darauf hinzuweisen, dass bei einer entsprechenden Angabe die erforderlichen Daten an den Krankenhausesseelsorger dieser Religionsgemeinschaft zur seelsorgerischen Betreuung übermittelt werden. Wenn ein Angehöriger einer Religionsgemeinschaft keine seelsorgerische Betreuung wünscht, so sollte keine entsprechende Angabe gemacht werden. Selbstverständlich kann der Patient diese Entscheidung jederzeit wieder zurücknehmen und das Krankenhauspersonal um die Vermittlung seelischen Beistandes bitten.

Es sollte jedoch auch möglich sein, dass ein Patient, der keiner Religionsgemeinschaft angehört, auf seinen Wunsch hin von einem Seelsorger seiner Wahl betreut wird. Der Wille des Patienten müsste dann mit den weiteren erforderlichen Daten übermittelt werden.

Zum Zweck der sozialen Betreuung ist lediglich die Erhebung und Speicherung des Willens des Patienten notwendig. In der weiteren Folge können, wie bei der seelsorgerischen Betreuung, die erforderlichen Daten an den sozialen Betreuer übermittelt werden.

Nach **Nummer 3** ist die Datenerhebung und -speicherung zur **Leistungsabrechnung** und Abwicklung von Ansprüchen zulässig. Danach darf beispielsweise der Patient um Angaben gebeten werden, die sich auf seine **Krankenversicherung** beziehen – also, ob und welche gesetzliche oder private Krankenversicherung besteht, ob er Selbstzahler ist oder ob ein Sozialleistungsträger (Sozialamt) die Behandlungskosten übernimmt. Aus diesen Angaben ergeben sich in der Regel weitere erforderliche Daten, wie die Krankenversicherungsnummer und dergleichen.

Treten während der Behandlung weitere Ansprüche auf, so können die zu ihrer Abwicklung notwendigen Daten erhoben werden. Hierbei kann es sich sowohl um Ansprüche des Patienten gegenüber dem Krankenhaus (z. B. auf Schadensersatz wegen eines ärztlichen Kunstfehlers) als auch um Ansprüche des Krankenhauses gegenüber dem Patienten (z. B. Erfüllung der vertraglichen Pflichten, wie Bezahlung von Wahlleistungen) handeln.

Über die genannten Aufgaben hinaus erlauben Rechtsvorschriften auch in weiteren Fällen das **Erheben** und **Speichern** von Patientendaten, beispielsweise nach dem Personenstandsgesetz bei der Geburt eines Kindes (siehe hierzu auch ärztliche Offenbarungsbefugnisse und -pflichten, Seiten 9 bis 11). Daneben ist das Erheben und Speichern von Patientendaten zulässig, wenn der Patient im Einzelfall eingewilligt hat. Die Einwilligung muss für den betroffenen Patienten immer als eine freie Willensentscheidung erkennbar sein. Ein Zwang zur Abgabe einer Einwilligung ist mit dem **Recht auf informationelle Selbstbestimmung** nicht vereinbar. Die Einwilligungserklärung muss dies gebührend berücksichtigen.

§ 15 Abs. 2 LKHG M-V

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Vor der Einwilligung ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über Art und Umfang der Verarbeitung und Nutzung der Daten, bei einer beabsichtigten Übermittlung auch über den Empfänger der Daten, aufzuklären und darauf hinzuweisen, dass die Einwilligung verweigert oder mit Wirkung für die Zukunft widerrufen werden kann. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Patient hierauf besonders hinzuweisen. Ist der Patient aus tatsächlichen oder rechtlichen Gründen nicht in der Lage, die Einwilligung zu erteilen, ist die Erklärung im Wege gesetzlicher Vertretung oder, wenn eine solche nicht vorhanden ist, durch Angehörige abzugeben.

Dieser Absatz regelt die **Einwilligung** in die Verarbeitung von Patientendaten. Von der geforderten **Schriftform** kann abgewichen werden, wenn besondere Umstände vorliegen, beispielsweise wenn der Patient wegen einer Verletzung nicht in der Lage ist, seinen Willen schriftlich darzulegen. In solchen Fällen reicht auch eine mündliche Einwilligung. In jedem Fall (schriftlich oder mündlich) muss die Einwilligung dokumentiert werden; wo, richtet sich nach ihrem Zweck. Eine Einwilligung in die Verarbeitung und Nutzung von Patientendaten, die der ärztlichen Schweigepflicht unterliegen, wird zweckmäßigerweise auch in der ärztlichen Dokumentation aufbewahrt.

Welche weiteren Forderungen die Einwilligung zu erfüllen hat, normiert insbesondere Satz 2. So ist der Patient vorher über die Bedeutung der Einwilligung in geeigneter Weise aufzuklären. Wie dies konkret zu geschehen hat, ist im Wesentlichen von ihrem Zweck, vom Umfang der Daten und nicht zuletzt auch davon abhängig, ob und wie der Betroffene den Sinn und die Reichweite seiner Erklärung erfassen kann. So ist die Verwendung einer **Patienteninformation** (Merkblatt) durchaus ein geeignetes Mittel zur Aufklärung, wenn in die Verwendung bestimmter Patientendaten zu Forschungszwecken eingewilligt werden soll. In anderen Fällen kann die Aufklärung in Form eines **Arzt-Patienten-Gesprächs** geeignet sein.

Die Einwilligung muss stets hinreichend bestimmt sein, das heißt, allgemeine Formulierungen, ohne über die Art und den Umfang der Verarbeitung und Nutzung oder – bei beabsichtigter Übermittlung – über den Empfänger der Daten aufzuklären, erfüllen nicht diese gesetzlichen Vorgaben. In jedem Fall ist darauf hinzuweisen, dass die Einwilligung freiwillig ist. Die **Freiwilligkeit** kann man noch betonen, indem der Betroffene den Hinweis erhält, dass er bei einer Verweigerung keine nachteiligen Folgen zu befürchten hat (Hinweis: Bei der Beantragung von Sozialleistungen kann eine Verweigerung der Einwilligung zur Folge haben, dass eine Leistung ganz oder teilweise versagt oder entzogen werden kann. Der Betroffene ist auf diese Folge hinzuweisen. Siehe § 66 SGB I).

Der Betroffene ist des Weiteren darauf hinzuweisen, dass die Einwilligung mit Wirkung für die Zukunft widerrufen werden kann. Sind seine Daten bis zu diesem **Widerruf** bereits verarbeitet und genutzt worden, so kann dies nicht mehr rückgängig gemacht werden. Die Stelle darf diese Patientendaten aber künftig nicht mehr verwenden, sie sind deshalb umgehend zu **löschen**. Ob auch der Widerruf dokumentiert werden muss, hängt davon ab, wie die Daten bereits verarbeitet und genutzt worden sind. Aus datenschutzrechtlicher Sicht ist es immer vorzuziehen, wenn bei einem Widerruf keine „Datenspuren“ über einen Betroffenen bestehen bleiben, wenn also die Einwilligung und die gespeicherten Daten gelöscht werden und der Widerruf nicht aufbewahrt wird. Sind die Daten jedoch schon genutzt und beispielsweise in einer Statistik verarbeitet worden, so kann es nach dem Löschen der Patientendaten erforderlich sein, dass die Einwilligung und der Widerruf aufbewahrt werden, um beispielsweise die Nutzung der nun nicht mehr personenbezogenen Daten zu dokumentieren.

Häufig werden Einwilligungen zusammen mit anderen Erklärungen, Hinweisen oder Informationen abgefordert. In solchen Fällen ist ausdrücklich darauf aufmerksam zu machen, dass es sich um eine Einwilligung handelt, damit der Betroffene beispielsweise mit dem „Kleingedruckten“ nicht etwas unterschreibt, ohne die Tragweite seiner Unterschrift zu erkennen. Die Einwilligung muss sich deshalb vom übrigen Text oder anderen Erklärungen im Schriftbild unterscheiden beziehungsweise hervorgehoben sein.

In Satz 4 ist schließlich geregelt, dass die Einwilligung durch einen gesetzlichen Vertreter oder einen Angehörigen abgegeben werden kann, wenn der Patient nicht in der Lage ist, sie zu erteilen. Dies kann zum Beispiel der Fall sein, wenn der Patient sich mit anderen Personen nicht verständigen kann oder bewusstlos ist (tatsächlicher Grund). Sobald der Patient sich wieder verständlich machen kann, sollte er zur Wahrnehmung seines **Rechts auf informationelle Selbstbestimmung** darüber informiert werden, dass ein Angehöriger für ihn in eine bestimmte Verarbeitung seiner Patientendaten eingewilligt hat. Dadurch wird es ihm möglich, die Verarbeitung und Nutzung seiner Daten zu widerrufen, wenn dieses nicht in seinem Interesse ist.

Rechtliche Gründe, welche eine Einwilligung nicht wirksam werden lassen, können gegeben sein, wenn es sich um ein Kind handelt, das noch nicht die für eine Einwilligung erforderliche **Einsichtsfähigkeit** besitzt. Unabhängig davon, ob eine Einwilligung juristisch gesehen eine rechtsgeschäftliche Willenserklärung im Sinne der §§ 104 ff. BGB oder eine Realhandlung ist, kann man davon ausgehen, dass analog § 104 Nr. 1 BGB bzw. § 828 Abs. 1 BGB ein Kind bis zu sieben Jahren die Einsichtsfähigkeit noch nicht besitzt. Dann ist die Einwilligung von den Eltern oder einem gesetzlichen Vertreter zu erteilen. Bei älteren Kindern muss jeweils im Einzelfall entschieden werden. Besitzt ein Kind die Einsichtsfähigkeit, kommt es auf den Willen der Eltern nicht mehr an. Weitere rechtliche Gründe können die Vertretung des Patienten durch einen Vormund (§§ 1773 ff. BGB) oder die Interessenwahrnehmung durch einen Betreuer (§§ 1896 ff. BGB) oder Pfleger (§§ 1909 ff. BGB) sein. Auch hier ist aber in erster Linie auf die Einsichtsfähigkeit des Patienten abzustellen.

§ 15 Abs. 3 LKHG M-V

Patientendaten dürfen, soweit sie nicht durch andere Stellen nach Maßgabe des § 21 im Auftrag verarbeitet oder an andere Stellen nach Maßgabe des § 17 übermittelt werden, als automatisierte Dateien nur auf Datenträgern gespeichert und durch Datenverarbeitungssysteme und Programme verarbeitet werden, die der ausschließlichen Verfügungsgewalt des Krankenhauses unterliegen.

Durch diese Rechtsvorschrift will der Gesetzgeber verhindern, dass Patientendaten auf Datenverarbeitungsanlagen oder mit Programmen verarbeitet werden, die nicht der ausschließlichen **Verfügungsgewalt** des Krankenhauses unterliegen. Abgesehen von der Auftragsdatenverarbeitung und der zulässigen Datenübermittlung ist es danach beispielsweise unzulässig, Patientendaten auf einem Rechner oder mit Programmen zu verarbeiten, die sich zwar im Krankenhaus befinden, aber während der Verarbeitung nicht seiner Verfügungsgewalt unterliegen. Dies könnte der Fall sein, wenn eine andere Stelle oder ein Unternehmen dem Krankenhaus Hard- oder Software zur Verfügung stellt, sich jedoch eigene Aktivitäten auf diesem Rechner oder mit den Programmen vorbehält oder sie durchführt. Da dann immer zu befürchten ist, dass auch Patientendaten zweckentfremdet verarbeitet oder genutzt werden, muss die Verfügungsgewalt darüber beim Krankenhaus verbleiben. Es ist jedoch durchaus zulässig, dass ein Krankenhaus Hardware mietet. Voraussetzung ist allerdings, dass die Datenverarbeitung auf dieser Anlage ausschließlich nach der Weisung des Krankenhauses erfolgt.

Sonderfälle in dieser Hinsicht stellen die **Wartung** und die **Pflege** von Datenverarbeitungsanlagen und Programmen dar. Sofern diese Tätigkeiten durch fremde Unternehmen ausgeführt werden, ist es unter Umständen nicht ausgeschlossen, dass dabei vorübergehend Patientendaten von der Wartungsfirma verarbeitet werden. Zur Wartung und Fernwartung haben die Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe herausgegeben (siehe Anhang).

Patientendaten dürfen auch nicht auf privaten Datenträgern gespeichert werden. Zudem ist auch aus Gründen der Datensicherheit und insbesondere wegen der Einschleppung von Computerviren die Verwendung privater Datenträger oder -rechner zu vermeiden. Eine Ausnahme zu dieser Regelung besteht bei der Verarbeitung und Nutzung von Patientendaten durch einen Arzt gemäß § 20 Abs. 6 LKHG M-V.

§ 16 Nutzen und Übermitteln von Daten im Krankenhaus

§ 16 Abs. 1 LKHG M-V

Patientendaten dürfen für die Zwecke genutzt werden, für die sie nach § 15 Abs. 1 erhoben worden sind. Darüber hinaus dürfen sie nur genutzt werden, soweit dies erforderlich ist für

1. die Geltendmachung von Ansprüchen des Krankenhauses sowie zur Abwehr von Ansprüchen oder die Verfolgung von Straftaten oder Ordnungswidrigkeiten,
2. Planungszwecke und Wirtschaftlichkeits- und Organisationsuntersuchungen,
3. die im Krankenhaus durchgeführte Aus-, Fort- und Weiterbildung in ärztlichen oder anderen Fachberufen des Gesundheitswesens,
4. Forschungszwecke gemäß § 20,

soweit der Zweck nicht mit anonymisierten Daten erreicht werden kann.

Die **Zweckbindung** ist ein wesentlicher datenschutzrechtlicher Grundsatz, der in allen Phasen der Verarbeitung personenbezogener Daten gilt und in Bezug auf Patientendaten

hier noch einmal betont wird. Die Zweckbindung der Daten geht auf die Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 im so genannten Volkszählungsurteil zurück. Das Gericht hat dort ausgeführt: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“

Falls eine Nutzung von Patientendaten für andere Zwecke uneingeschränkt erlaubt wäre, könnte genau der Fall eintreten, dass ein Patient nicht mehr überschauen kann, wer was wann über ihn weiß. Patientendaten dürfen deshalb nur für die Zwecke genutzt werden, für die sie zulässigerweise erhoben worden sind (§ 15 Abs. 1 LKHG M-V).

Nach Satz 2 dürfen Patientendaten auch für die Geltendmachung von Ansprüchen des Krankenhauses, für Planungszwecke oder Wirtschaftlichkeits- und Organisationsuntersuchungen, für Aus-, Fort- und Weiterbildungsmaßnahmen in ärztlichen oder Gesundheitsberufen oder für Forschungszwecke genutzt werden, allerdings nur dann, wenn diese Aufgaben nicht mit anonymisierten Daten erfüllt werden können. Kommt das Krankenhaus bei einer Prüfung zu dem Ergebnis, dass Patientendaten erforderlich sind, so sollte bei der Beteiligung anderer als der datenspeichernden Stelle geprüft werden, ob nicht auch zumindest **pseudonymisierte Daten** ausreichen. Anhand pseudonymisierter Daten ist der Patient zwar bei der Daten speichernden Stelle jederzeit zu bestimmen, der anderen Stelle ist dies aber nicht ohne weiteres möglich. Als Pseudonym könnte im einfachsten Fall die Patientennummer unter der Voraussetzung verwendet werden, dass die andere Stelle aus ihr keine Person bestimmen kann, weil sie beispielsweise nicht über die entsprechende Zuordnungstabelle zwischen Patientennummer und Name/Anschrift verfügt.

Im Übrigen sollten bei der Kommunikation mit anderen Stellen generell pseudonymisierte Patientendaten genutzt werden, um das Risiko der Verletzung von Persönlichkeitsrechten des betroffenen Patienten gering zu halten. Beispielsweise kann bei der Inanspruchnahme von **Labordienstleistungen** auf die Übermittlung identifizierender Daten verzichtet und statt dessen ein Datensatz verwendet werden, der es nur der behandelnden Abteilung im Krankenhaus ermöglicht, die Ergebnisse dem Patienten zuzuordnen. Dieses Verfahren kann mit technischer Unterstützung sehr sicher gestaltet werden, so dass Zuordnungsfehler auszuschließen sind (z. B. Verwendung von Strichcodes mit der dazugehörigen Infrastruktur). Auch bei der Nutzung der **Telemedizin** ist die Verwendung pseudonymisierter Daten angebracht, denn vielfach diskutieren Mediziner ohnehin fallbezogen, das heißt, ohne identifizierende Daten zu übermitteln oder auszutauschen. Bei Verwendung pseudonymisierter Daten ist für beide Seiten die gleiche Sicherheit hinsichtlich der Integrität der Daten und hinsichtlich der Revision gegeben wie bei identifizierenden Patientendaten.

Nach **Nummer 1** können Patientendaten für die **Geltendmachung von Ansprüchen** des Krankenhauses sowie zur Abwehr von Ansprüchen oder für die Verfolgung von Straftaten oder Ordnungswidrigkeiten genutzt werden, soweit diese Aufgaben nicht mit **anonymisierten** Daten erreicht werden. Hierbei geht es nicht um Ansprüche eines bestimmten Patienten gegen das Krankenhaus oder um Ansprüche des Krankenhauses gegen einen bestimmten Patienten bzw. die Abwehr der jeweiligen Ansprüche. Solche Aufgaben lassen sich kaum mit anonymisierten Daten lösen. Vielmehr muss es sich um Ansprüche handeln, die nur mittelbar die Beziehung Krankenhaus – Patient betreffen. Ein Beispiel in diesem Sinne ist der so genannte Herzklappenskandal, bei dem Ärzte zu hohe Kosten abgerechnet und im Gegenzug von den Herstellern dieser Mittel Provisionen erhalten haben sollen. Liegt hier eine Straftat oder Ordnungswidrigkeit vor, so ist diese zweifellos mit Patienten-

daten verbunden. Die Patienten, die solche Herzklappen erhielten, hatten jedoch daraus weder einen Vorteil, noch mussten sie Nachteile befürchten. Zur Feststellung, in wie vielen Fällen unkorrekt abgerechnet worden ist, sind keine Patientendaten erforderlich. Dazu reichen anonymisierte Daten prinzipiell aus. Ob und in welchem Umfang Patientendaten für diesen Zweck genutzt werden dürfen, richtet sich aber entscheidend nach der Fragestellung. Wenn Einzelfälle belegt werden müssen, ist die Nutzung von Patientendaten nicht zu umgehen. Es könnte beispielsweise sein, dass die geschädigte **Krankenkasse** nachweisen muss, in welchen Fällen nicht korrekt abgerechnet wurde, damit das Gericht die Schadenssumme ermitteln kann. Mit diesem Nachweis wäre auch eine Datenübermittlung von der Krankenkasse an das Gericht verbunden. Diese Datenübermittlung ist aber nach den speziellen Übermittlungsvorschriften des Sozialgesetzbuches zu beurteilen (SGB V, SGB X). Darüber hinaus kann das Gericht auch das Krankenhaus auffordern, entsprechende Patientendaten zu übermitteln, um vergleichen zu können, ob der Krankenkasse bei der entsprechenden Abrechnung tatsächlich ein Schaden entstanden ist.

Gemäß **Nummer 2** können Patientendaten für **Planungszwecke** sowie **Wirtschaftlichkeits- und Organisationsuntersuchungen** genutzt werden, soweit diese Zwecke nicht mit anonymisierten Daten zu erreichen sind. In aller Regel sollten dafür aber anonymisierte Daten ausreichend sein. Es lässt sich zwar nicht immer ausschließen, dass beispielsweise bei einer Organisationsuntersuchung Patientendaten als Quelle genutzt werden, jedoch ist die weitere Auswertung überwiegend ohne Daten, mit denen ein Patient bestimmbar ist, möglich – siehe hierzu auch Absatz 4.

Für Aus-, Fort- und Weiterbildungszwecke in ärztlichen und anderen Fachberufen des Gesundheitswesens werden in der Regel keine personenbezogenen Patientendaten benötigt. Zulässig ist ihre Nutzung daher nur, wenn anderenfalls der jeweilige Zweck nicht erreicht werden kann.

Für Forschungszwecke können Patientendaten unter den Voraussetzungen des § 20 LKHG M-V genutzt werden (siehe Seite 38).

§ 16 Abs. 2 LKHG M-V

Krankenhausmitarbeiter dürfen Patientendaten nur für den zu ihrer jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck übermitteln.

Dieser Absatz stellt bei der **Datenübermittlung durch Krankenhausmitarbeiter** auf die rechtmäßige Aufgabenerfüllung und die Zweckbindung ab. Ist beispielsweise einem Mitarbeiter die Aufgabe übertragen worden, Krankenhausleistungen bei Krankenkassen abzurechnen, so darf er die dazu erforderlichen Patientendaten übermitteln. Außerhalb seiner Aufgabenerfüllung ist diese Datenübermittlung nicht zulässig. So darf ein Mitarbeiter, der ausschließlich für die Leistungsabrechnung mit gesetzlichen Krankenkassen zuständig ist, keine medizinischen Daten an einen nachbehandelnden Arzt übermitteln. Ob und in welchem Umfang Daten für eine Nachbehandlung eines Patienten übermittelt werden, muss der behandelnde Krankenhausarzt entscheiden. Diese Entscheidung kann nicht von einem Krankenhausarzt getroffen werden, der an der Behandlung unbeteiligt war, denn der würde keine Kenntnis darüber haben, ob der Patient mit der Nachbehandlung bei dem anfordernden Arzt überhaupt einverstanden war und dort in Behandlung ist.

Krankenhausmitarbeiter dürfen auch nur aufgrund einer ausdrücklichen Rechtsgrundlage oder auf der Basis einer freiwilligen Entscheidung des Patienten dessen Daten übermitteln.

Im Falle der Abrechnung mit gesetzlichen Krankenkassen ist die anzuwendende Übermittlungsvorschrift § 301 SGB V. Bei einer Datenübermittlung für eine Nachbehandlung kommt es auf die konkludente Einwilligung des Patienten an (siehe § 17 LKHG M-V).

§ 16 Abs. 3 LKHG M-V

Für die Übermittlung von Patientendaten zwischen Behandlungseinrichtungen verschiedener Fachrichtungen in einem Krankenhaus (Fachabteilungen, medizinische Bereiche, Institute) gilt § 17 Abs. 1 entsprechend.

Dieser Absatz regelt speziell die Übermittlung von Patientendaten zwischen verschiedenen Fachabteilungen in einem Krankenhaus und verweist auf die zwölf Aufgaben in § 17 Abs. 1, nach denen eine solche Datenübermittlung zulässig ist. Verkürzt könnte man hierzu feststellen, dass unter denselben Voraussetzungen, nach denen eine Übermittlung an Stellen außerhalb des Krankenhauses zulässig ist, auch Patientendaten innerhalb eines Krankenhauses übermittelt werden dürfen. Der Gesetzgeber hat damit gleichfalls festgelegt, dass innerhalb eines Krankenhauses eine unbeschränkte Übermittlung von Patientendaten nicht zulässig ist. Diese Vorschrift kann deshalb auch als eine krankenhauserne Abkottung der Patientendaten angesehen werden.

In der Regel werden die Patientenunterlagen von der mit- oder nachbehandelnden Abteilung angefordert. Der behandelnde Arzt dieser Abteilung muss letztlich auch entscheiden, welche Daten er benötigt. Allerdings sind derartige Zugriffe auf die Unterlagen entsprechend zu protokollieren, um die Datennutzung nachvollziehbar zu machen. Dies ergibt sich ebenso aus den berufsrechtlichen **Dokumentationspflichten**. Dabei spielt es grundsätzlich keine Rolle, ob es sich um konventionelle Patientenakten handelt oder um elektronische. Unterschiedlich ist nur die Art der Protokollierung (siehe Seite 11).

Zu beachten ist vor allem, dass der Patient über eine solche **Datenübermittlung** zu informieren ist und ihr nach § 17 Abs. 1 Nr. 2 LKHG M-V auch **widersprechen** kann. Eine ausdrückliche Einwilligung ist hingegen nicht erforderlich. Es reicht vielmehr aus, dass der Patient von der ursprünglich behandelnden Abteilung darauf hingewiesen wird, dass es erforderlich oder zu empfehlen ist, eine andere Abteilung hinzuzuziehen. Ist der Patient mit der eigentlichen Mit- oder Nachbehandlung einverstanden, so ist davon auszugehen, dass er damit auch in die dafür erforderliche Datenübermittlung einwilligt.

In **Notfällen**, wenn der Patient zum Beispiel aufgrund von Bewusstlosigkeit oder Ähnlichem nicht von einer notwendigen Mit- oder Nachbehandlung informiert werden kann, ist zu diesem Zweck auch die Datenübermittlung zulässig. Dies gilt allerdings dann nicht, wenn ein ausdrücklicher oder mutmaßlicher entgegenstehender Wille des Patienten, beispielsweise in Form einer für diesen Zweck beim Krankenhaus oder einer anderen Stelle oder Person hinterlegten **Patientenverfügung**, bekannt ist. Bestimmte Notfalldaten sollten ohnehin für den ärztlichen Zugriff jederzeit zur Verfügung stehen.

§ 16 Abs. 4 LKHG M-V

Sofern Patientendaten aus dem medizinischen Bereich durch die Verwaltung oder andere nichtmedizinische Stellen im Krankenhaus für Zwecke nach Absatz 1 Nr. 2 genutzt werden, darf dies grundsätzlich nur mit anonymisierten Daten geschehen. Im Einzelfall dürfen Patientendaten zur Vermeidung mehrfacher Erhebung derselben Daten zusammengeführt werden, wenn sie vorher mit Ausnahme einer Kennziffer anonymisiert worden sind. Nach

der Zusammenführung der Datensätze sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, zu löschen.

In diesem Absatz ist die **Nutzung** von Patientendaten aus dem medizinischen Bereich durch die Verwaltung oder andere nichtmedizinische Stellen des Krankenhauses für Planungszwecke sowie Wirtschaftlichkeits- und Organisationsuntersuchungen speziell geregelt. Patientendaten aus dem medizinischen Bereich sind bei der Nutzung zu diesen Zwecken grundsätzlich **zu anonymisieren**. Nur wenn bei einer Planung oder bei einer Wirtschaftlichkeits- oder Organisationsuntersuchung bereits vorhandene Patientendaten erneut erhoben werden müssten, dürfen beispielsweise solche des medizinischen Bereiches mit denen des Verwaltungsbereiches zusammengeführt werden, wenn sie vorher mit Ausnahme einer Kennziffer anonymisiert worden sind. Nach der Zusammenführung sind die Daten zu löschen, mit denen ein **Patientenbezug** wiederhergestellt werden kann. Wenn beispielsweise über die Kennziffer ein Patientenbezug herstellbar ist, so muss sie nach der Zusammenführung gelöscht werden. Es kann aber auch durchaus sein, dass sich nach der Zusammenführung der Daten neue Kombinationsmöglichkeiten für die Herstellung eines Patientenbezuges ergeben. Dies ist zu prüfen, und gegebenenfalls sind die entsprechenden Daten zu aggregieren oder zu löschen. Da gerade für Planungszwecke oder für Wirtschaftlichkeitsuntersuchungen Daten häufig an andere Stellen weitergegeben werden, ist die Anonymisierung dieser Daten von besonderer Bedeutung.

Mit dieser Rechtsvorschrift wird die allgemeinere Vorschrift des Absatzes 1 Nr. 2 für den Verwaltungsbereich oder andere nichtmedizinische Stellen in der Weise weiter untersetzt, dass Daten aus dem medizinischen Bereich für diesen Zweck nur anonymisiert genutzt werden dürfen. Sofern es im medizinischen Bereich aber unerlässlich ist, für Planungszwecke oder für Wirtschaftlichkeits- oder Organisationsuntersuchungen mit Patientendaten umzugehen, so wäre dies nach Absatz 1 Nr. 2 hingegen zulässig.

§ 17 Übermitteln an Stellen außerhalb des Krankenhauses

§ 17 Abs. 1 LKHG M-V

Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ist nur zulässig, soweit dies erforderlich ist

1. zur Erfüllung des Behandlungsvertrages,
2. zur Durchführung einer Mit- oder Nachbehandlung, soweit der Patient nichts anderes bestimmt hat,
3. zur Abwehr einer gegenwärtigen Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Patienten oder Dritter, wenn diese Rechtsgüter das Geheimhaltungsinteresse des Patienten wesentlich überwiegen,
4. zur Unterrichtung von Angehörigen oder anderen Bezugspersonen, für die Übermittlung medizinischer Daten jedoch nur, falls die Einwilligung des Patienten nicht rechtzeitig erlangt werden kann, kein gegenteiliger Wille kundgetan wurde oder sonstige Anhaltspunkte dafür bestehen, dass eine Übermittlung nicht angebracht ist,
5. zur Erfüllung einer Behandlungspflicht oder einer gesetzlich vorgeschriebenen Mitteilungspflicht, soweit diese der ärztlichen Schweigepflicht vorgeht,
6. zu Forschungszwecken nach Maßgabe des § 20,
7. zur Durchsetzung von Ansprüchen aus dem Behandlungsvertrag,
8. zur Feststellung der Leistungspflicht der Kostenträger und zur Abrechnung mit diesen,
9. zur Rechnungsprüfung durch den Krankenhausträger, einen von ihm beauftragten Wirtschaftsprüfer oder den Landesrechnungshof und zur Überprüfung der Wirtschaftlichkeit

durch Beauftragte im Rahmen des § 113 SGB V und des Pflegesatzverfahrens nach der Bundespflegesatzverordnung,

10. zur sozialen und seelsorgerischen Betreuung des Patienten nach Maßgabe der §§ 11 und 15,
11. zur Bearbeitung von Patientenbeschwerden,
12. zur Durchführung qualitätssichernder Maßnahmen, soweit der Zweck nicht mit anonymisierten Daten erreicht werden kann und das öffentliche Interesse an der Durchführung der Maßnahme die Patientenschutzrechte wesentlich überwiegt.

Die Übermittlung von Patientendaten an Stellen oder Personen innerhalb oder außerhalb eines Krankenhauses stellt eine **Offenbarung eines Privatgeheimnisses** dar (§ 203 StGB). § 17 ist eine Rechtsvorschrift, nach der eine solche Offenbarung zulässig sein kann. Voraussetzung ist, dass die **Übermittlung** für die enumerativ genannten Zwecke **erforderlich** ist. Konkret bedeutet dies, dass **vor** jeder Übermittlung geprüft werden muss, ob eine Aufgabe nicht auch ohne Patientendaten erfüllbar ist, zum Beispiel mit anonymisierten Daten. Nur wenn diese Prüfung ergibt, dass die Aufgabe ausschließlich mit Patientendaten erfüllt werden kann, ist deren Übermittlung zulässig. In einem zweiten Schritt ist zu prüfen, welche Patientendaten konkret für die Aufgabenerfüllung erforderlich sind. Die Tiefe der Prüfungsschritte richtet sich selbstverständlich danach, ob und wie konkret die Datenübermittlung in anderen gesetzlichen Rechtsgrundlagen geregelt ist. Wenn beispielsweise Patientendaten an eine gesetzliche Krankenkasse übermittelt werden sollen, so ist für den Fall der Leistungsabrechnung in § 301 SGB V klar geregelt, welche Daten zu übermitteln sind. Die Prüfung kann dann darauf beschränkt sein, dass vor der Übermittlung untersucht wird, ob die bereitgestellten Daten mit dem Datenkatalog des § 301 SGB V übereinstimmen. Die Erforderlichkeit ist durch die Rechtsvorschrift gegeben, und der Umfang der zu übermittelnden Daten ergibt sich aus dem Katalog.

Auf welchem **Übertragungsweg** Patientendaten gegebenenfalls übermittelt werden können, ist nur in Ausnahmefällen geregelt, wie in § 301 Abs. 1 SGB V – maschinenlesbar. Das Krankenhaus muss in den nicht näher geregelten Fällen einen Weg wählen, der eine der Sensibilität der Daten entsprechende Sicherheit bietet. Dabei kann nicht pauschal gesagt werden, auf welche Art und Weise zulässige Datenübermittlungen erfolgen sollten. Folgende Faktoren spielen jedoch eine entscheidende Rolle:

- die Sensibilität der zu übermittelnden Daten (Grundsatz: je sensibler desto sicherer der Übertragungsweg),
- die Dringlichkeit der Übermittlung (Grundsatz: je dringlicher die Übermittlung z. B. zur Lebenserhaltung ist, desto eher sind Abstriche von der Sicherheit der Übertragungswege denkbar).

In Abhängigkeit von beiden Faktoren muss jeweils im Einzelfall entschieden werden, welche Art der Übermittlung von Patientendaten notwendig und ausreichend ist, um jeweils ein angemessenes Niveau der Datensicherheit zu gewährleisten.

Weit verbreitete Praxis ist es, Patientendaten per **Telefax** zu übermitteln. Dies ist zwar eine sehr bequeme und schnelle Art der Übertragung, birgt aber aus Sicht des Datenschutzes auch Gefahren. Zum einen kann nicht sichergestellt werden, dass auf der Empfängerseite nur der wahre Adressat Kenntnis von den übermittelten Patientendaten erlangt. Faxgeräte befinden sich oft an zentralen Orten von Behörden oder Unternehmen. Da die Faxe offen ankommen, kann potentiell eine Vielzahl von Personen Einsicht in die Sendungen nehmen, ohne dass der Absender irgendeine Möglichkeit der Einflussnahme hat. Bei der Übermitt-

lung auf dem Postwege können Daten zielgenauer an den einzelnen Empfänger gerichtet werden. Das Risiko einer unbefugten Einsichtnahme ist zwar auch hier nicht ausgeschlossen, aber es ist wesentlich geringer.

Zum anderen ist die Gefahr von Fehlleitungen eines Telefaxes wesentlich höher als bei einer Übermittlung auf dem Postwege. So kann es passieren, dass versehentlich eine falsche Telefaxnummer eingegeben wird. Moderne Telefaxgeräte haben zudem in der Regel eine Vielzahl von Stationstasten zur Speicherung häufig gewählter Anschlüsse. Wird versehentlich die falsche Taste gedrückt, kommen die Patientendaten beim falschen Empfänger an und die Kenntnisnahme durch Unbefugte ist unvermeidbar. Derartige Fälle mögen zwar abwegig klingen, kommen aber in der Praxis durchaus vor. So sind beispielsweise Patientendaten versehentlich an den Landesbeauftragten für den Datenschutz übermittelt worden, da die Faxnummer des Krankenhauses eine ähnliche Zahlenfolge wie die Telefon-/Faxnummer des Datenschutzbeauftragten hatte.

Fazit dieser Überlegungen ist, dass auf eine Übermittlung von Patientendaten per Telefax verzichtet werden sollte. Vielmehr empfiehlt sich die Übermittlung auf dem Postwege, die wesentlich sicherer und zielgenauer ist und in der Regel auch nur einen Tag dauert. Gleiches gilt auch für die Datenübermittlung innerhalb des Krankenhauses. Handelt es sich um derart dringende Fälle, dass jede andere Form der Übermittlung aufgrund ihrer Dauer ausscheidet, ist selbstverständlich auch eine Datenübermittlung per Telefax zulässig.

Bei Übermittlungen auf dem Wege der Telekommunikation sollten die Daten kryptographisch verschlüsselt übertragen werden. In jedem Falle sind Datenübermittlungen in der Patientenakte zu protokollieren.

Im Folgenden wird beispielhaft erläutert, wie Patientendaten zu den in Absatz 1 genannten Zwecken und soweit dies erforderlich ist übermittelt werden können:

Nummer 1

Der **Behandlungsvertrag** (Krankenhausaufnahmevertrag) ist eine zweiseitige Vereinbarung zwischen dem Patienten und dem Krankenhausträger. Behandlungsverträge werden in der Regel mit allen Krankenhauspatienten geschlossen. Es kommt nicht darauf an, wer die Behandlungskosten übernimmt. Folglich werden solche Verträge mit gesetzlich und privat versicherten Patienten, mit Selbstzahlern und mit Sozialhilfeempfängern geschlossen. Mit dem Vertrag wird ein bürgerlich-rechtliches Rechtsverhältnis begründet. Der Patient erwirbt damit einen unmittelbaren Anspruch auf sachgemäße Behandlung. Der Krankenhausträger verpflichtet sich, eine Gesamtleistung des Krankenhauses zu erbringen. Diese setzt sich aus ärztlichen Leistungen, Pflege, Verpflegung, Unterkunft und Nebenleistungen zusammen.

Eine eventuell erforderliche Datenübermittlung für ärztliche Leistungen ist insbesondere in Nummer 2 geregelt (Mit- oder Nachbehandlung). Eine Übermittlung von Patientendaten könnte sich danach auf die Teilbereiche Pflege, Verpflegung, Unterkunft oder Nebenleistungen erstrecken. Ob sie für diese Aufgaben tatsächlich erforderlich ist, muss stets im Einzelfall geprüft werden. Auch eine regelmäßige Datenübermittlung an den Krankenhausträger als Vertragspartner ist nicht notwendig.

Im Unterschied zum Krankenhausaufnahmevertrag ist die Rechtsbeziehung eines Krankenhauses zu einer Krankenkasse öffentlich-rechtlicher Natur (§§ 107 ff. SGB V).

Nummer 2

Die Übersendung eines **Arztbriefes** an den Hausarzt zur Nachbehandlung ist der klassische Fall der Datenübermittlung nach dieser Befugnisnorm. Allerdings ist darauf zu achten, dass die Versendung des Arztbriefes nicht zum Automatismus wird. Der Patient muss gefragt werden, ob er mit einer Nachbehandlung durch einen bestimmten Arzt einverstanden ist, beziehungsweise ist über die erforderliche Nach- oder Mitbehandlung durch einen bestimmten Arzt aufzuklären. Sofern dann der Patient dieser Behandlung nicht widerspricht, dürfen die erforderlichen Daten übermittelt werden. Eine ausdrückliche Einwilligung dazu ist nicht erforderlich.

Die Datenübermittlung zur **Mit- oder Nachbehandlung** ist auch der wesentliche Fall, der durch § 16 Abs. 3 eröffnet wird. So dürfen auch zwischen Fachabteilungen eines Krankenhauses Patientendaten nur übermittelt werden, wenn der Patient über eine Mitbehandlung aufgeklärt wurde und nichts anderes bestimmt hat (datenschutzrechtlich handelt es sich dann um eine konkludente Einwilligung).

Unzulässig wäre eine Datenübermittlung nach dieser Rechtsvorschrift allerdings, wenn der Patient über eine Mit- oder Nachbehandlung erst vom mit- oder nachbehandelnden Arzt erfährt. Die konkludente Einwilligung würde dann nicht vorliegen, da die Daten bereits übermittelt worden sind, ohne dass der Patient dies beeinflussen konnte. Die Einwilligung muss immer vor der Datenübermittlung erteilt werden.

Nummer 3

Die Zulässigkeit einer derartigen Datenübermittlung ist bereits in der Einleitung unter dem Stichwort „Offenbarungsbefugnis“ behandelt worden (siehe Seite 9). Gemäß § 34 StGB ist ein Arzt befugt, der Geheimniswahrung unterliegende Tatsachen Dritten mitzuteilen, wenn dadurch eine **Gefahr** für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut abgewendet werden kann. Als Beispiel ist die Mitteilung einer HIV-Infektion genannt worden. In Fortführung dieses Beispiels ist es zulässig, einen mitbehandelnden Arzt einer anderen Fachabteilung über die AIDS-Erkrankung eines Patienten zu informieren, damit dieser Maßnahmen gegen eine mögliche Ausbreitung der Krankheit bei Dritten treffen kann (§ 16 Abs. 3 i. V. m. § 17 Abs. 1 Nr. 3). Gleiches gilt für die Übermittlung an einen nachbehandelnden Arzt – die Datenübermittlung ist dann gemäß § 17 Abs. 1 Nr. 3 und unter der Voraussetzung der Nr. 2 zulässig.

Nach einer **Rechtsgüterabwägung** ist auch die Frage zu entscheiden, ob und in welchem Umfang der Arzt/das Krankenhaus eine Misshandlung eines Kindes offenbaren darf. Wenn sich im Ergebnis einer ärztlichen Untersuchung der Verdacht einer Misshandlung manifestiert, darf der Arzt im Interesse des Kindes das Jugendamt oder die Polizei informieren. Der Arzt oder das Krankenhaus würde sich dadurch nicht der Gefahr der Strafverfolgung wegen Offenbarung eines Privatgeheimnisses aussetzen.

Nummer 4

Diese Übermittlungsvorschrift dürfte in der Praxis häufig Anwendung finden. **Angehörige** oder Bezugspersonen des Patienten wollen beispielsweise wissen, wo sich der Patient im Krankenhaus befindet, um ihn besuchen zu können. Der Patient sollte allerdings bei der Aufnahme gefragt werden, ob über seinen Aufenthalt im Krankenhaus bei Nachfrage eines Besuchers an der Pforte Auskunft gegeben werden darf (Pfortnerliste). Eine besondere Einwilligung ist nicht erforderlich, sondern lediglich die Willensentscheidung des Patienten. Wenn sich der Patient gegen eine solche Auskunftserteilung ausgesprochen hat, bedeutet dies jedoch nicht, dass kein Besucher zu ihm vorgelassen werden darf, denn der

Patient kann selbst Besucher über seinen Krankenhausaufenthalt informieren. Soweit der Patient keine Besuche wünscht, kann ein entsprechendes Vorgehen nur auf der Behandlungsstation geklärt werden.

Bei der Übermittlung medizinischer Daten an einen Angehörigen oder eine Bezugsperson gelten strengere Maßstäbe. Für diese Daten ist eine Einwilligung erforderlich, und somit sind die Vorschriften des § 15 Abs. 2 anwendbar. Ist ein Patient nicht in der Lage einzuwilligen, so muss der behandelnde Arzt prüfen, ob ein gegenteiliger Wille des Patienten oder andere Anhaltspunkte vorliegen, die gegen eine Übermittlung der Daten sprechen. Ohne Einwilligung des Patienten beziehungsweise Prüfung seines Willens durch den Arzt dürfen auch Angehörige oder Bezugspersonen keine Daten über den Krankheitszustand erhalten. **Notfälle** können allerdings von der tiefgehenden Prüfung des Patientenwillens ausgenommen werden. Auch im Interesse der Angehörigen sollte ihnen dann der Gesundheitszustand kurz beschrieben werden.

Die telefonische Übermittlung von Patientendaten sollte die Ausnahme sein und nur in Betracht kommen, wenn der Empfänger ausreichend sicher identifizierbar ist.

Nummer 5

Eine Behandlungspflicht liegt regelmäßig in **Not- oder Unglücksfällen** vor. Diese Pflicht kann auch bestehen, wenn ein Patient von einem anderen Arzt in ein Krankenhaus eingewiesen wird. Dann hat der Krankenhausaufnahmekrankenarzt den Patienten zu untersuchen. Kommt er zu dem Ergebnis, dass eine sofortige Krankenhausbehandlung nicht erforderlich ist, so kann er unter weiteren Voraussetzungen (fehlendes Vertrauensverhältnis, Querulanten etc.), insbesondere wenn die Behandlung an einer anderen Stelle ebenso möglich ist, diese ablehnen.

Stellt der Krankenhausarzt bei einem Notfall fest, dass ein anderes Krankenhaus besser für die Behandlung geeignet ist, so kann er den Patienten – unter Berücksichtigung seines Zustandes – dorthin überweisen. Die für die weitere Behandlung erforderlichen Daten dürfen nach dieser Rechtsvorschrift dem anderen Krankenhaus zur Erfüllung der Behandlungspflicht übermittelt werden.

Gesetzliche Mitteilungspflichten, die der Schweigepflicht vorgehen, bestehen

- bei bestimmten übertragbaren Krankheiten nach den §§ 6 und 7 IfSG,
- bei Abwendung eines geplanten schweren Verbrechens nach § 138 StGB,
- nach Maßgabe des § 100 SGB X (eingeschränkte Auskunftspflicht eines Arztes an Sozialleistungsträger),
- bei Krebserkrankungen nach § 2 Krebsregisterausführungsgesetz M-V sowie
- beim Tod eines Patienten nach § 6 BestattG M-V und § 34 PStG.

Nummer 6

Soweit die Nutzung von Patientendaten für **Forschungszwecke** zulässig ist, dürfen sie auch an andere Stellen übermittelt werden. Weiteres wird dazu unter § 20 LKHG M-V ausgeführt.

Nummer 7

Solche Übermittlungen können notwendig sein, wenn eine Vertragspartei ihre vertraglichen Verpflichtungen nicht oder nicht vollständig erfüllt. Beispiele sind:

Ein Patient beansprucht **Schadensersatz**. Zur Erfüllung oder Abwehr der Ansprüche kann es erforderlich sein, dass Patientendaten an eine Haftpflichtversicherung, an den Krankenhausträger oder auch an ein Gericht übermittelt werden.

Macht ein Patient falsche Angaben über seine Krankenversicherung, so kann das Krankenhaus Daten an den Krankenhausträger oder auch an ein Gericht übermitteln, um die Bezahlung der erbrachten Leistung durchzusetzen. In einem solchen Fall sollte dem Patienten jedoch vor der Übermittlung eine Frist eingeräumt werden, innerhalb der ein möglicherweise doch bestehender Krankenversicherungsschutz nachgewiesen werden kann.

Nummer 8

In der gesetzlichen **Krankenversicherung** stellt das Krankenhaus vor beziehungsweise während einer Krankenhausbehandlung bei der Krankenkasse des Patienten einen **Antrag auf Übernahme der Kosten**. Die Kasse kann so prüfen, ob der Patient krankenversichert und ob die Behandlung notwendig ist (§ 27 SGB V). Bei einer positiven Entscheidung hat das Krankenhaus die Gewähr, dass die Leistung vergütet wird. Nach erfolgter Behandlung kann das Krankenhaus eine Rechnung stellen und die in § 301 SGB V bezeichneten Daten an die Krankenkasse übermitteln.

Für die Feststellung der Leistungspflicht anderer Kostenträger sind die Vorschriften des Sozialgesetzbuches nicht maßgebend. Deshalb wurde diese Übermittlungsregelung in das Landeskrankenhausgesetz aufgenommen. Danach ist es beispielsweise zulässig, die zu diesem Zweck erforderlichen Daten eines Patienten, der Sozialhilfeleistungen erhält, an das Sozialamt als dem zuständigen Kostenträger zu übermitteln.

Bei Privatpatienten kann eine Übermittlung an die private Krankenversicherung erforderlich sein, da häufig auch hier eine Kostenübernahmeerklärung in den Vertragsbedingungen festgelegt ist. Bei Selbstzahlern ist diese Vorschrift nicht anwendbar, da sich der Vergütungsanspruch für die Behandlung direkt an die Patienten richtet.

Nummer 9

Diese Rechtsvorschrift soll trotz der Pflicht zur Verschwiegenheit über ärztliche Behandlungen die **Rechnungsprüfung** gewährleisten. Der Krankenhausträger oder ein von ihm bestellter Wirtschaftsprüfer darf die für diesen Zweck erforderlichen, konkret bezeichneten Patientendaten erhalten. Es ist dem Rechnungsprüfer allerdings unbenommen, den gewünschten Datenkatalog im Laufe der Prüfung zu präzisieren beziehungsweise zu erweitern.

Auch die Krankenkassen und die Krankenhausträger können einvernehmlich bestellte Prüfer beauftragen, die Wirtschaftlichkeit, Leistungsfähigkeit und Qualität der zugelassenen Krankenhäuser zu untersuchen (§ 113 SGB V). Diesen Prüfern sind ebenfalls die erforderlichen und von ihnen bezeichneten Patientendaten zu übermitteln.

Nummer 10

Die wesentlichen Voraussetzungen zum Umgang mit Patientendaten für diesen Zweck wurden bereits bei der Datenerhebung erläutert. Hat ein Patient solche Daten auf freiwilliger Basis angegeben oder entspricht eine soziale oder seelsorgerische Betreuung seinem mutmaßlichen Willen, so dürfen die entsprechenden Daten an einen Sozialarbeiter oder Seelsorger übermittelt werden (siehe die Erläuterungen zu § 15 LKHG M-V, Seite 16).

Nummer 11

Wenn sich ein Patient bei einer anderen Stelle über seine Krankenhausbehandlung beschwert, so kann es notwendig sein, dieser Stelle die zur Bearbeitung erforderlichen Patientendaten zu übermitteln. Durch die **Beschwerde** willigt der Patient konkludent darin ein, dass die andere Stelle sein Anliegen bearbeitet. Einer gesonderten ausdrücklichen Einwilligung bedarf es daher nicht. Mit dem Umfang seiner Beschwerde gibt er den Umfang der zu übermittelnden Daten vor, der für die Bearbeitung dieser Beschwerde erforderlich ist (siehe dazu auch Seite 8).

Nummer 12

Um einen bundeseinheitlichen Standard bei der **Qualitätssicherung** zu erreichen, wurde eine Servicestelle Qualitätssicherung (SQS) beim Deutschen Krankenhausinstitut (DKI) eingerichtet. Die für diesen Zweck benötigten Daten sollen die Krankenhäuser auf vorgegebenen Formularen anonym an SQS übermitteln. Hier sind in der Praxis jedoch Defizite zu beobachten. So sind zu den einzelnen Behandlungsfällen häufig derart detaillierte Angaben zu machen, dass ein Personenbezug gerade in kleineren Häusern ohne weiteres herstellbar ist. Dazu folgendes Beispiel: In einer Datei zur Qualitätssicherung der neonatologischen Behandlung werden Geburtstag, Geschlecht, Uhrzeit der Geburt, Postleitzahl des Wohnortes abgefragt.

In solch einem Falle kann von einer Anonymisierung kaum noch gesprochen werden. Deshalb sollte das Krankenhaus bei jeder Datenübermittlung zur Qualitätssicherung kritisch prüfen, ob diese einzelnen Daten tatsächlich dafür erforderlich sind oder ob auch aggregierte Daten ausreichen, so dass bereits vom Krankenhaus zusammengefasste Daten übermittelt werden. Im genannten Beispiel könnte es statt der genauen Geburtszeit etwa genügen, nur zu übermitteln, ob die Geburt vormittags, nachmittags oder nachts stattfand, falls diese Daten überhaupt erforderlich sind.

Müssen in Ausnahmefällen zu diesem Zweck Patientendaten genutzt werden, so sollte die zuständige oberste Aufsichtsbehörde prüfen, ob das öffentliche Interesse die Patientenschutzrechte wesentlich überwiegt.

§ 17 Abs. 2 LKHG M-V

Personen oder Stellen, denen nach diesem Gesetz Patientendaten übermittelt werden, dürfen diese nur zu dem Zweck verwenden, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung der Daten durch diese Personen oder Stellen an Dritte bedarf der Zustimmung des Krankenhauses. Im Übrigen haben sie diese Daten unbeschadet sonstiger Datenschutzbestimmungen in demselben Umfang geheim zu halten wie das Krankenhaus selbst.

Die Rechtsvorschrift betont die generell zu beachtende **Zweckbindung** der befugt übermittelten Patientendaten beim Empfänger. Eine Verwendung der Daten zu anderen Zwecken durch den Empfänger ist nicht zulässig. Dieses datenschutzrechtliche Grundprinzip beruht auch auf dem Volkszählungsurteil des Bundesverfassungsgerichts und soll sicherstellen, dass die Patientendaten nicht so genutzt werden, dass der betroffene Patient nicht mehr überschauen kann, wer was wann über ihn weiß. Die Datenverwendung muss für den Betroffenen nachvollziehbar sein (**Transparenzgebot**).

Sollte es dennoch notwendig sein, dass der Datenempfänger die Daten zu anderen Zwecken nutzen möchte, so ist dies nur mit Zustimmung des Krankenhauses zulässig. Auch

dann gilt, dass die Daten über eine zugestimmte **Zweckänderung** hinaus nicht für weitere Zwecke verwendet werden dürfen.

Das Krankenhaus sollte zudem auch Patientendatenübermittlungen und Zustimmungen zur Verwendung zu anderen Zwecken dokumentieren, damit die Datenflüsse nachvollziehbar und transparent bleiben (siehe hierzu auch § 18 LKHG M-V).

Dem Datenempfänger ist darüber hinaus auferlegt, die Daten im selben Umfang geheim zu halten wie das Krankenhaus. Folglich müssen beim Datenempfänger auch geeignete **technische und organisatorische Maßnahmen** vorhanden sein, um einen Missbrauch der Daten zu vermeiden.

Wenn der Datenempfänger die Patientendaten so aufbereitet, dass ein Patient nicht mehr bestimmbar ist, zum Beispiel durch Aggregation, so können sie ohne Einschränkungen genutzt oder auch veröffentlicht werden. Es ist aber darauf zu achten, dass tatsächlich aus diesen Daten kein Patient mehr bestimmt werden kann. Insbesondere ist zu bedenken, dass auch Statistiken nicht in jedem Fall als anonym gelten können.

§ 17 Abs. 3 LKHG M-V

Soweit die Vorschriften dieses Gesetzes auf die Datenempfänger keine Anwendung finden, ist eine Übermittlung in den Fällen des Absatzes 1 nur zulässig, wenn die Empfänger sich zur Einhaltung der Vorschriften des Absatzes 2 verpflichten. Im Falle einer Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes gilt § 16 des Landesdatenschutzgesetzes entsprechend.

Bei einer befugten **Datenübermittlung** muss das Krankenhaus einen Datenempfänger, für den die Vorschriften des LKHG M-V nicht gelten, verpflichten, die Zweckbindung der Daten einzuhalten. Dies ist vor allem dann bedeutsam, wenn der Umgang mit den Daten beim Datenempfänger nicht gesetzlich geregelt ist. Werden zum Beispiel Patientendaten zu **Forschungszwecken** nach Abs. 1 Nr. 6 an eine Stelle übermittelt, auf die die Vorschriften des LKHG M-V nicht anwendbar sind, muss sie sich entsprechend verpflichten. Andererseits muss eine gesetzliche Krankenkasse nicht verpflichtet werden, wenn ihr Daten nach Abs. 1 Nr. 8 und § 301 SGB V übermittelt werden, da für Krankenkassen der Umgang mit den Daten im SGB V und X gesondert geregelt ist.

Patientendaten dürfen an Stellen außerhalb des Geltungsbereiches des Grundgesetzes befugt übermittelt werden. Dies kann beispielsweise notwendig sein, wenn der Kostenträger für die Krankenhausbehandlung eine ausländische Stelle ist. In diesem Fall ist neben dieser Rechtsvorschrift im LKHG M-V der § 16 DSGVO M-V bzw. § 4b BDSG entsprechend anzuwenden. Es muss dabei geprüft werden, ob die weiteren, dort genannten Zulässigkeitsvoraussetzungen erfüllt sind.

Bei einer Verlegung eines Patienten in eine ausländische Spezialklinik zur Mit- und Nachbehandlung und bei der damit eventuell verbundenen Datenübermittlung stellt sich diese Frage allerdings dann nicht, wenn der Patient zumindest konkludent, besser aber ausdrücklich, eingewilligt hat.

§ 18 Auskunft und Akteneinsicht

§ 18 Abs. 1 LKHG M-V

Patienten ist auf Antrag kostenfrei Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen und Einsicht in die Krankenunterlagen einschließlich der ärztlichen und pflegerischen Dokumentation zu gewähren. Dieses Recht erstreckt sich auch auf Angaben über die Personen und Stellen, denen Patientendaten übermittelt worden sind. Die Datenschutzrechte Dritter sind zu beachten. Sind Patientendaten mit personenbezogenen Daten Dritter untrennbar verbunden, kann die Einsicht in diese Daten verwehrt werden, wenn dadurch überwiegende schutzwürdige Interessen dieser Personen gefährdet würden. Im Übrigen bleibt das Einsichtsrecht unberührt.

Die kostenfreie **Auskunft** ist ein datenschutzrechtlicher Grundsatz, der für den Krankenhausbereich durch diese Vorschrift näher ausgeformt wird. Neben diesem Auskunftsrecht zu allen über sie gespeicherten Daten haben Patienten ein ausdrückliches **Einsichtsrecht** in die ärztliche und pflegerische Dokumentation. Die Vorschrift entspricht auch dem für eine erfolgreiche Behandlung notwendigen Vertrauensverhältnis zwischen Arzt und Patient und fördert dieses.

Grundsätzlich besteht das Einsichtsrecht des Patienten in „seine“ Krankenunterlagen, zu denen auch Röntgenaufnahmen und alle sonst bildgebenden Befunde gehören. Ausgeschlossen ist jedoch in der Regel ein Anspruch auf Herausgabe der **Originalunterlagen** zum endgültigen Verbleib beim Patienten. Wo die Einsichtnahme in den Räumen des Krankenhauses oder der Arztpraxis nicht ausreichend ist, hat der Patient einen Anspruch auf Fotokopien gegen Kostenerstattung. Im Einzelfall können jedoch besondere Umstände die zeitlich befristete Herausgabe der Originalunterlagen rechtfertigen. So entschied das Landgericht München in dem Fall eines Patienten, der zur Prüfung, ob ein Behandlungsfehler vorlag, vorübergehend die Originalunterlagen haben wollte, dass die Originalunterlagen dann zeitlich befristet herauszugeben sind, wenn die Kopie eines bildgebenden Befundes eine klare Diagnose nicht ermöglicht (Landgericht München vom 15.11.2000 – 9 O 12451/00). Nach Ansicht des Gerichtes könne dem Patienten nicht zugemutet werden, zunächst mit Kopien zu arbeiten, die wegen ihrer Ungenauigkeit in der Regel eine klare Diagnose nicht zuließen, um dann zu erfahren, dass der Privatgutachter doch die Originale benötigt, oder um dann im Verfahren anhand der Originale feststellen zu müssen, dass der angenommene Behandlungsfehler sich entgegen der Aussagen der Kopien mit den Originalen gar nicht feststellen lasse und insoweit von vornherein ein Verfahren gegen den behandelnden Arzt aussichtslos gewesen ist.

Darüber hinaus ist dem Patienten auf seinen Wunsch hin mitzuteilen, an welche Personen und Stellen seine Daten übermittelt worden sind. Auch aus diesem Grund ist es deshalb wichtig, dass insbesondere unregelmäßige Datenübermittlungen ausreichend dokumentiert werden. Beispielsweise sollte in der Patientenakte festgehalten werden, wenn dem MDK bestimmte Unterlagen übermittelt wurden oder dieser die Patientenakte für seine gutachtliche Stellungnahme an die gesetzliche Krankenkasse eingesehen hat. Bei der Übermittlung auf der Grundlage des § 301 SGB V ist dagegen eine gesonderte Dokumentation in der Patientenakte bei Patienten der gesetzlichen Krankenversicherung nicht notwendig, denn dies ist für diesen Personenkreis eine regelmäßige Übermittlung auf einer gesetzlichen Grundlage.

Um die **Datenschutzrechte Dritter** zu beachten, hat der Gesetzgeber festgelegt, dass die Einsicht verwehrt werden kann, wenn die Patientendaten untrennbar mit personenbezoge-

nen Daten Dritter (oder auch Daten anderer Patienten) verbunden sind. Beispielsweise kann die Einsicht in eine zu einem bestimmten zulässigen Zweck erstellte Patientenliste verwehrt werden, da ein Patient auch die Daten der anderen Patienten einsehen könnte. Der Patient könnte aber die Liste einsehen, wenn die Daten der anderen Patienten abgedeckt würden. Andererseits könnte dem Betroffenen mitgeteilt werden, welche Daten über ihn in der Liste enthalten sind.

§ 18 Abs. 2 LKHG M-V

Das Krankenhaus kann im Einzelfall die Auskunft über die gespeicherten Daten oder die Akteneinsicht durch einen Arzt vermitteln lassen, sofern anderenfalls eine unverhältnismäßige Beeinträchtigung der Gesundheit des Patienten zu befürchten ist. Die Notwendigkeit der Vermittlung ist zu begründen und schriftlich in der Krankenakte festzuhalten.

Um einen schnellen und ungestörten Heilungsprozess zu erreichen, kann es notwendig sein, dass der Patient (noch) nicht vollständig über seinen Krankheitszustand aufgeklärt wird. Dennoch besteht aber das **Einsichtsrecht**. In diesem Fall kann das Krankenhaus die Auskunft oder Einsicht durch einen Arzt vermitteln lassen, um zu verhindern, dass der Gesundheitszustand des Patienten durch die Wahrnehmung seines Rechts und die mögliche Konfrontation mit sehr belastenden Daten beeinträchtigt wird. Dies muss begründet und in der Krankenakte dokumentiert werden. Die Vermittlung durch einen Arzt soll bewirken, dass der Patient nicht verunsichert wird, wenn er seine Krankenakte einsieht. Der Arzt sollte dem Patienten bei der Einsicht auch die medizinischen Sachverhalte erklären, damit der Betroffene seinen Krankheitszustand beurteilen kann.

§ 18 Abs. 3 LKHG M-V

Absatz 1 gilt entsprechend, soweit Dritte im Sinne des § 14 Abs. 1 Satz 2 Auskunft über die zu ihrer Person gespeicherten Daten verlangen und schutzwürdige Belange des Patienten nicht entgegenstehen.

Die Behandlung eines Patienten im Krankenhaus macht es in der Regel auch erforderlich, dass Daten seiner **Angehörigen** oder anderer Bezugspersonen mit erhoben und verarbeitet werden. Auch diese Personen haben ein Recht auf Auskunft über die zu ihrer Person im Zusammenhang mit der Behandlung des Patienten gespeicherten Daten sowie Einsicht in die Krankenakten. Für sie gilt der Absatz 1 des § 18 LKHG M-V entsprechend. Das Aktenauskunfts- und Einsichtsrecht kann jedoch nur dann gewährt werden, wenn der Auskunft oder Einsicht keine schutzwürdigen Belange des Patienten entgegenstehen. Ob dieses der Fall ist, ist vom Krankenhaus in jedem Einzelfall gesondert zu prüfen.

§ 19 Löschung und Sperrung von Daten

§ 19 Abs. 1 LKHG M-V

Patientendaten in Krankenunterlagen sind nach Abschluss der Behandlung zu sperren und spätestens nach Ablauf von 30 Jahren zu löschen. Im Übrigen sind Patientendaten zu löschen, wenn sie zur Erfüllung der Nutzungszwecke nach diesem Gesetz nicht mehr erforderlich sind. An die Stelle der Löschung tritt eine Sperrung, solange

1. der Löschung eine durch Rechtsvorschrift oder durch die ärztliche Berufsordnung vorgeschriebene Aufbewahrungsfrist entgegensteht oder

2. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Patienten beeinträchtigt würden.

Soweit die Voraussetzungen nach Satz 3 nicht vorliegen, können Daten anstelle der Löschung anonymisiert werden, wenn sichergestellt ist, dass der Personenbezug in keiner Weise wiederhergestellt werden kann.

Die **Aufbewahrungsfrist** von ärztlichen Aufzeichnungen ist in der Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern geregelt. Abweichungen von dieser allgemeinen Vorschrift ergeben sich aus gesetzlichen Spezialregelungen. Die 30-jährige Aufbewahrungsfrist nach Abschluss der Behandlung ist für den Krankenhausbereich eine solche spezialgesetzliche Regelung. Nach Satz 1 sind Patientendaten spätestens nach 30 Jahren zu löschen. Dies bedeutet, dass sie auch vor dem Ablauf dieser Frist gelöscht werden können. Entschließt sich das Krankenhaus, bestimmte Unterlagen früher zu löschen, so gilt die in der Berufsordnung festgelegte Frist von der mindestens zehnjährigen Aufbewahrung. Wenn von der 30-jährigen Aufbewahrung abgewichen wird, ist zu prüfen, ob durch die Verkürzung schutzwürdige Belange des Patienten beeinträchtigt werden. Davon wäre beispielsweise auszugehen, wenn der Patient an einer chronischen Krankheit oder auch an den Spätfolgen einer Operation leidet und die Daten für einen Rentenanspruch benötigt werden.

Eine vorzeitige Löschung von konventionell aufbewahrten Patientenunterlagen ist sehr aufwendig, da dies in jedem Einzelfall ein Arzt entscheiden müsste. In der Krankenhauspraxis ist es deshalb weit verbreitet, die Patientenakten generell 30 Jahre nach Abschluss der Behandlung aufzubewahren. Bei verstorbenen Patienten können die Daten aber auch schon nach zehn Jahren gelöscht werden.

Patientendaten, die nicht der ärztlichen Dokumentation dienen, sind dann zu **löschen**, wenn sie für den einmal gespeicherten Zweck nicht mehr erforderlich sind. Beispielsweise kann mit Zustimmung eines Patienten eine Liste angefertigt werden, um Besuchern Auskunft über die Behandlungsstation und die Zimmernummer geben zu können (Pfortnerliste). Diese Daten sind jedoch nicht mehr erforderlich, wenn der Patient das Krankenhaus verlassen hat, und müssen deshalb dann gelöscht werden. Bei allen außerhalb der ärztlichen Dokumentation gespeicherten Patientendaten muss regelmäßig geprüft werden, ob sie noch zur Erfüllung der jeweiligen Aufgabe notwendig sind. Ist das nicht der Fall, sind sie zu sperren beziehungsweise zu löschen.

Zu beachten ist weiterhin, dass Patientendaten nach Abschluss der Behandlung zu **sperren** sind. Darüber hinaus sind sie zu sperren, wenn sie wegen einer anderen Rechtsvorschrift oder einer Aufbewahrungsfrist nicht gelöscht werden dürfen, obwohl sie zur Erfüllung dieser Aufgabe nicht mehr benötigt werden. Sie sind schließlich auch zu sperren, wenn durch eine Löschung schutzwürdige Belange des betroffenen Patienten beeinträchtigt würden. Die gesperrten Daten dürfen dann nur noch eingeschränkt genutzt und verarbeitet werden.

Daten über Krankheiten sind für die medizinische Wissenschaft und **Forschung** häufig sehr interessant. Der letzte Satz dieser Rechtsvorschrift eröffnet deshalb die Möglichkeit, Patientendaten zu anonymisieren, um sie dann länger als 30 Jahre aufbewahren zu können. Dabei ist sehr umsichtig vorzugehen, denn es darf aus den verbleibenden Daten kein Personenbezug mehr hergestellt werden können. Nicht ausreichend wäre eine Anonymisierung, bei der nur auf den Namen und die Wohnanschrift verzichtet wird, da sich auch über das vollständige Geburts- und Sterbedatum ein Personenbezug herstellen lässt. Es sind

folglich alle Daten zu entfernen, die geeignet sein können, den Patienten wieder zu identifizieren.

§ 19 Abs. 2 LKHG M-V

Gesperrte Daten sind gesondert zu speichern. Soweit dies nicht möglich ist, sind die Daten mit einem Sperrvermerk zu versehen. Gesperrte Daten dürfen vor Ablauf der Sperrfrist nicht verändert oder gelöscht werden. Zur Erschließung der Akten ist im Krankenhausarchiv ein Nachweis zu führen, zu dem kein direkter Zugriff anderer Bereiche besteht. Die Sperrung kann nur aufgehoben werden für die Durchführung einer Behandlung, mit der die frühere Behandlung in einem medizinischen Sachzusammenhang steht, zur Behebung einer Beweisnot, für eine spätere Übermittlung nach § 17 Abs. 1 oder wenn der Patient einwilligt. Die Aufhebung der Sperrung ist zu begründen und in der Krankenunterlage zu vermerken.

Beim Umgang mit gesperrten Daten wird zunächst gefordert, dass sie **gesondert zu speichern** sind. Damit wird bezweckt, dass diese Daten nicht mehr beziehungsweise nur eingeschränkt genutzt werden können, nachdem die Behandlung abgeschlossen worden ist. Würden sie im aktuell verfügbaren Datenbestand gespeichert und lediglich als gesperrt gekennzeichnet, so könnten sie weiterhin gelesen und genutzt werden, was durch die Sperrung aber gerade verhindert werden soll. Gesonderte Speicherung bedeutet folglich, dass ein Zugriff auf diese Daten bei der üblichen Verarbeitung nicht mehr möglich sein darf.

Eine Sperrung sämtlicher Patientendaten wäre aus organisatorischer Sicht aber nicht sinnvoll, da bei der Aufnahme eines Patienten nicht mehr festgestellt werden könnte, ob er bereits einmal in diesem Krankenhaus behandelt wurde. Um die Aufnahme zu erleichtern und möglicherweise wichtige Informationen über frühere Krankenhausaufenthalte für die Behandlung zur Verfügung zu stellen, ist es zulässig, Daten, die nicht gesondert gespeichert werden können, mit einem **Sperrvermerk** zu versehen. Dies wird im Wesentlichen bestimmte, für die Verwaltung erforderliche „Stammdaten“ wie Name, Vorname, Geburtsdatum und Anschrift betreffen. Das Aufnahmepersonal sollte den Sperrvermerk bei einer Neuaufnahme entfernen und danach weitere Stammdaten wie Bezeichnung der Krankenkasse, Krankenversicherungsnummer, Versichertenstatus, Beginn des Versichertenstatus oder auch Daten über andere Kostenträger „freischalten“ können. Wenn die Stammdaten wieder aktiviert sind, muss es für die behandelnde Fachabteilung möglich sein, auf frühere Behandlungsdaten zuzugreifen, soweit dies für die aktuelle Behandlung erforderlich ist.

§ 19 Abs. 2 LKHG M-V verlangt in Satz 4 weiter, dass zur Erschließung der Akten im Archiv ein Nachweis zu führen ist, auf den andere Bereiche nicht direkt zugreifen dürfen. Daraus folgt zweierlei: Zum einen stellt der Gesetzgeber damit die simple Forderung auf, dass ein Nachweis oder ein Verzeichnis der Akten zu führen ist, um sie aufzufinden und zu erschließen. Unerheblich ist dabei, ob es sich um eine Kartei oder um einen rechnergestützten Nachweis handelt. Anhand dieses Nachweises ist es dem Archivpersonal möglich, auf Anforderung von Ärzten Suchkriterien einzugeben und den Aufbewahrungsort der Unterlagen zu ermitteln. Zum zweiten verlangt der Gesetzgeber, dass auf diesen Nachweis „kein direkter Zugriff anderer Bereiche“ bestehen darf. Das bedeutet nicht nur, dass der Nachweis selbst nur dem Archiv zur Verfügung stehen darf, sondern vor allem, dass die Akten im Archiv so abgelegt werden müssen, dass sie auch nur mit Hilfe dieses Nachweises zuzuordnen sind und andere Bereiche des Hauses die Akten nicht ohne diesen Nachweis erschließen können. Anderenfalls hätte es keinen Sinn, extra einen Nachweis zur Erschließung zu führen, wenn jedermann auch ohne diesen jederzeit jede Patientenakte ohne

weiteres finden würde. Deshalb sollte das entscheidende Ordnungsmerkmal bei der Ablage der Akten nicht das Geburtsdatum und bei gleichen Geburtsdaten die alphabetische Ordnung der Namen sein. Es empfiehlt sich daher, die Akten geordnet nach Behandlungsfällen und getrennt nach Abteilungen aufzubewahren. Für **Notfälle** ist es zulässig, den Nachweis beispielsweise der Notaufnahme zur Verfügung zu stellen. Es sollte jedoch nur ein kleiner und bestimmter Personenkreis Zugang dazu haben. Zugriffe auf den Nachweis sollten protokolliert werden.

Die im Archiv aufbewahrten und gesperrten Patientenunterlagen dürfen nur unter den Voraussetzungen des Absatzes 2 Satz 5 entsperrt und genutzt werden. Ein wichtiger Fall der **Entsperrung** ist die erneute Behandlung desselben Patienten. Dies ist jedoch nur dann zulässig, wenn ein **medizinischer Sachzusammenhang** zu der früheren Behandlung und den archivierten Unterlagen besteht. Wird ein Patient also in ein Krankenhaus aufgenommen, in dem er schon einmal behandelt wurde, muss zunächst festgestellt werden, ob ein medizinischer Zusammenhang besteht, der es zulässt, dass die archivierten Unterlagen genutzt werden. Dies kann nicht das Archivpersonal entscheiden, sondern nur ein Arzt aus der jetzt behandelnden Abteilung. Nach Satz 6 muss der anfordernde Arzt begründen, warum die Sperrung aufzuheben ist. Die Aufhebung der Sperrung und die dazugehörige Begründung ist in der Krankenunterlage zu protokollieren, damit später nachvollzogen werden kann, wann und zu welchem Zweck Unterlagen aus der Akte verwendet wurden und ob dies erforderlich war.

Für die Aufbewahrung folgt daraus, dass Patientenakten getrennt nach Fachabteilungen und Krankenhausaufenthalten abgelegt werden sollten. Dies ist erforderlich, um bei erneuter Behandlung eines Patienten sicherzustellen, dass ohne weiteres nur diejenigen Unterlagen aus dem Archiv herausgegeben werden, die mit dem gegenwärtigen Aufenthalt in einem medizinischen Zusammenhang stehen. Beispiel: War eine Patientin einmal zu einer gynäkologischen Behandlung im Krankenhaus, sind alle Unterlagen dieser Behandlung für die spätere Behandlung eines Knochenbruches in der Regel nicht erforderlich.

Querverweise auf das Vorhandensein weiterer archivierter Unterlagen über einen Patienten und deren Fundort sind selbstverständlich zulässig und auch erforderlich.

Vor dem Hintergrund, dass in Krankenhausarchiven vielfach nur eine Akte über einen Patienten mit Unterlagen aus sämtlichen Behandlungen in verschiedenen Fachabteilungen existiert, müssen sich die **Entsperrungen** auf konkrete Behandlungsunterlagen einer oder mehrerer bestimmter Fachabteilungen beziehen. Die Entsperrung der vollständigen Akte ist jedenfalls nicht zulässig, da dann auch Unterlagen verfügbar wären, die eben in keinem medizinischen Sachzusammenhang mit der gegenwärtigen Behandlung stehen. Deshalb ist auch eine Art der Archivierung vorzuziehen, bei der nicht alle Unterlagen von mehreren Behandlungen in einer Akte abgelegt werden, sondern bei der je Behandlung ein Vorgang angelegt wird. Wenn dies aus organisatorischen oder anderen Gründen nicht praktikabel ist und je Patient nur eine Akte vorhanden sein soll, müssten zumindest die einzelnen Behandlungen beispielsweise durch Zwischenblätter auffällig getrennt werden, um das Auffinden und Trennen der zu entsperrenden Teile zu erleichtern.

Daten und Unterlagen dürfen auch zur Behebung einer Beweisnot entsperrt werden, zum Beispiel um festzustellen, ob der Patient tatsächlich über die Risiken einer Operation aufgeklärt wurde.

Des Weiteren dürfen Daten für eine Übermittlung nach § 17 Abs. 1 oder mit Einwilligung des Patienten entsperrt werden. Die Einwilligung muss hinreichend konkret sein und insbesondere die in § 15 Abs. 2 genannten Bedingungen erfüllen.

Von der Art der Verarbeitung und dem vorgesehenen Nutzungszweck ist es abhängig, wie die Aufhebung der Sperrung begründet und in der Krankenunterlage vermerkt wird. Werden beispielsweise automatisiert gespeicherte Stammdaten entsperrt, so ist es ausreichend, wenn als Grund dafür „Neuaufnahme“ in der Datei vermerkt und dies protokolliert wird. Allerdings unterliegt dann das Protokoll auch den Aufbewahrungsfristen dieses Gesetzes, da es als eine Krankenunterlage zu werten ist. Entnimmt man hingegen Unterlagen aus einer archivierten Akte, so sind die Begründung und der Nachweis über die Entsperrung in der Krankenakte aufzubewahren.

§ 19 Abs. 3 LKHG M-V

Soweit Patientendaten in automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert werden, ist nach Abschluss der Behandlung die Möglichkeit des Direktabrufs zu sperren.

Die Verarbeitung von Patientendaten in **medizinischen Informationsnetzen** wird auch im Krankenhausbereich zunehmen. Gerade in diesen Fällen sind durch **technische und organisatorische Maßnahmen** Zugriffsberechtigungen festzulegen. Solche Berechtigungen können auch als Direktabruf ausgestaltet sein. Wenn beispielsweise eine Abteilung eine weitere in die Behandlung einbezieht, so können die Daten auf dem Rechner der erstbehandelnden, selbstverständlich unter Berücksichtigung von Integrität, Vertraulichkeit und Authentizität, der anderen Abteilung zum Direktabruf bereitgestellt werden. **Direktabruf** bedeutet, dass die speichernde Stelle nicht beeinflusst, ob und wann ein Berechtigter die Daten abrufen kann. Der Abruf selbst ist allerdings zu protokollieren, damit festgestellt werden kann, ob tatsächlich nur Berechtigte die Daten abgerufen haben. Ist die Behandlung jedoch abgeschlossen, so ist auch der Direktabruf zu sperren.

§ 20 Datenverarbeitung für Forschungszwecke

§ 20 Abs. 1 LKHG M-V

Die Verarbeitung und Nutzung von Patientendaten, die im Rahmen von § 15 Abs. 1 gespeichert worden sind, ist für Forschungszwecke zulässig, wenn der Patient eingewilligt hat.

Nach dem Krankenhausgesetz zulässig erhobene Patientendaten können für **Forschungszwecke** genutzt werden, wenn der Patient eingewilligt hat. Dies sollte der Regelfall sein. Die **Einwilligung** muss die schon angesprochenen Voraussetzungen erfüllen (§ 15 Abs. 2) und kann immer nur für einen konkreten Forschungszweck abgegeben werden. Eine Einwilligung mit Wirkung auf in Zukunft festzulegende Forschungen und ohne einen konkreten Zweck ist deshalb unzulässig.

Allerdings erstreckt sich die Einwilligung nicht auf die Erhebung zusätzlicher Daten, wenn für ein Forschungsvorhaben neben den für die Behandlung erforderlichen Daten weitere benötigt werden. Um diese auf freiwilliger Basis zu erhalten, müssen die Patienten ihr Einverständnis geben. **Freiwilligkeit** bedeutet in diesem Zusammenhang auch, dass ihnen

keine Nachteile bei der ärztlichen Behandlung entstehen, wenn sie nicht mit dieser Erhebung einverstanden sind. Auch darauf ist in der Einverständniserklärung hinzuweisen.

§ 20 Abs. 2 LKHG M-V

Patientendaten dürfen ohne Einwilligung des Patienten nur für bestimmte Forschungsvorhaben verarbeitet und genutzt werden, soweit

1. dessen schutzwürdige Belange wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Nutzung nicht beeinträchtigt werden oder
2. die für das Krankenhaus zuständige oberste Aufsichtsbehörde festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten erheblich überwiegt und der Zweck des Forschungsvorhabens nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Soweit Patientendaten unter diesen Voraussetzungen an Hochschulen oder andere mit wissenschaftlicher Forschung beauftragte Stellen übermittelt werden, hat das Krankenhaus die empfangende Stelle, die Art der zu übermittelnden Daten, den Kreis der betroffenen Personen, das von der empfangenden Stelle genannte Forschungsvorhaben sowie das Vorliegen der Voraussetzungen des Satzes 1 aufzuzeichnen. Der Datenschutzbeauftragte des Krankenhauses ist zu beteiligen.

Abweichend vom Regelfall dürfen Patientendaten nur unter ganz bestimmten Voraussetzungen auch **ohne Einwilligung** des Patienten für ein konkretes Forschungsvorhaben verarbeitet werden.

Nach der **ersten Ausnahme** dürfen Patientendaten ohne Einwilligung für die Forschung verarbeitet werden, wenn schutzwürdige Belange eines Patienten wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Nutzung nicht beeinträchtigt werden. Ob schutzwürdige Belange beeinträchtigt sein können, muss das Krankenhaus sehr sorgfältig prüfen. Bestehen in dieser Hinsicht Zweifel, sollte das Vorhaben mit Einwilligung der Patienten durchgeführt werden.

Werden zum Beispiel pseudonymisierte Daten an eine Forschungsstelle übermittelt, könnte der Fall vorliegen, dass schutzwürdige Belange des Betroffenen wegen der Art der Daten nicht beeinträchtigt sind. Sie können dann ohne Einwilligung des Betroffenen für einen Forschungszweck genutzt werden.

Pseudonymisierte Patientendaten sind solche, die keine unmittelbare Zuordnung zu einem Patienten ermöglichen. Patientendaten können pseudonymisiert werden, indem man anstelle von Identifikationsdaten wie Name, Vorname, Geburtsdatum und Anschrift oder auch der Krankenversicherungsnummer eine krankenhausinterne Datensatz- bzw. Patientenummer verwendet. Die Daten sind dann immer noch Patientendaten, da ihre Zuordnung zu einem Patienten im Krankenhaus jederzeit möglich ist. Die forschende Stelle kann ohne dieses Zusatzwissen aber keine Zuordnung vornehmen.

Der Fall, dass Patientendaten offenkundig sind und aus diesem Grund schutzwürdige Belange nicht beeinträchtigt werden, dürfte in der Praxis sehr selten auftreten. Bereits die Tatsache, dass sich ein Patient bei einem bestimmten Arzt oder in einem bestimmten Krankenhaus in Behandlung befindet, unterliegt der Schweigepflicht. Unter Umständen wären Patientendaten offenkundig, wenn sie mit Einwilligung der Patienten veröffentlicht worden sind und die Veröffentlichung auch erforderlich war.

Ein Beispiel dafür, dass schutzwürdige Belange der Patienten wegen der Art der Nutzung nicht beeinträchtigt sind, könnte eine Statistik über den Einzugsbereich eines Krankenhauses und die Altersstruktur der Patienten anhand der Postleitzahl ihrer Wohnorte und ihrer Geburtsdaten sein. Das Geburtsdatum und die Postleitzahl erlauben zwar die Zuordnung weiterer personenbezogener Daten und sind damit prinzipiell geeignet, einen Patienten bestimmbar zu machen, insbesondere wenn es sich dabei um sehr alte Personen handelt. Werden diese Daten jedoch zu einer Statistik zusammengestellt, die immer eine ausreichend große Anzahl von Einzelmerkmalen in einer Merkmalsklasse enthält, so ist wegen dieser Nutzung nicht zu befürchten, dass schutzwürdige Belange eines Patienten beeinträchtigt werden. Diese Nutzung ist deshalb ohne Einwilligung des Betroffenen zulässig.

Nach der **zweiten Ausnahme** dürfen Patientendaten zu einem Forschungszweck ohne Einwilligung des Patienten genutzt werden, wenn das Sozialministerium als zuständige oberste **Aufsichtsbehörde** festgestellt hat, dass überwiegende öffentliche Interessen die schutzwürdigen Belange des Patienten überwiegen. Dabei muss die Aufsichtsbehörde prüfen, ob der Zweck der Forschung nicht auf andere Weise erfüllt werden kann – zum Beispiel durch Verzicht auf Patientendaten und Nutzung von Falldaten. Können auch Falldaten zu einem befriedigenden Ergebnis führen, so kann die Aufsichtsbehörde die Verarbeitung und Nutzung von Patientendaten ohne Einwilligung nicht genehmigen, weil pseudonymisierte oder anonymisierte Daten ausreichend sind.

Kommt die Aufsichtsbehörde jedoch zu dem Ergebnis, dass der Zweck auch mit Falldaten erreicht werden kann, dies aber mit einem unverhältnismäßigen Aufwand verbunden ist, so könnte sie die Nutzung der Patientendaten ohne Einwilligung genehmigen.

Die Abwägung zwischen öffentlichem Interesse und schutzwürdigen Belangen der Patienten sollte sehr gründlich erfolgen. Im Zweifelsfall ist den schutzwürdigen Belangen der Patienten der Vorrang zu geben, da immer die Möglichkeit besteht, die Daten auch mit Einwilligung der betroffenen Patienten für die Forschungsaufgabe zu verarbeiten.

Bei einer Datenübermittlung an eine wissenschaftliche Forschungseinrichtung unter den oben genannten Voraussetzungen hat das Krankenhaus **Dokumentationspflichten** zu erfüllen. Aufzuzeichnen ist die empfangende Stelle (vollständige Adresse der wissenschaftlichen Forschungseinrichtung), die Art der übermittelten Daten, beispielsweise Patientennummer, Geburtsdatum, Diagnose, Therapie etc., der von der Datenübermittlung betroffene Patientenkreis, beispielsweise alle Patienten der Jahrgänge 19xx bis 19xx mit Fraktur eines oder beider Beine im Zeitraum vom 01.01.19xx bis 31.12.20xx, die Bezeichnung des Vorhabens und unter welchen Voraussetzungen die Übermittlung ohne Einwilligung erfolgt, zum Beispiel schutzwürdige Belange der Patienten werden nicht beeinträchtigt oder die Aufsichtsbehörde hat die Durchführung der Forschungsaufgabe genehmigt.

Der **Datenschutzbeauftragte** des Krankenhauses ist bei dem gesamten Verfahren zu beteiligen und soll die Leitung des Krankenhauses beraten.

§ 20 Abs. 3 LKHG M-V

Jede weitere Nutzung der Patientendaten unterliegt den Anforderungen der Absätze 1 und 2. Die übermittelnde Stelle hat sich vor der Übermittlung davon zu überzeugen, dass die empfangende Stelle bereit und in der Lage ist, diese Vorschriften einzuhalten.

Oft möchte eine weitere Forschungseinrichtung Patientendaten nutzen, die bereits von einer forschenden Stelle verarbeitet und genutzt wurden. Patientendaten dürfen von einer Forschungsstelle an eine andere übermittelt werden, wenn die in dieser Rechtsvorschrift genannten Voraussetzungen erfüllt sind. Die Daten übermittelnde Stelle muss sich davon überzeugen, dass die Daten empfangende Stelle in der Lage ist, diese Vorschriften einzuhalten. Der Begriff „Vorschriften“ sollte hier weit ausgelegt werden, und zwar im Sinne von Datenschutzvorschriften. Es sind also nicht nur die Bestimmungen der Datenverarbeitung für Forschungszwecke zu beachten, sondern beispielsweise auch die Auflagen, die das Krankenhaus der ersten Forschungseinrichtung zum Umgang mit den Daten vorgegeben hat, oder die technischen und organisatorischen Maßnahmen, die einen sicheren Umgang mit den Daten gewährleisten sollen.

§ 20 Abs. 4 LKHG M-V

Sobald der Forschungszweck es erlaubt, sind die Merkmale, mit deren Hilfe ein Patientenbezug hergestellt werden kann, gesondert zu speichern. Die Merkmale sind zu löschen, sobald der Forschungszweck dies gestattet. Die Forschung betreibende Stelle darf Patientendaten nur mit schriftlicher Einwilligung der Betroffenen veröffentlichen.

In dieser Vorschrift wird die Anonymisierung der Daten mit einer Zwischenstufe geregelt. Sobald es möglich ist, sind Merkmale, mit denen ein Patient bestimmt werden kann, **gesondert zu speichern**. Solche Merkmale können der Name oder eine Patientennummer oder auch eine Krankenversicherungsnummer im Zusammenhang mit einer Fallnummer sein (Pseudonym). Über die Fallnummer können, soweit dies erforderlich ist, die Identifikationsdaten mit den wissenschaftlichen Daten verbunden werden. Die gesonderte Speicherung soll verhindern, dass die Merkmale zur Identifizierung verarbeitet oder genutzt werden, obwohl dies bei der wissenschaftlichen Bearbeitung der Daten nicht erforderlich ist. Wenn abzusehen ist, dass die Merkmale, die den Patientenbezug ermöglichen, mit den für die wissenschaftliche Aufgabe interessanten Daten nicht mehr verbunden werden müssen, sind diese Merkmale zu löschen. Wenn kein Personenbezug mehr herstellbar ist, handelt es sich um anonymisierte Daten, die nicht mehr den datenschutzrechtlichen Bestimmungen unterliegen.

Ob aufgrund des Löschens der Merkmale der **Identifizierung** allerdings bereits anonymisierte Daten vorliegen, hängt von vielen Faktoren ab, insbesondere auch von der Art der Daten und der Möglichkeit, einzelne wissenschaftliche Daten einer Person zuzuordnen. Unter Umständen entstehen deshalb durch Löschen der Merkmale zur Identifizierung wiederum lediglich nur pseudonymisierte Daten. Als Beispiel sei hier an den 100-jährigen Patienten erinnert (siehe Seite 15). Wird diese Altersangabe mit den wissenschaftlich interessanten Daten gespeichert, reicht das Löschen der Merkmale zur Identifizierung nicht aus, um die Daten zu anonymisieren, da möglicherweise allgemein bekannt ist, dass in einer bestimmten Stadt/Region nur eine Person dieses Alters lebt. Solche Daten sind erst dann anonymisiert, wenn mehrere Personen in einer Klasse mit einer ausreichend großen Spannweite zusammengefasst werden (z. B. alle Patienten älter als 75 Jahre).

Die Forschungseinrichtung darf Patientendaten nur mit schriftlicher Einwilligung des Betroffenen veröffentlichen. Eine Einwilligung wäre jedoch unwirksam, wenn die Veröffentlichung nicht erforderlich ist.

§ 20 Abs. 5 LKHG M-V

Soweit die Vorschriften dieses Gesetzes auf die empfangende Stelle keine Anwendung finden, dürfen Patientendaten nur übermittelt werden, wenn die empfangende Stelle sich verpflichtet, die Vorschriften der Absätze 2 und 4 einzuhalten und sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

Öffentliche Stellen und öffentlich-rechtlich geführte Krankenhäuser des Landes Mecklenburg-Vorpommern unterliegen den Vorschriften des DSGVO M-V beziehungsweise des LKHG M-V und damit der Kontrolle durch den Landesbeauftragten für den Datenschutz. Da aber auch **nicht-öffentliche** Stellen wissenschaftliche Forschung betreiben, dürfen an diese Stellen Patientendaten nur übermittelt werden, wenn sie sich verpflichten, bei deren Verarbeitung ohne Einwilligung der Betroffenen die Vorschriften des Absatzes 2 und das in Absatz 4 vorgeschriebene Verfahren beim Umgang mit den Daten einzuhalten. Selbstverständlich können sich diese Stellen die Patientendaten auch mit Einwilligung der Betroffenen übermitteln lassen. Jedoch auch dann ist das in Absatz 4 vorgegebene Verfahren anzuwenden. Das Krankenhaus sollte die Forschungseinrichtung schriftlich zur Einhaltung der entsprechenden Vorschriften **verpflichten**. Unabhängig davon, ob die nicht-öffentliche Forschungseinrichtung die Daten mit Einwilligung des Betroffenen oder nach der Ausnahmeregelung des Absatzes 2 erhält, muss sie sich hinsichtlich der Einhaltung der Regelungen der Absätze 2 und 4 der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwerfen. Insoweit (so der Wortlaut in Absatz 5) ist der LfD dann befugt, nicht nur die Übermittlungsvoraussetzungen, sondern auch die Vorschriften der Absätze 2 und 4 zu prüfen.

Übermittelt ein Krankenhaus des Landes Mecklenburg-Vorpommern Patientendaten an eine öffentliche Stelle des Bundes oder eines anderen Bundeslandes für einen Forschungszweck, so unterliegt dies ebenfalls Absatz 5, da auf diese Stellen das LKHG M-V ebenfalls keine Anwendung findet. Auch hier muss sich die empfangende Stelle zur Einhaltung der Absätze 2 und 4 verpflichten und insoweit der Kontrolle des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern unterwerfen. Die Zulässigkeit und die Kontrolle der darüber hinausgehenden Datenverarbeitung richtet sich dann jeweils nach dem für die empfangende Stelle einschlägigen Bundes- bzw. Landesdatenschutzrecht. Die Kontrolle des Landesdatenschutzbeauftragten Mecklenburg-Vorpommern ist somit auf die Einhaltung der Absätze 2 und 4 von § 20 LKHG beschränkt.

§ 20 Abs. 6 LKHG M-V

Ein Arzt darf für eigene Diagnose-, Behandlungs- oder Forschungszwecke Dateien mit Patientendaten anlegen. Der Arzt hat entsprechend §§ 21 und 22 des Landesdatenschutzgesetzes insbesondere sicherzustellen, dass Dritte keinen Zugriff auf die Daten haben, soweit sie diese nicht zur Mitbehandlung benötigen. Dazu hat er gegenüber dem Krankenhausträger den Nachweis zu erbringen, dass hierzu bei ihm die technischen und organisatorischen Voraussetzungen zur Durchsetzung des Datenschutzes im Sinne des Gesetzes gewährleistet sind. Sobald es der Verarbeitungszweck erlaubt, sind die Daten zu anonymisieren.

Die Vorschriften dieses Absatzes erlauben es einem Krankenhausarzt, außerhalb der obligatorischen Dokumentation in der Patientenakte für die hier genannten eigenen Zwecke und unter Einhaltung der weiteren Bedingungen Dateien mit Patientendaten anzulegen. Der Grundsatz der Erforderlichkeit ist wie bei jedem anderen Umgang mit personenbezogenen oder Patientendaten auch hier zu beachten. Ist also für diese Zwecke kein Personenbezug erforderlich, sind nur Falldaten zu verarbeiten und zu nutzen.

Der Zugang zu Patientendaten wird für den behandelnden Krankenhausarzt erleichtert, um beispielsweise Diagnose- oder Behandlungsmethoden auch nach **Abschluss der Behandlung** und Sperrung der entsprechenden Patientendaten vergleichen und auswerten zu können. Auch für **eigene Forschungszwecke** darf der Arzt diese Daten nutzen, vorausgesetzt, dass technische und organisatorische Maßnahmen realisiert sind, die einen Zugriff durch an der Behandlung nicht beteiligte Dritte verhindern. Zum Beispiel können die Daten verschlüsselt oder statt auf der Festplatte des Rechners auf Disketten gespeichert werden. Die Disketten sind verschlossen aufzubewahren. Die Daten sollten auch nicht beziehungsweise nur, wenn weitere Sicherheitsmaßnahmen realisiert sind, auf einem an ein öffentliches Netz angeschlossenen Rechner verarbeitet werden. Neben dem Zugriffsschutz sind weitere der in §§ 21 und 22 DSGVO M-V bzw. § 9 BDSG genannten Maßnahmen anzuwenden. Außerdem muss der Krankenhausarzt gegenüber dem Krankenhausträger nachweisen, dass er die datenschutzrechtlichen Voraussetzungen nach dem Landeskrankenhausgesetz erfüllt. Als entsprechender Nachweis ist eine Beschreibung des verwendeten Rechners, des Verfahrens der Datenverarbeitung und eine Beschreibung der gespeicherten Dateien in Form eines Verzeichnisses geeignet. In dem Verfahrensverzeichnis im Sinne von § 18 DSGVO M-V sollten auch die realisierten allgemeinen und speziellen Maßnahmen zur Datensicherheit enthalten sein.

Der Krankenhausarzt muss die Patientendaten sobald wie möglich **anonymisieren**. Da der Umgang mit anonymen Daten aus datenschutzrechtlicher Sicht unproblematisch ist, sollte jeder Arzt bestrebt sein, die Daten so zu speichern, dass ein Patient nicht bestimmbar ist.

Dem Landesbeauftragten für den Datenschutz obliegt die Kontrolle, ob die datenschutzrechtlichen Bestimmungen bei diesem Umgang mit Patientendaten durch den Krankenhausarzt eingehalten werden.

§ 21 Datenverarbeitung im Auftrag

§ 21 Abs. 1 LKHG M-V

Das Krankenhaus darf die Verarbeitung von Patientendaten einem Auftragnehmer übertragen, wenn

1. Störungen im Betriebsablauf sonst nicht vermieden werden können,
2. die Datenverarbeitung dadurch erheblich kostengünstiger gestaltet werden kann oder
3. das Krankenhaus seinen Betrieb einstellt.

Vor der Erteilung des Auftrags zur Verarbeitung von Patientendaten außerhalb des Krankenhauses ist zu prüfen, ob der Zweck auch mit verschlüsselten oder pseudonymisierten Patientendaten erreicht werden kann.

Die Verarbeitung von Patientendaten im Krankenhaus bietet umfassende Schutzmöglichkeiten gegen zweckentfremdete und unzulässige Nutzung. Insbesondere können Patientendaten, die im Krankenhaus verarbeitet werden, gemäß § 97 Abs. 2 StPO nicht beschlagnahmt werden. Dennoch kann es in einigen Fällen geboten sein, die Daten ausnahmsweise durch eine Stelle außerhalb des Krankenhauses verarbeiten zu lassen. Diese Fälle sind in Absatz 1 zusammengefasst.

Ein solcher Fall kann nach **Nummer 1** dann gegeben sein, wenn wegen eines Schadens an der Datenverarbeitungsanlage des Krankenhauses oder wegen einer sonstigen, bereits eingetretenen oder bevorstehenden Störung fremde Dienste in Anspruch genommen werden müssen.

Ferner soll dem Krankenhaus nach **Nummer 2** eine Datenverarbeitung im Auftrag außerhalb des Krankenhauses möglich sein, um Kostenvorteile zu realisieren, die sich durch die Zentralisierung der Datenverarbeitung bei einem anderen Krankenhaus oder bei einem gewerblichen Anbieter ergeben können. So können oft auch Teilvorgänge, auf die das Krankenhaus nicht eingerichtet ist, häufig durch gewerbliche Anbieter kostengünstiger erledigt werden, wie beispielsweise die **Mikroverfilmung** von Patientenakten.

Schließlich kann eine Übertragung des Datenbestandes und damit der Datenverarbeitung auf eine außenstehende Stelle immer auch dann gemäß **Nummer 3** erforderlich sein, wenn das Krankenhaus seinen Betrieb einstellt.

Für all diese Fälle der Datenverarbeitung durch außenstehende Stellen hat der Gesetzgeber auch ein Interesse der betroffenen Patienten an einer kostengünstigen und effektiven Dokumentation gesehen, so dass es gerechtfertigt ist, hier auf die sonst erforderlich werdende Einwilligung jedes einzelnen Patienten zu verzichten, wenn die in den Absätzen 3 bis 5 näher geregelten Sicherungen eingehalten werden. Die in der Datenübermittlung liegende Offenbarung der Daten erfolgt bei Einhaltung dieser Voraussetzungen dann „befugt“ im Sinne von § 203 Abs. 1 StGB.

Erfolgt die Datenverarbeitung automatisiert und außerhalb des Krankenhauses, wären **kryptographische Verfahren** zur Verschlüsselung und zum Schutz der Daten geeignete Maßnahmen, wenn die Entschlüsselung nur im Krankenhaus möglich ist. Die verschlüsselten Daten könnten dann selbst bei ihrer Beschlagnahme nicht gelesen werden.

Bei der **Archivierung** von Patientenakten außerhalb des Krankenhauses wäre zum Schutz der Daten eine Aufbewahrung in einem verschlossenen Container dann eine geeignete Maßnahme, wenn der Behälter nur im Krankenhaus geöffnet werden kann und der Auftragnehmer keine Kenntnis davon hat, von welchen Patienten sich welche Daten und Akten in dem Behälter befinden. Würde beispielsweise eine Akte eines bestimmten Patienten von dem Krankenhaus benötigt werden, so könnte dieses mit Hilfe eines Verzeichnisses feststellen, in welchem Behälter sich die Akte befindet. Das Archivierungsunternehmen transportiert den Behälter mit der ermittelten Nummer in das Krankenhaus, wo er aufgeschlossen und die Akte entnommen wird. Anschließend wird der Behälter wieder verschlossen dem Unternehmen zur Aufbewahrung übergeben.

§ 21 Abs. 2 LKHG M-V

Eine über drei Monate hinausgehende Speicherung von Patientendaten durch den Auftragnehmer ist außerhalb des Krankenhauses nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für das Krankenhaus verwahrt.

Während Absatz 1 für eine Datenverarbeitung sowohl innerhalb als auch außerhalb des Krankenhausgeländes gilt, trifft Absatz 2 für eine dauerhafte Speicherung außerhalb des Krankenhauses wegen der damit verbundenen erhöhten Gefährdung zusätzliche Einschränkung. Die Regelung gilt dann, wenn die Daten mehr als drei Monate vom Auftragnehmer gespeichert und verarbeitet werden. Damit sollen die nur vorübergehenden, nicht länger als drei Monate dauernde Speicherungen, wie sie zum Beispiel bei der Erstellung von Leistungsabrechnungen erforderlich werden, nicht erschwert werden.

Geht die Speicherung zeitlich über drei Monate hinaus, sind die Patientendaten auf getrennten Datenträgern zu speichern, die der Auftragnehmer für das Krankenhaus verwahrt. Dieses **Trennungsgebot** bedeutet, dass Patientendaten aus dem ärztlichen Bereich von denen aus dem reinen Verwaltungsbereich physisch getrennt, das heißt nicht in einer Datei, zu verarbeiten sind. Diese Trennung erleichtert die Unterscheidung zwischen den Daten, die aufgrund einer gesetzlichen Regelung übermittelt werden dürfen (z. B. § 301 SGB V), und den Daten, die – weil es keine Übermittlungsvorschrift gibt – mit Einwilligung oder unter den Voraussetzungen für die sonstige Datenverarbeitung im Auftrag übermittelt und verarbeitet werden dürfen.

Durch den Zusatz, dass die Patientendaten vom Auftragnehmer für das Krankenhaus zu „verwahren“ sind, bringt der Gesetzgeber im Hinblick auf § 97 Abs. 2 StPO zum Ausdruck, dass sich die Daten auch beim Auftragnehmer noch „im Gewahrsam“ des Krankenhauses befinden und damit nicht ohne weiteres beschlagnahmt werden dürfen, weil dem Krankenhaus auch weiterhin das Bestimmungsrecht zusteht.

§ 21 Abs. 3 LKHG M-V

Der Auftragnehmer ist vom Krankenhaus sorgfältig auszuwählen. Die Einzelheiten des Auftrags und die vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherungsmaßnahmen sind schriftlich zu vereinbaren. Eine Abschrift der Vereinbarung hat das Krankenhaus dem Landesbeauftragten für den Datenschutz unverzüglich zu übersenden.

In § 14 Abs. 2 LKHG M-V wird § 4 DSGVO M-V (Verarbeitung von personenbezogenen Daten im Auftrag) von der entsprechenden Anwendung ausdrücklich ausgenommen. Dies gilt entsprechend auch für § 11 BDSG (Datenverarbeitung im Auftrag), auch wenn § 14 Abs. 2 LKHG M-V dies nicht ausdrücklich sagt (siehe hierzu Seite 12). Einzelne Regelungen des § 4 DSGVO M-V bzw. des § 9 BDSG sind aber auch bei der **Auftragsdatenverarbeitung** von Patientendaten im Krankenhaus sinnvoll. Daher sind diese Regelungen in den Absätzen 3 und 4 sinngemäß wiedergegeben worden.

Auch wenn das Krankenhaus die Datenverarbeitung auf einen Auftragnehmer überträgt, bleibt es dafür verantwortlich, dass die Verarbeitung den gesetzlichen Bestimmungen entsprechend erledigt und das Datenschutzrecht eingehalten wird. Ansprüche der Patienten, die sich aus der Verarbeitung ihrer personenbezogenen Daten ergeben, wie beispielsweise Berichtigung (§ 13 Abs. 1 DSGVO M-V, § 35 Abs. 1 BDSG) oder Löschung und Sperrung der Daten (§ 19 LKHG), sind gegen das auftraggebende Krankenhaus zu richten. Die Übertragung der Datenverarbeitung auf Dritte ändert daran nichts. Vielmehr hat sich das Krankenhaus dann bei dem Auftragnehmer durch Regressansprüche schadlos zu halten. Das Krankenhaus hat daher auch im eigenen Interesse bei der Auswahl eines geeigneten Auftragnehmers darauf zu achten, dass dieser in der Lage ist, die hohen Anforderungen, einschließlich der erforderlichen Sicherheitsmaßnahmen nach §§ 21 und 22 DSGVO M-V oder § 9 BDSG, tatsächlich zu erfüllen, die an die Verarbeitung von Patientendaten gestellt werden.

Der Auftrag ist schriftlich zu erteilen. In diesem sind beispielsweise die Verantwortungsgebiete von Auftragnehmer und Auftraggeber abzugrenzen, Art, Umfang und Dauer der Verarbeitung der personenbezogenen Daten zu regeln und die vom Auftragnehmer zu treffenden, allgemeinen und speziellen Sicherungsmaßnahmen nach §§ 21 und 22 DSGVO M-V bzw. § 9 BDSG festzulegen. Darüber hinaus ist in Absatz 3 Satz 3 vorgesehen,

dass der Landesbeauftragte für den Datenschutz nicht nur zu informieren ist (§ 4 Abs. 3 DSG M-V), sondern eine Abschrift der Vereinbarung über die Datenverarbeitung erhält.

§ 21 Abs. 4 LKHG M-V

Der Auftragnehmer darf die ihm überlassenen Patientendaten nur im Rahmen des Auftrags und der Weisungen des Krankenhauses verarbeiten. Sofern die §§ 14 bis 20 für den Auftragnehmer nicht gelten, hat das Krankenhaus sicherzustellen, dass der Auftragnehmer diese Vorschriften entsprechend anwendet und sich insoweit der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

Die dem Auftragnehmer übermittelten Patientendaten sind **zweckgebunden**. Er darf sie nur im Rahmen des Auftrages und der Weisungen des Krankenhauses verarbeiten. Geht der Auftragnehmer bei der Datenverarbeitung über diesen Grundsatz hinaus, handelt er unbefugt und setzt sich Schadensersatzansprüchen aus dem Vertrag mit dem Krankenhaus oder gar der Beendigung des Auftragsverhältnisses durch eine außerordentliche Kündigung aus. Gegenüber den betroffenen Patienten haftet das Krankenhaus als verantwortliche Stelle der Datenverarbeitung.

Satz 2 stellt sicher, dass hinsichtlich des Patientendatenschutzes beim Auftragnehmer – unabhängig von seiner Rechtsnatur – zumindest im Ergebnis dieselben Vorschriften gelten, wie sie für das Krankenhaus im Rahmen der §§ 14 bis 20 LKHG M-V gelten (zur Anwendbarkeit der sonstigen allgemeinen Datenschutzvorschriften des DSG M-V oder des BDSG siehe Seite 12). Eine direkte Anwendung der §§ 14 bis 20 LKHG M-V hätte wegen des begrenzten Geltungsbereichs von Landesgesetzen nur für im Land Mecklenburg-Vorpommern, nicht aber für in anderen Bundesländern ansässige Auftragnehmer geregelt werden können. Das Krankenhaus hat daher sicherzustellen, dass der Auftragnehmer diese Vorschriften des LKHG M-V entsprechend anwendet. Dies erfolgt in der Regel dadurch, dass sich der Auftragnehmer vertraglich diesen Vorschriften unterwirft. Die Unterwerfung unter die Kontrolle des Landesbeauftragten für den Datenschutz erfolgt in gleicher Weise durch eine entsprechende Erklärung des Auftragnehmers im Vertrag.

An sich besteht die Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern (LfD M-V) hinsichtlich der Verarbeitung personenbezogener Daten und der Einhaltung der Vorschriften des DSG M-V nur gegenüber den öffentlichen Stellen des Landes, § 2 DSG M-V. Vor diesem Hintergrund könnte man in den Fällen der privatrechtlich geführten Krankenhäuser annehmen, dass der LfD M-V hinsichtlich der Übersendung der Abschrift der Vereinbarung wegen fehlender Kontrollzuständigkeit bei privaten Krankenhäusern falscher Adressat dieser Vertragsabschrift ist. § 21 Abs. 4 LKHG M-V macht aber deutlich, dass, sofern die Vorschriften §§ 14 bis 20 LKHG M-V für den Auftragnehmer nicht gelten (weil er keine Einrichtung im Sinne des Krankenhausgesetzes ist), sich der Auftragnehmer der Kontrolle des LfD M-V unterwerfen soll. Mit dieser Unterwerfung wird eine Kontrollzuständigkeit für den LfD M-V gemäß § 30 DSG M-V begründet. Insoweit ist es daher auch erforderlich, dass der LfD M-V unaufgefordert von der Übertragung der Datenverarbeitung auf einen Auftragnehmer und damit von seiner Kontrollzuständigkeit gerade für diese Stelle erfährt. Dass damit letztlich ein Auseinanderfallen der Kontrollkompetenzen verbunden sein kann (private Krankenhäuser – Datenschutzaufsichtsbehörde im Innenministerium, privater Auftragnehmer – LfD M-V aufgrund Unterwerfung), scheint vom Gesetzgeber so gewollt zu sein. Besser wäre es hingegen, wenn die Kontrollzuständigkeit für beide Stellen – Krankenhaus und Auftragnehmer – in einer Hand wären.

Ist der Auftragnehmer eine nicht-öffentliche Stelle, gelten für ihn außerdem § 11 Abs. 3 und 4 BDSG und damit beispielsweise die Vorschrift § 5 BDSG über das Datengeheimnis.

§ 21 Abs. 5 LKHG M-V

Eine Übertragung des Auftrages auf Dritte oder die Erteilung von Unteraufträgen ist nur mit Zustimmung des Krankenhauses zulässig. Die Absätze 2 bis 4 gelten entsprechend.

In dem Vertrag über die Datenverarbeitung im Auftrag wird in der Regel ein Passus enthalten sein, der eine Übertragung des Auftrages an Dritte oder die Erteilung von **Unteraufträgen** durch den Auftragnehmer nach vorheriger Zustimmung ausdrücklich zulässt oder ausschließt. Mit der Übertragung des Auftrages oder der Unterbeauftragung kommt ein neuer oder ein weiterer Auftragnehmer hinzu, der mit der Datenverarbeitung ebenfalls Kenntnis von den personenbezogenen Daten der Patienten nimmt. Der Kreis ändert sich daher oder wird größer und gegebenenfalls auch unübersichtlicher. Um dennoch einen hinreichenden Schutz der Patientendaten zu gewährleisten und um zu verhindern, dass das Krankenhaus die Beherrschung „seiner“ Daten durch eine weitverzweigte Verlagerung der Aufgabenbereiche durch Erteilung von Unteraufträgen verliert, sieht Absatz 5 eine ausdrückliche Zustimmung des Krankenhauses vor. Durch den Verweis auf die entsprechende Geltung der Absätze 2 bis 4 soll sichergestellt werden, dass auch für diese Auftragnehmer dieselben Schutzvorschriften wie beim ursprünglichen Auftrag gelten. So muss auch hier das Krankenhaus den Auftragnehmer nach seiner Geeignetheit auswählen und in einem schriftlichen Vertrag mit diesem die Vertragsbedingungen festlegen, wie sie die Absätze 2 bis 4 vorschreiben.

§ 21 Abs. 6 LKHG M-V

Übernimmt der Auftragnehmer nach einer Betriebseinstellung eines Krankenhauses den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle hinsichtlich der Verarbeitung dieser Daten die Vorschriften dieses Abschnitts. Bei der Übernahme ist vertraglich sicherzustellen, dass Patientendaten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten.

Absatz 6 trifft eine Regelung für den Sonderfall, dass ein Krankenhaus **aufgelöst** wird. Wenn ein Krankenhaus als Rechtsträger wegfällt, ist eine mittelbare Verwahrung „für das Krankenhaus“ im Sinne von Absatz 2 und damit ein entsprechender **Beschlagnahmeschutz** nicht mehr möglich. Gleichwohl ist es im Interesse der Patienten dringend erforderlich, dass die Patientendaten nicht vernichtet werden, sondern für Rückfragen und als Basis für spätere Behandlungen weiterhin zur Verfügung stehen. In einem solchen Sonderfall übernimmt der Auftragnehmer die Verantwortung hinsichtlich der Verarbeitung dieser von ihm übernommenen Daten und der Einhaltung der Datenschutzbestimmungen. Für ihn gelten dann insoweit die Bestimmungen der §§ 14 bis 21 LKHG M-V.

Die in Satz 2 genannte Frist von zehn Jahren knüpft an die für ärztliche Aufzeichnungen geltende Aufbewahrungsfrist in § 10 Abs. 3 BOÄ M-V an. Bei der Übertragung der Verantwortlichkeiten ist vertraglich sicherzustellen, dass die betroffenen Patienten in gleicher Weise wie bisher für die Dauer von zehn Jahren nach Abschluss der Behandlung Auskunft und Einsicht in ihre Unterlagen erhalten. Hierdurch soll gewährleistet werden, dass die von der Auflösung des Krankenhauses betroffenen Patienten nicht schlechter gestellt werden, als die Patienten, deren Krankenhaus nicht aufgelöst wurde.

§ 22 Beauftragte für den Datenschutz (aufgehoben)

Die ursprünglich im LKHG M-V geregelte Pflicht, einen Datenschutzbeauftragten zu bestellen, ist durch das Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 28. März 2002 nicht gänzlich weggefallen, sondern gilt durch den in § 14 geregelten Verweis auf § 20 DSG M-V (Behördlicher Datenschutzbeauftragter) für den öffentlich-rechtlichen Krankenhausbereich fort. Für Krankenhäuser in privater Trägerschaft gelten §§ 4f, 4g BDSG, im kirchlichen Bereich das kirchliche Datenschutzrecht.

Die weiteren Ausführungen beziehen sich nur auf § 20 DSG M-V. Bei etwaigen Fragen zum Beauftragten für den Datenschutz in privaten Krankenhäusern sind diese an die Datenschutzaufsichtsbehörde für den privaten Bereich im Innenministerium zu richten.

In § 20 DSG M-V heißt es:

(1) Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Der behördliche Datenschutzbeauftragte soll Beschäftigter der Daten verarbeitenden Stelle sein; soweit dadurch die Erfüllung seiner Aufgaben nicht beeinträchtigt wird, können mehrere Daten verarbeitende Stellen denselben behördlichen Datenschutzbeauftragten bestellen. Bestellt werden darf nur, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt. Der behördliche Datenschutzbeauftragte ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes unabhängig und weisungsfrei. Er ist dem Leiter der öffentlichen Stelle unmittelbar unterstellt, kann sich direkt an ihn wenden und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Beschäftigten der Daten verarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

(2) Die Bestellung zum behördlichen Datenschutzbeauftragten kann befristet werden. Sie kann schriftlich widerrufen werden, wenn ein Interessenkonflikt mit seinen anderen dienstlichen Aufgaben eintritt oder sonst ein wichtiger Grund in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches vorliegt. Vor der Entscheidung über den Widerruf ist der behördliche Datenschutzbeauftragte zu hören.

(3) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu überwachen und Hinweise zur Umsetzung zu geben. Er kann Auskünfte verlangen und Einsicht in Akten und Dateien nehmen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Berufs- und Amtsgeheimnisse können ihm nicht entgegengehalten werden. Zu seiner Unterstützung kann er sich jederzeit an den Landesbeauftragten für den Datenschutz wenden. Zu seinen Aufgaben gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 18, 21 und 22 erforderlichen Maßnahmen zu unterstützen,
4. das Verzeichnis nach § 18 zu führen und
5. die Vorabkontrolle nach § 19 durchzuführen.

(4) Das Verzeichnis nach § 18 Abs. 1 kann von jedermann eingesehen werden. Dies gilt nicht für die Angaben nach § 18 Abs. 1 Nr. 7 und die Verfahren, die nach § 24 Abs. 4 Nr. 2 und 3 nicht der Auskunftspflicht unterliegen.

§ 20 DSGVO M-V führt die ausnahmslose **Verpflichtung** jeder Daten verarbeitenden Stelle des Landes ein, einen **behördlichen Datenschutzbeauftragten** zu bestellen. Die Vorschrift sieht damit zwingend eine interne Eigenkontrolle durch eine institutionalisierte Instanz vor. Die Bezeichnung „behördlicher Datenschutzbeauftragter“ ist missverständlich, da die Pflicht, einen Datenschutzbeauftragten zu bestellen, für alle öffentlichen Stellen im Sinne von § 2 DSGVO M-V gilt, die personenbezogene Daten für sich verarbeiten oder durch andere in ihrem Auftrag verarbeiten lassen und somit Daten verarbeitende Stellen gemäß § 3 Abs. 5 DSGVO M-V sind.

Dieser Paragraph regelt detailliert **die Bestellung, die Aufgaben und die Befugnisse des Datenschutzbeauftragten** und orientiert sich dabei an den seit langem bewährten Regelungen des Bundesdatenschutzgesetzes für einen betrieblichen Datenschutzbeauftragten bei nicht-öffentlichen Stellen. Neben der Kontrolle haben dabei vor allem die Beratung und die Begleitung datenschutzrelevanter Projekte eine herausragende Bedeutung. Der Datenschutzbeauftragte ist deshalb frühzeitig in Prozesse einzubinden, damit er sein Wissen und seine Erfahrungen einbringen, auf datenschutzrelevante Aspekte hinweisen und entsprechende Empfehlungen geben kann. Damit diese Aufgabe auch in angemessener Art und Weise wahrgenommen wird, muss er über die notwendige persönliche sowie fachliche Eignung verfügen und organisatorisch in besonderer Weise in die Verwaltung eingebunden werden. Der Gesetzgeber hat den behördlichen Datenschutzbeauftragten mit weitreichenden Befugnissen ausgestattet.

Die Pflicht des Datenschutzbeauftragten zur **Verschwiegenheit** ergibt sich unmittelbar aus § 6 DSGVO M-V (Datengeheimnis) und besteht auch nach Beendigung seiner Tätigkeit fort. Die Verpflichtung darauf ist mit der Bestellung durch den Leiter der Daten verarbeitenden Stelle vorzunehmen.

Absatz 1 regelt die Bestellung und Rechtsstellung des Datenschutzbeauftragten. Ferner werden die von ihm zu erfüllenden Anforderungen festgelegt. Darüber hinaus enthält die Vorschrift ein Anrufungsrecht gegenüber dem behördlichen Datenschutzbeauftragten für Mitarbeiter der Daten verarbeitenden Stelle.

Die **Bestellung** des behördlichen Datenschutzbeauftragten hat schriftlich zu erfolgen. In der Niederschrift sind alle wesentlichen Punkte, die die Wahrnehmung dieser Tätigkeit betreffen, detailliert festzuhalten. Neben einer umfassenden Aufgabenbeschreibung gehören hierzu auch die Rechte und Pflichten des behördlichen Datenschutzbeauftragten sowie organisatorische Regelungen. Ein Muster für die Bestellung ist im Anhang abgedruckt.

Die Bestellung ist in der Daten verarbeitenden Stelle allen Mitarbeitern bekannt zu geben, zum Beispiel durch Hausmitteilung oder Aushang. In diesem Zusammenhang ist auch über die Aufgaben und Befugnisse des behördlichen Datenschutzbeauftragten zu **unterrichten**. Nur wenn die Aufgaben und die Person entsprechend bekannt sind, kann der Datenschutzbeauftragte seine Funktion wirksam und im Interesse der Dienststelle wahrnehmen. Die Mitarbeiter sind darauf hinzuweisen, dass sie verpflichtet sind, den Datenschutzbeauftragten über datenschutzrelevante Vorhaben, insbesondere die Einführung neuer Verfahren, rechtzeitig zu informieren, ihn bei der Durchführung seiner Aufgaben, vor allem bei datenschutzrechtlichen Prüfungen, umfassend zu unterstützen und

schutzrechtlichen Prüfungen, umfassend zu unterstützen und die von ihm geforderten notwendigen Zuarbeiten zu erbringen.

Darüber hinaus ist auch ein **Vertreter** zu bestellen, der in Abwesenheit des behördlichen Datenschutzbeauftragten dessen Aufgaben wahrnimmt. Der behördliche Datenschutzbeauftragte und sein Vertreter müssen vertrauensvoll zusammenarbeiten und ihr Tätigwerden abstimmen. Durch den Vertreter ist gewährleistet, dass bei einem – zum Beispiel krankheitsbedingten – Ausfall des behördlichen Datenschutzbeauftragten Aufgaben nicht über einen längeren Zeitraum liegen bleiben, Vorhaben nicht ohne datenschutzrechtliche Prüfung durchgeführt werden und für die Mitarbeiter ständig ein Ansprechpartner in allen Datenschutzfragen zur Verfügung steht. Für den Vertreter gelten diese Vorschriften deshalb in gleichem Maße.

Wegen der umfassenden Kontrollrechte des behördlichen Datenschutzbeauftragten und den damit verbundenen weitreichenden Befugnissen soll diese Funktion grundsätzlich durch einen **Beschäftigten der Daten verarbeitenden Stelle** wahrgenommen werden. Ausnahmen hiervon sind zwar möglich, so dass auch Externe (in erster Linie Beschäftigte anderer öffentlicher Stellen) als Datenschutzbeauftragte bestellt werden können, jedoch ist dies nur in eng begrenzten Fällen zulässig. Der Gesetzeswortlaut „soll“ verdeutlicht die restriktive Auslegung, da er eine Verpflichtung deutlich macht, von der nur in einem besonders gelagerten Ausnahmefall abgewichen werden darf. Ein solcher Bedarf könnte beispielsweise in besonders kleinen öffentlichen Stellen bestehen, die aufgrund ihrer geringen Personalstärke diese Aufgabe nicht durch einen eigenen Mitarbeiter wahrnehmen können. Dies ist im Einzelfall sehr genau zu prüfen und zu begründen. Auch ein Externer, der zum behördlichen Datenschutzbeauftragten bestellt wird, unterliegt der Kontrolle durch den Landesbeauftragten für den Datenschutz. Da er nicht in die Verwaltung eingebunden ist, sind über die in der Anlage bereits genannten Anforderungen hinaus noch weitere Festlegungen zur Verarbeitung personenbezogener Daten im Rahmen der Kontrollbefugnisse zu treffen.

§ 20 Abs. 1 Satz 2 2. Alternative DSGVO M-V erlaubt es ausdrücklich, einen **gemeinsamen Datenschutzbeauftragten** für mehrere Daten verarbeitende Stellen mit diesen Aufgaben zu betrauen. Vor allem kleinere Einrichtungen können so ohne übermäßigen Aufwand fachliche Kompetenz bündeln und effektiv nutzen. In diesem Fall sind Art und Umfang der Tätigkeit bei den einzelnen Stellen konkret festzulegen, um so eine effektive und abgestimmte Aufgabenwahrnehmung zu gewährleisten. Auch im Hinblick auf die anteilige Finanzierung durch die beteiligten Stellen empfiehlt es sich, die Tätigkeiten vom inhaltlichen und zeitlichen Umfang genau zu definieren. Der gemeinsame (externe) Datenschutzbeauftragte verfügt dann auch bei den Stellen, deren Mitarbeiter er nicht ist, über die in der Vorschrift beschriebenen Rechte und Pflichten.

Behördliche Datenschutzbeauftragte haben Zugang zu sensiblen personenbezogenen Daten (vgl. Absatz 3 Sätze 2 und 3). Werden **Mitarbeiter nicht-öffentlicher Stellen** oder **Privatpersonen** dazu bestellt, so ist der datenschutzgerechte Umgang mit diesen Daten bei ihnen wesentlich schwerer zu gewährleisten und durch den Landesbeauftragten für den Datenschutz zu kontrollieren als bei Mitarbeitern öffentlicher Stellen.

Aufgrund dieser Ausführungen ergibt sich bei der Prüfung, wer als behördlicher Datenschutzbeauftragter der öffentlichen Stelle X zu bestellen ist, eine Rangfolge, wobei die nächste Stufe erst dann in Betracht kommt, wenn auf der vorhergehenden eine Bestellung aus wichtigen Gründen ausscheidet:

- Mitarbeiter der öffentlichen Stelle X
- Mitarbeiter der öffentlichen Stelle Y, der auch behördlicher Datenschutzbeauftragter der öffentlichen Stelle Y ist
- Mitarbeiter der öffentlichen Stelle Y, der nicht behördlicher Datenschutzbeauftragter der öffentlichen Stelle Y ist
- Mitarbeiter einer nicht-öffentlichen Stelle oder Privatperson

Der **Personalrat** sollte bei der Bestellung des behördlichen Datenschutzbeauftragten wegen dessen weitreichender Kontrollbefugnisse beteiligt werden.

Vor allem für allgemeine Fragen der Organisation der Verfahren und für technische Beratungen können darüber hinaus auch private Dienstleister oder sonstige Externe als Sachverständige herangezogen werden. Im Bereich der Aufgaben nach Abs. 3 Satz 5 Nr. 2 bis 4 kann ein externer „Datenschutzberater“ den behördlichen Datenschutzbeauftragten in erheblichem Umfang entlasten. Ist dies der Fall, so kommt auch in Betracht, den behördlichen Datenschutzbeauftragten in geringerem Maße von anderen Aufgaben freizustellen, als es sonst erforderlich wäre. Zugriff auf personenbezogene Daten darf den externen Beratern jedoch nur im Einzelfall dann gewährt werden, wenn der Betroffene zugestimmt hat. Die in dieser Vorschrift genannten Aufgaben verbleiben aber trotz der unterstützenden Hilfstätigkeiten durch Externe in der Verantwortung des behördlichen Datenschutzbeauftragten.

Um den von Art. 18 Abs. 2 der Datenschutzrichtlinie des Europäischen Parlamentes und Rates vom 24. Oktober 1995 geforderten effektiven Datenschutz zu gewährleisten, hat der Datenschutzbeauftragte einige Mindestanforderungen hinsichtlich seiner fachlichen und persönlichen Eignung zu erfüllen. So muss er über die erforderliche Sachkunde und Zuverlässigkeit verfügen.

Die besondere Vertrauensstellung des behördlichen Datenschutzbeauftragten und seine weitreichenden Befugnisse, unter anderem in Unterlagen und Dateien mit zum Teil sehr sensiblen personenbezogenen Daten einsehen zu können, erfordern eine integre und zuverlässige Persönlichkeit. Neben der Verschwiegenheit kommt es dabei auch auf Eigenschaften wie Verantwortungsbewusstsein und Durchsetzungsvermögen an. Soweit im Einzelfall keine besonderen Anhaltspunkte, zum Beispiel über einschlägige Verurteilungen, vorliegen, wird man davon ausgehen können, dass die Zuverlässigkeit bei den Mitarbeiterinnen und Mitarbeitern des öffentlichen Dienstes gegeben ist.

Zur erforderlichen **Sachkunde** gehört die Kenntnis der maßgeblichen Datenschutzregelungen und ein Mindestmaß an technischem Verständnis, um die automatisierte Verarbeitung personenbezogener Daten kontrollieren zu können. Ferner sollte der behördliche Datenschutzbeauftragte die Verwaltungsabläufe in der Daten verarbeitenden Stelle kennen. Externe und Berufsanfänger erfüllen dieses Kriterium in aller Regel nicht.

Der Leiter der Daten verarbeitenden Stelle ist verantwortlich, dass diese Voraussetzungen erfüllt sind, und hat sich hiervon vorab zu überzeugen. Sollen Personen zu Datenschutzbeauftragten bestellt werden, bei denen diese Kenntnisse bisher nicht oder nicht in ausreichendem Maße vorliegen, so ist ihnen noch vor der Bestellung Gelegenheit zu geben, sich in entsprechenden Kursen zu qualifizieren und die erforderlichen Kenntnisse zu erwerben. Gleiches gilt für den zu bestellenden Vertreter. Es reicht beispielsweise nicht aus, wenn dieser erst zum Zeitpunkt des Ausfalls des behördlichen Datenschutzbeauftragten die notwendigen Fähigkeiten und Kenntnisse bei Fortbildungen erwirbt. Eine solche Verfahrens-

weise wäre zum einen praxisfern und stände zum anderen im Widerspruch zum Willen des Gesetzgebers.

Darüber hinaus hat sich auch der behördliche Datenschutzbeauftragte im Rahmen seiner Tätigkeit regelmäßig fortzubilden, um den aus der rasanten technischen Entwicklung und den neuen datenschutzrechtlichen Regelungen resultierenden erhöhten Anforderungen gerecht zu werden. Auch der Erfahrungsaustausch mit anderen behördlichen Datenschutzbeauftragten, zum Beispiel bei Workshops, kann ihm dabei für seine Arbeit wichtige Impulse geben und ein geeignetes Mittel der Fortbildung sein. Informationen über Schulungs- und Fortbildungsangebote können beim Landesbeauftragten für den Datenschutz erfragt werden.

Die Tätigkeit des behördlichen Datenschutzbeauftragten darf zu keiner **Interessenkollision** mit seinen anderen dienstlichen Aufgaben führen. Damit scheidet zum Beispiel die Bestellung des Leiters der IT-Abteilung grundsätzlich aus. Entsprechendes gilt für den Leiter der Daten verarbeitenden Stelle sowie den Leiter der Personalakten führenden Stelle, da hier Entscheidungs- und Kontrollfunktion in einer Hand lägen. Besteht bei der Daten verarbeitenden Stelle eine Organisationseinheit, die für die Rechnungsprüfung zuständig ist, so hat es sich bewährt, einem Mitarbeiter dieser Stelle die Aufgabe des Datenschutzbeauftragten zu übertragen. Ebenso kommt die Übernahme dieser Aufgabe durch einen Mitarbeiter der Rechtsabteilung in Betracht. Auch die Bündelung mit anderen Aufgaben, wie kommunaler Ausländerbeauftragter, bietet sich gegebenenfalls an. Dies ist im Einzelfall genau zu prüfen.

Die **Rechtsstellung** des behördlichen Datenschutzbeauftragten innerhalb der öffentlichen Stelle wurde in Anlehnung an die des Landesdatenschutzbeauftragten ausgestaltet. Satz 4 regelt ausdrücklich, dass der Datenschutzbeauftragte in Ausübung seiner Tätigkeit unabhängig und weisungsfrei ist. Somit legt der Datenschutzbeauftragte weitgehend selbst die Schwerpunkte seiner Arbeit fest. In seiner Funktion ist er dem Leiter der öffentlichen Stelle unmittelbar unterstellt. Diese organisatorische Regelung macht deutlich, dass trotz der gesetzlich vorgeschriebenen Institution des Datenschutzbeauftragten der Leiter von der eigenen Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen nicht freigestellt ist. Die Anbindung an die Behördenleitung sichert dem behördlichen Datenschutzbeauftragten gleichzeitig ein unmittelbares Vortragsrecht beim Leiter der Verwaltung, was insbesondere bei unterschiedlichen Auffassungen zwischen Datenschutzbeauftragten und einzelnen Verwaltungseinheiten von Bedeutung ist. Dieses ist auch deshalb notwendig, da der behördliche Datenschutzbeauftragte keine Weisungsbefugnis besitzt.

Eine Benachteiligung des behördlichen Datenschutzbeauftragten wegen der Ausübung seines Amtes, etwa wegen nicht genehmer interner Prüfungen oder wegen der Weitermeldung von Missständen an den Landesbeauftragten für den Datenschutz, ist unzulässig. Die Vorschrift stellt klar, dass nachteilige arbeitsrechtliche oder beamtenrechtliche Maßnahmen, die auf die Wahrnehmung der Tätigkeit eines Datenschutzbeauftragten zurückgehen, unwirksam sind.

Satz 6 sieht vor, dass die Beschäftigten der Dienststelle sich ohne Einhaltung des Dienstweges in allen datenschutzrechtlichen Angelegenheiten an den behördlichen Datenschutzbeauftragten wenden können. Dies betrifft sowohl Sachverhalte, in denen eigene datenschutzrechtliche Belange berührt sind, als auch solche, die die Verarbeitung anderer personenbezogener Daten durch die Dienststelle betreffen. Dabei kann es zum Beispiel um Verstöße gegen datenschutzrechtliche Bestimmungen oder um Aspekte der Datensicherheit

gehen. Wer von dieser Möglichkeit Gebrauch macht, darf hierdurch keinen nachteiligen Folgen ausgesetzt sein. Hierauf sollten die Mitarbeiter ebenfalls hingewiesen werden.

Der Datenschutzbeauftragte muss die Identität von Betroffenen – Patienten als auch Mitarbeitern des Krankenhauses – verschweigen, die sich an ihn wenden, und darf auch keine Umstände preisgeben, die eine Identifizierung ermöglichen. Sollten zur Klärung eines Sachverhaltes Daten zur Identifizierung erforderlich sein, so muss zur Verwendung dieser Daten das Einverständnis der Betroffenen vorliegen.

Der Datenschutzbeauftragte muss über die Unterlagen verfügen, die zur Erfüllung seiner Aufgabe erforderlich sind, insbesondere ist dies das Verzeichnisse nach § 18 DSGVO. Darüber hinaus sind ihm – soweit für weitere Aufgaben erforderlich – Hilfspersonal, Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Nach Absatz 2 ist es möglich, den behördlichen Datenschutzbeauftragten befristet zu bestellen. Eine **Befristung** kommt beispielsweise in Frage, wenn diese Aufgabe nur vorübergehend wahrgenommen werden soll oder um anfänglich möglichen Kollisionen mit sonstiger hoher Arbeitsbelastung zu entgehen und gegebenenfalls bei auftretenden Schwierigkeiten entsprechend zu handeln. Eine missbräuchliche Nutzung der Befristung, um etwa einen aus Sicht der Daten verarbeitenden Stelle zu unbequemen behördlichen Datenschutzbeauftragten auch ohne Vorliegen der in Satz 2 genannten Gründe nicht auf Dauer zu haben, widerspricht der Intention des Gesetzgebers.

Ein **Widerruf** der Bestellung ist nur vorgesehen, wenn es zu einem vorher nicht absehbaren Interessenkonflikt mit den sonstigen dienstlichen Aufgaben des behördlichen Datenschutzbeauftragten kommt oder sonst ein wichtiger Grund in entsprechender Anwendung von § 626 BGB vorliegt. Eine wiederholte Befristung ohne erkennbaren sachlichen Grund würde dazu führen, dass die hohen Anforderungen an den Widerruf einer Bestellung umgangen werden, und wäre somit unzulässig. Vor einem Widerruf ist der behördliche Datenschutzbeauftragte anzuhören.

Absatz 3 nennt die wesentlichen **Aufgaben** und damit verbunden weitere **Befugnisse** des behördlichen Datenschutzbeauftragten. Seine Rechte entsprechen weitgehend denen des Landesdatenschutzbeauftragten und sollen es ihm ermöglichen, für eine effektive Umsetzung der datenschutzrechtlichen Bestimmungen zu sorgen.

Die zentrale Aufgabe des behördlichen Datenschutzbeauftragten ist die Überwachung der datenschutzrechtlichen Vorschriften – durch anlassbezogene oder routinemäßige Kontrollen – und die Unterstützung der Daten verarbeitenden Stelle bei ihren Bemühungen, diese einzuhalten. Die Überwachung ist kein Selbstzweck. Stellt der behördliche Datenschutzbeauftragte Fehler oder Mängel fest, so hat er die Daten verarbeitende Stelle darauf hinzuweisen und ihr dabei zu helfen, rechtmäßige Zustände herzustellen.

Der behördliche Datenschutzbeauftragte ist Berater für die Dienststellenleitung sowie die Mitarbeiter in allen Datenschutzfragen. Die Hinweise zur Umsetzung der datenschutzrechtlichen Bestimmungen können sich auf alle Sachverhalte beziehen, bei denen es um die Verarbeitung personenbezogener Daten geht, zum Beispiel auf die Aktenführung, den Inhalt und die Gestaltung von Formularen zur Datenerhebung, die Einhaltung von Löschungsfristen, die ordnungsgemäße Datenträgervernichtung, den Einsatz von datenschutzgerechter Soft- und Hardware, die Beseitigung von Schwachstellen und Risiken bei der

Datensicherheit, die Unterrichtung von Betroffenen, die Zulässigkeit der Datenverarbeitung in Einzelfällen etc.

Um effektiv zu kontrollieren, kann der behördliche Datenschutzbeauftragte **Auskünfte** verlangen und selbst **Einsicht** in Akten und Dateien nehmen, soweit dies für seine Aufgabenerfüllung erforderlich ist. Über die Erforderlichkeit entscheidet er eigenverantwortlich. Die in diesem Zusammenhang notwendigen Zuarbeiten sind durch die Mitarbeiter der öffentlichen Stelle zu erbringen. Bei Prüfungen kann die jeweilige Stelle die Herausgabe von Unterlagen oder Auskünfte nicht mit dem Hinweis verweigern, dass diese Daten für die Wahrnehmung der Kontrollbefugnisse nicht erforderlich seien. Berufs- und Amtsgeheimnisse können ihm ebenfalls nicht entgegengehalten werden. Demzufolge steht ihm ein uneingeschränktes Kontrollrecht zu, zum Beispiel auch bei Daten, die dem Steuergeheimnis gemäß § 30 AO unterliegen. Die personenbezogenen Daten, die der behördliche Datenschutzbeauftragte bei der Wahrnehmung seiner Kontrollaufgabe zur Kenntnis nimmt und gegebenenfalls speichert, unterliegen der Zweckbindung.

Der behördliche Datenschutzbeauftragte ist jederzeit berechtigt, sich an den Landesbeauftragten für den Datenschutz zu wenden, um von dort Hinweise und Unterstützung zu erhalten. Dies kann sich auf allgemeine datenschutzrechtliche Fragen, aber beispielsweise auch auf Sachverhalte beziehen, die zwischen dem behördlichen Datenschutzbeauftragten und der Dienststellenleitung strittig sind. Ob, in welcher Art und Weise sowie zu welchem Zeitpunkt der behördliche Datenschutzbeauftragte hiervon Gebrauch macht, entscheidet er grundsätzlich in eigener Verantwortung. Im Rahmen der Vorabkontrolle hat er in Zweifelsfällen den Landesbeauftragten für den Datenschutz zu konsultieren.

Satz 5 enthält ergänzend zur bereits genannten Datenschutzkontrolle eine beispielhafte Aufzählung weiterer wichtiger Aufgaben des behördlichen Datenschutzbeauftragten.

Bei der Einführung neuer Datenverarbeitungsmaßnahmen hat der behördliche Datenschutzbeauftragte gemäß **Satz 5 Nummer 1** zu prüfen, ob diese im Einklang mit den datenschutzrechtlichen Bestimmungen stehen, und gegebenenfalls Empfehlungen für eine datenschutzgerechte Ausgestaltung zu geben. Erfasst ist jeder Vorgang, der eine Datenverarbeitung im Sinne von § 3 Abs. 4 Satz 1 DSGVO darstellt, unabhängig davon, ob es sich um eine automatisierte oder eine nicht automatisierte Verarbeitung handelt. Damit diese Aufgabe sachgerecht wahrgenommen werden kann, hat die Daten verarbeitende Stelle sicherzustellen, dass der behördliche Datenschutzbeauftragte frühzeitig und umfassend hierüber unterrichtet wird. Es empfiehlt sich bei der Einführung neuer Maßnahmen, den Datenschutzbeauftragten von Anfang an zu beteiligen, um so zu datenschutzgerechten Lösungen zu kommen.

Damit in der täglichen Verwaltungsarbeit die datenschutzrechtlichen Bestimmungen hinreichend Beachtung finden, kommt der Sensibilisierung der Mitarbeiter für diese zuweilen schwierige Rechtsmaterie besondere Bedeutung zu. Der behördliche Datenschutzbeauftragte hat nach **Satz 5 Nummer 2** die Aufgabe, die Beschäftigten mit den einschlägigen Vorschriften vertraut zu machen, wozu auch die im Zusammenhang mit dem Datengeheimnis nach § 6 Satz 2 DSGVO vorgesehene Unterrichtspflicht zählt. Darüber hinaus sollen grundsätzliche datenschutzrechtliche Regelungen in einer Dienstanweisung aufgenommen werden, die von allen Mitarbeitern der Daten verarbeitenden Stelle zu berücksichtigen sind. Notwendige Detailregelungen bleiben den jeweiligen Fachbereichen vorbehalten. Dem Datenschutzbeauftragten kommt die Funktion eines Multiplikators zu. Er kann unter anderem Schulungen anbieten oder Vorträge halten, Informationsblätter erstellen

sowie bei Dienstberatungen über ausgewählte Themen informieren. Er muss die Beschäftigten allerdings nicht selbst unterrichten oder schulen, sondern kann sich dafür auch anderer Einrichtungen bedienen. Für einzelne Fachgebiete werden beispielsweise spezielle Seminare angeboten. Der behördliche Datenschutzbeauftragte soll hierüber informieren und die Teilnahme an Fortbildungsmaßnahmen anregen.

Durch **technische und organisatorische Maßnahmen** ist eine nach dem Stand der Technik und der Sensibilität der zu verarbeitenden Daten hinreichende Datensicherheit zu gewährleisten. Für **automatisierte Verfahren** ist ein Sicherheitskonzept obligatorisch. Deshalb sollte bei der Auswahl von am Markt angebotenen Verfahren schon zu einem frühen Zeitpunkt auf die Einhaltung von Datenschutz und Datensicherheit geachtet werden. Eine rechtzeitige Berücksichtigung der datenschutzrechtlichen und datensicherheitstechnischen Aspekte ist immer auch eine Kostenfrage, denn das Nachrüsten von datenschutzgerechter Technik ist in jedem Falle um ein Vielfaches teurer. Aus diesem Grund sollten diese Punkte stets Bestandteil von Ausschreibungen sein. Der behördliche Datenschutzbeauftragte hat hier gemäß Satz 5 **Nummer 3** eine Unterstützungsfunktion. Er berät in diesem Zusammenhang, prüft, ob es sich um ein den datenschutzrechtlichen Vorschriften entsprechendes Verfahren handelt, und gibt Anregungen zur Verbesserung des Verfahrens. Diese Aufgabe kann er jedoch nur erfüllen, wenn er rechtzeitig und vollständig über die geplante Einführung neuer oder die Änderung bestehender Verfahren informiert wird. Darüber hinaus hat der behördliche Datenschutzbeauftragte die Daten verarbeitende Stelle beim Erstellen von Verfahrensbeschreibungen zu unterstützen.

Zu den Aufgaben des Datenschutzbeauftragten gehört es nach Satz 5 **Nummer 4** auch, für die bei der jeweiligen Stelle eingesetzten Verfahren das Verzeichnis gemäß § 18 Abs. 1 DSGVO M-V zu führen. Die Daten verarbeitende Stelle hat das Verzeichnis zu erstellen und dem behördlichen Datenschutzbeauftragten zu übermitteln. Die Führung der Verfahrensbeschreibungen schließt neben deren Sammlung auch ihre Kontrolle auf Plausibilität, Vollständigkeit und Aktualität ein. Die beim behördlichen Datenschutzbeauftragten vorhandenen Verfahrensbeschreibungen sind sowohl für ihn als auch für den Landesbeauftragten für den Datenschutz Prüfungsgrundlage und sind Letzterem nach § 18 Abs. 3 Satz 2 DSGVO M-V auf Anforderung zu übersenden. Neben der Aufbewahrung dieser Beschreibungen hat der behördliche Datenschutzbeauftragte sie auch für die Einsichtnahme nach Absatz 4 zur Verfügung zu stellen.

Die Vorabkontrolle nach § 19 Abs. 2 DSGVO M-V obliegt ebenfalls gemäß Satz 5 **Nummer 5** dem behördlichen Datenschutzbeauftragten. Vor der Einrichtung oder wesentlichen Änderung eines der dort genannten Verfahren ist ihm im Rahmen einer angemessenen Frist Gelegenheit zur datenschutzrechtlichen Prüfung zu geben. Diese umfasst sowohl die Rechtmäßigkeit der Datenverarbeitung als auch die technischen und organisatorischen Maßnahmen zur Gewährleistung einer erforderlichen und angemessenen Datensicherheit.

Über diese nicht abschließenden Tätigkeitsschwerpunkte hinaus ist im Einzelfall zu prüfen, wo Änderungen im Verwaltungsablauf, zum Beispiel durch Umstrukturierungen bei bestehenden Aufgaben oder die Übernahme neuer Aufgaben, oder sonstige Maßnahmen von datenschutzrechtlicher Relevanz sind und damit der Datenschutzbeauftragte zu beteiligen ist.

Unter anderem ist der behördliche Datenschutzbeauftragte auf jeden Fall einzubinden, wenn eine **Auftragsdatenverarbeitung** gemäß § 21 LKHG M-V vorgesehen ist. Der behördliche Datenschutzbeauftragte hat auch hier eine Unterstützungs- und Beratungsfunkti-

on bei der Ausgestaltung des Auftragsverhältnisses, und die Auftragsdatenverarbeitung unterliegt ebenfalls seiner Kontrolle.

Bei der Verarbeitung personenbezogener Daten zum Zwecke der wissenschaftlichen **Forschung** nach § 20 LKHG M-V sollte ebenfalls die Zustimmung des behördlichen Datenschutzbeauftragten eingeholt werden, auch wenn dies § 2 LKHG M-V nicht ausdrücklich vorsieht. Der Datenschutzbeauftragte kann dann prüfen, ob die schutzwürdigen Belange der Betroffenen dieser Datenverarbeitung nicht entgegenstehen, ob die Voraussetzungen von § 20 LKHG M-V erfüllt werden und gegebenenfalls Verbesserungsvorschläge unterbreiten.

Bei der Umsetzung von Hinweisen des Landesbeauftragten für den Datenschutz, insbesondere bei Beanstandungen, sollte der behördliche Datenschutzbeauftragte regelmäßig beratend hinzugezogen werden.

Darüber hinaus empfiehlt es sich, den behördlichen Datenschutzbeauftragten zu beteiligen, wenn **Auskunftsersuchen** Betroffener nicht oder nur teilweise entsprochen werden soll.

Das vom behördlichen Datenschutzbeauftragten geführte **Verfahrensverzeichnis** kann gemäß **Absatz 4** von jedermann ohne Vorliegen besonderer Voraussetzungen eingesehen werden. Hiervon ausgenommen sind Informationen über die zur Datensicherheit getroffenen Maßnahmen. Im Einzelfall werden zu Verfahren keine Auskünfte erteilt, bei denen diese zu einer Gefährdung der öffentlichen Sicherheit oder Ordnung führen oder sonst dem Wohle eines Landes oder des Bundes Nachteile bereiten würden oder bestimmte Sachverhalte aufgrund von Rechtsvorschriften oder ihrem Wesen nach geheim gehalten werden müssen. Da zu den Verfahren in diesem Zusammenhang nur allgemeine Auskünfte erteilt werden, ohne dass damit eine Aussage verbunden ist, ob und in welchem Umfang Daten zur Person des Betroffenen gespeichert sind, kommt es nicht darauf an, wer um Einsicht ersucht. Daher hat die Daten verarbeitende Stelle bereits bei der Weitergabe der Verfahrensbeschreibung den behördlichen Datenschutzbeauftragten darüber zu informieren, ob ein solcher Fall vorliegt.

Einzelprobleme beim Datenschutz im Krankenhaus

Prüfungen des Medizinischen Dienstes der Krankenversicherung (MDK)

Schon wegen der teilweise unterschiedlichen Interessenlage der Beteiligten (Krankenkasse, Krankenhaus, MDK), aber auch wegen der komplizierten und nicht gerade übersichtlichen gesetzlichen Vorschriften, bergen Prüfungen des MDK in Krankenhäusern einigen Zündstoff. Ebenso zeigen viele Anfragen, dass häufig Unsicherheiten über die Kompetenzen und Befugnisse des MDK bei seinen Prüfungen bestehen.

Gesetzliche Grundlagen

Aufgaben und Befugnisse des MDK sind insbesondere in den §§ 275 bis 277 SGB V geregelt. Es folgen mit den §§ 278 bis 283 SGB V Vorschriften über die Organisation, die Finanzierung, die Spitzenverbände und die bundesweite Koordinierung des Medizinischen

Dienstes. Schließlich hat der MDK auch die Aufgabe, Fehlbelegungsprüfungen nach § 17a KHG vorzunehmen.

Zuständigkeit des MDK

Häufig besteht bei den Krankenhäusern, aber auch den Krankenkassen selbst, Unsicherheit, welcher Medizinische Dienst für die **Begutachtung** der Behandlung eines Versicherten zuständig ist, wenn dieser beispielsweise in einem anderen Bundesland behandelt worden ist. So gibt es immer wieder Fälle, in denen Krankenhäuser die vom MDK angeforderten Krankenunterlagen nicht herausgeben, weil der anfragende MDK zu einem anderen Bundesland gehört, als das den Versicherten behandelnde Krankenhaus.

Eine gesetzliche Regelung über die Zuständigkeiten der einzelnen Medizinischen Dienste der Bundesländer existiert nicht. § 278 Abs. 1 SGB V regelt lediglich, dass die Krankenkassen der in Absatz 2 genannten Kassenarten in jedem Land eine Arbeitsgemeinschaft „Medizinischer Dienst der Krankenversicherung“ zu errichten haben. Im Hinblick auf die Unterscheidung zwischen landes- und bundesunmittelbaren Krankenkassen könnten sich aber folgende Zuständigkeiten des MDK ergeben:

Der für die landesunmittelbaren Krankenkassen (z. B. AOK M-V) und deren Versicherte tätig werdende MDK ist für alle Mitglieder der beauftragenden Krankenkasse zuständig, unabhängig vom Wohnort des Versicherten. Entscheidend ist die Zugehörigkeit des Versicherten zu der Krankenkasse, von der beziehungsweise für die der MDK gemäß § 278 SGB V eingerichtet worden ist.

Hinsichtlich der bundesunmittelbaren Krankenkassen (z. B. DAK), deren Tätigkeiten sich nicht regional auf ein Bundesland beschränken lassen, sollte die Zuständigkeit des MDK nach dem Wohnsitz des Versicherten bestimmt werden. Beispiel: Für einen in Rostock wohnenden und bei der DAK Hamburg Versicherten wäre der MDK Mecklenburg-Vorpommern zuständig.

Begutachtung nach § 275 SGB V

Die datenschutzrechtlich relevante Vorschrift, in der die Befugnisse des MDK zu Datenerhebung, -verarbeitung sowie Akteneinsicht usw. geregelt sind, ist § 276 SGB V. Da diese Norm nicht isoliert von den in § 275 SGB V genannten Aufgaben des MDK gesehen werden kann, sollen diese zum besseren Verständnis erläutert werden.

In Absatz 1 ist zunächst festgehalten, dass der MDK nur im Auftrag einer Krankenkasse tätig werden kann. Schon damit ist klar, dass der MDK **nicht** auf eigene Initiative an die Krankenhäuser herantreten kann. Die drei wesentlichen Bereiche, in denen die Krankenkassen verpflichtet sind, den MDK mit einer gutachtlichen Stellungnahme zu beauftragen, sind nach § 275 Abs. 1 SGB V

- Erbringung von Leistungen (§ 275 Abs. 1 Nr. 1 SGB V),
- Einleitung von Maßnahmen zur Rehabilitation (§ 275 Abs. 1 Nr. 2 SGB V),
- Arbeitsunfähigkeit (§ 275 Abs. 1 Nr. 3 SGB V).

Im Folgenden soll der Schwerpunkt auf die Vorschrift des **§ 275 Abs. 1 Nr. 1 SGB V**, also auf die Begutachtung bei der Erbringung von Leistungen, gelegt werden, da dies in der Praxis sehr häufig vorkommt und zudem ein großes Konfliktpotential enthält.

Bevor die **Krankenkasse** ein solches Gutachten einholt, muss sie zunächst darüber befinden, ob dies nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist. Diese einschränkenden Voraussetzungen konkretisieren letztlich den Verhältnismäßigkeitsgrundsatz. Die Verhältnismäßigkeit muss die Krankenkasse jeweils im Einzelfall prüfen. Daraus folgt, dass Pauschalprüfungen oder Stichproben unabhängig von konkreten Einzelfällen nicht zulässig sind.

Welche Befugnisse zum Umgang mit Patientendaten folgen nun daraus? Die Antwort ergibt sich aus § 276 Abs. 2 Satz 1 2. Halbsatz SGB V. Hat die Krankenkasse den MDK mit der Einholung eines Gutachtens nach § 275 Abs. 1 SGB V beauftragt, sind die **Leistungserbringer** verpflichtet, Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln, soweit dies für das Gutachten **erforderlich** ist.

Das Krankenhaus ist, wie sich aus § 69 SGB V ergibt, ein **Leistungserbringer** im Sinne des SGB V. Welche Daten erforderlich sind, hängt letztlich vom Einzelfall ab, das heißt vom konkreten Gutachtenauftrag und dessen Umfang. Entscheidend für die Krankenhäuser ist in diesem Zusammenhang, wer beurteilt, welche Daten konkret erforderlich sind. § 276 SGB V enthält insofern keine Vorgaben. Daher muss auf allgemein geltende Übermittlungsgrundsätze zurückgegriffen werden. Zwar spricht § 276 Abs. 2 SGB V ausschließlich von „Sozialdaten“. Das führt aber nicht dazu, dass auf die allgemeinen Regeln des Sozialdatenschutzes (§§ 67 ff. SGB X) zurückgegriffen werden kann. Die Regeln finden auf Krankenhäuser keine Anwendung, da diese keine **Leistungsträger** im Sinne der §§ 35, 12 SGB I, sondern vielmehr **Leistungserbringer** sind. Nur erstere werden durch das SGB X verpflichtet. Leistungsträger im Bereich der gesetzlichen Krankenversicherung sind gemäß § 21 Abs. 2 SGB I ausschließlich die gesetzlichen Krankenkassen und mit ihnen auch der MDK. Deshalb sind die nach § 276 Abs. 2 SGB V zu übermittelnden Daten nur aus Sicht des MDK Sozialdaten, nicht aus Sicht des Krankenhauses.

Da die §§ 16 ff. LKHG M-V nicht festlegen, wer für die Zulässigkeit der Übermittlung verantwortlich ist, gelten die Auffangregelungen des DSGVO M-V beziehungsweise des BDSG (siehe Seite 12). Nach § 14 Abs. 2 Satz 1 DSGVO M-V liegt die Verantwortung für die Zulässigkeit der Datenübermittlung bei der übermittelnden Stelle, das heißt hier beim Krankenhaus. Erfolgt – wie im Falle der Anforderung durch den MDK – die Übermittlung auf Ersuchen des Empfängers, trägt nach § 14 Abs. 2 Satz 2 DSGVO M-V dieser die Verantwortung. Die übermittelnde Stelle prüft nach Satz 3 der Vorschrift nur, ob das **Übermittlungsersuchen** im Rahmen der Aufgaben des Empfängers liegt. Bei der Übermittlung von Patientendaten an den MDK ist dieser Grundsatz jedoch zu modifizieren: Diese unterliegen der ärztlichen Schweigepflicht. Die Verantwortung für die Durchbrechung der Schweigepflicht kann aber nicht einfach dem MDK übertragen werden. Der Träger der Schweigepflicht (Arzt oder Gehilfe) kann seine strafrechtliche Verantwortlichkeit nach § 203 StGB nicht delegieren. Aus diesem Grunde ist das Krankenhaus gehalten, die Zulässigkeit der Übermittlung genauer zu prüfen, als es § 14 Abs. 2 Satz 3 DSGVO M-V nahe legt.

Übertragen auf die Datenübermittlung vom Krankenhaus an den MDK bedeutet dies: Da der Prüfauftrag der Krankenkasse für jeden Einzelfall sowohl inhaltlich als auch vom Umfang her unterschiedlich gefasst sein kann, muss der MDK gegenüber der von ihm angefragten Stelle konkret darlegen, was Inhalt seines Prüfauftrages ist. Das Krankenhaus muss erkennen können, welche Daten welches Patienten in welchem Umfang und für welchen Zweck benötigt werden. Insbesondere bei einer aus mehreren Teilleistungen bestehenden Krankenhausbehandlung ist es für den offenbarenden Arzt oder das Krankenhaus notwendig zu wissen, in welchem Umfang – von welcher Teilleistung – die Daten nach § 276

Abs. 2 Satz 1 SGB V offenbart werden müssen. Kennt der Arzt den Prüfauftrag nicht, könnte er möglicherweise Daten offenbaren, die für das Gutachten des MDK nicht erforderlich sind, und sich so der Gefahr der strafrechtlich bewehrten Verletzung der ärztlichen Schweigepflicht aussetzen.

Das Übermittlungsersuchen des MDK muss daher hinreichend konkret sein und den Anlass nennen, aus dem das Gutachten eingeholt wird. Da der MDK darlegen muss, dass er die Daten zur Erfüllung seiner bestimmten Aufgabe benötigt, kann das Krankenhaus lediglich prüfen, ob das Übermittlungsersuchen nachvollziehbar und plausibel ist. Das Krankenhaus selbst muss dann prüfen, ob die vom MDK geforderten Daten für die Erstellung des Gutachtens erforderlich sind und somit ihre Übermittlung zulässig ist. Welche Daten dies im Einzelfall sein können, ist eine fachliche Frage, die ein Arzt entscheiden muss. Dies alles setzt zwingend voraus, dass der MDK Datenübermittlungen nur in begründeten Einzelfällen verlangen kann. Anderenfalls kann das Krankenhaus nicht entscheiden, ob die Durchbrechung der Schweigepflicht gerechtfertigt ist. Pauschale oder stichprobenartige Übermittlungsersuchen sind bei der Erfüllung der Aufgaben nach den §§ 275 ff. SGB V folglich unzulässig und müssen vom Krankenhaus abschlägig beschieden werden.

Kommt das Krankenhaus nach Prüfung der Plausibilität des Ersuchens zu der Auffassung, dass die Daten im Rahmen der Aufgaben des MDK für das Gutachten erforderlich sind, hat es keine Wahl: Nach § 276 Abs. 2 Satz 1 SGB V **muss** das Krankenhaus die Daten übermitteln. Ein Ermessen besteht insoweit nicht. Deshalb wäre die pauschale Weigerung eines Krankenhauses, Daten an den MDK zu übermitteln, ebenso wenig zulässig. Diese Einschränkung des **Rechts auf informationelle Selbstbestimmung** der Patienten hat der Gesetzgeber in verfassungsrechtlich nicht zu beanstandender Weise durch das SGB V zugelassen.

Die mit der Berechtigung des MDK korrespondierende Verpflichtung der Leistungserbringer zur Übermittlung der Patientendaten besteht nur, wenn die angeforderten Informationen für die gutachterliche Stellungnahme und Prüfung **erforderlich** sind und damit die konkrete Aufgabe des MDK ohne diese Daten nicht ordnungsgemäß erledigt werden kann.

§ 276 Abs. 2 Satz 1 SGB V spricht von „erforderlichen Sozialdaten“ (gemeint sind Patienten- bzw. Versichertendaten). Eine Differenzierung zwischen selbst erhobenen Daten des Krankenhauses und so genannten **Fremdbefunden** dritter Behandler (einschließlich Krankenhausentlassungsberichten) nimmt der Gesetzgeber nicht vor. Danach kommt es für eine zulässige Übermittlung nur darauf an, ob die beim Behandler vorliegenden Unterlagen für die konkrete Aufgabenerfüllung des MDK erforderlich sind. Zumindest soweit Fremdbefunde in die Entscheidungen der Leistungserbringer eingeflossen sind und damit untrennbarer Bestandteil der Behandlung und der dazugehörigen Aufzeichnungen des jeweiligen Leistungserbringers geworden sind, bestehen gegen eine Übermittlung auch dieser Fremdbefunde an den MDK von vornherein keine datenschutzrechtlichen Bedenken.

Die Zulässigkeit der Übermittlung der übrigen, in die Behandlung des Patienten (noch) nicht einbezogenen Fremdbefunde, ist für jeden einzelnen Fall nach dem Erforderlichkeitsprinzip gesondert zu prüfen. Dass die Übermittlung solcher Fremdbefunde an den MDK von vornherein unzulässig – rechtswidrig – ist, lässt sich dem Wortlaut und dem Sinn und Zweck des Gesetzes nicht entnehmen: Die Verpflichtung zur Wahrung der ärztlichen Schweigepflicht trifft allein den Arzt beziehungsweise den behandelnden Arzt des Krankenhauses. Insoweit hat der übersendende Arzt (des Krankenhauses) im Hinblick auf die ihm vorliegenden eigenen und/oder fremden Unterlagen zu beurteilen, welche Aus-

künfte und Unterlagen, also auch Fremdbefunde, für die gutachterliche Stellungnahme und Prüfung des MDK erforderlich sind und so entsprechend den Umfang seiner Auskunft nach § 276 Abs. 2 SGB V zu bestimmen. Überblickt der Arzt die Aktualität der nicht von ihm stammenden Unterlagen oder die Vollständigkeit anderweitig durchgeführter Untersuchungen nicht, ist er nicht in der Lage, die Erforderlichkeit dieser Unterlagen für die Aufgabenerfüllung des MDK zu beurteilen. In diesem Fall hat der Arzt dann zu entscheiden, ob er – sozusagen als Minus zur Übersendung von Fremdbefunden – entsprechend § 276 Abs. 2 SGB V verpflichtet ist, dem MDK stattdessen den Arzt oder das Krankenhaus zu benennen, von dem die Befunde erstellt worden sind. Der MDK wäre dann gehalten, sich an den eigentlichen Urheber der Berichte zu wenden.

Gemäß § 18 Abs. 1 LKHG M-V ist dem Patienten auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen und Einsicht in die Krankenunterlagen zu gewähren. Dieses Recht erstreckt sich auch auf Angaben über Personen und Stellen, denen Patientendaten übermittelt worden sind. Daher ergibt sich aus § 22 Abs. 4 DSGVO M-V (§ 78 a SGB X gilt nur für Leistungsträger!) beziehungsweise für bereits archivierte Patientenunterlagen aus § 19 Abs. 2 Satz 6 LKHG M-V die Verpflichtung, jede Übermittlung an den MDK in der Krankenakte zu dokumentieren.

Eine **Datenübermittlung** direkt an die Krankenkassen – etwa die Übersendung von Teilen der Krankenakte zur Prüfung, ob die Kasse überhaupt den MDK einschaltet – ist nach den §§ 275 ff. SGB V selbstverständlich nicht zulässig. Das Bundessozialgericht hat in seinem Urteil vom 23. Juli 2002 (B 3 KR 64/01 R) extra darauf hingewiesen, dass die gesetzlichen Krankenkassen kein Recht haben, Krankenakten der Krankenhäuser einzusehen. Dieses Recht steht „exklusiv“ dem MDK zu, der auch selbst entscheiden muss, welche Unterlagen für seine Begutachtung erforderlich sind.

Begutachtung nach § 276 Abs. 4 SGB V

§ 276 Abs. 4 SGB V regelt mit der Prüfung von Dauer und Notwendigkeit einer stationären Behandlung einen speziellen Fall der gutachtlichen Stellungnahme durch den MDK, der von den oben genannten „normalen“ Fällen des § 275 Abs. 1 SGB V zu trennen ist. Da die Prüfung nach § 276 Abs. 4 SGB V üblicherweise einen umfassenderen Charakter haben wird als diejenige nach § 275 Abs. 1 SGB V, hat der Gesetzgeber den Ärzten des MDK das Recht eingeräumt, in der Zeit zwischen 8.00 und 18.00 Uhr Einsicht in Patientenunterlagen zu nehmen oder den Patienten zu untersuchen. Auch hier sind einige Dinge zu beachten:

Zunächst gilt, dass die Einsichtnahme in die Patientenakte nur zulässig ist, wenn es **im Einzelfall** für die gutachtliche Stellungnahme erforderlich ist. Dies schreibt schon der Gesetzeswortlaut vor. Der MDK kann in diesem Falle nur tätig werden, wenn ihn die Krankenkasse nach Zweifeln an der Notwendigkeit oder der Dauer eines **Krankenhausaufenthaltes** bei einem bestimmten Versicherten um eine gutachtliche Stellungnahme ersucht. Der MDK-Arzt muss dem Krankenhaus darlegen, dass ein solcher Gutachtenauftrag bei einem bestimmten Versicherten vorliegt. Das Krankenhauspersonal muss prüfen, ob die Voraussetzungen des § 276 Abs. 4 SGB V erfüllt sind. Verantwortlich für die Zulässigkeit der Akteneinsicht ist wegen der Schweigepflicht auch hier das Krankenhaus. Es gelten dieselben rechtlichen Vorgaben, wie bereits im Abschnitt 2 dargestellt, da auch die Akteneinsicht eine Form der Datenübermittlung ist. Vor diesem Hintergrund ist es nicht zulässig, im Krankenhausarchiv einen Arbeitsplatz mit freier Verfügung über die Patientenakten für den Arzt des MDK einzurichten.

Die Übermittlung der Patientenakte oder von Teilen davon im Sinne einer Übersendung an den MDK ist in § 276 Abs. 4 SGB V nicht vorgesehen. Als Ort dieser umfassenden Prüfung der Unterlagen ist vielmehr ausschließlich das Krankenhaus vorgesehen.

Auf der anderen Seite kann das Krankenhaus den Prüfauftrag des MDK nicht einschränken: So lässt sich – entgegen der von Krankenhausesseite gelegentlich vertretenen Auffassung – aus § 276 Abs. 4 SGB V nicht herleiten, dass der MDK-Arzt nur dann Patientenunterlagen einsehen darf, solange der Patient noch in Behandlung ist. Diese Auslegung ist vom Wortlaut der Vorschrift her nicht zwingend, auch wenn dort die Befugnisse zur Einsichtnahme und zur Untersuchung des Patienten mit „und“ verknüpft sind. Sinn und Zweck der Vorschrift (nämlich die Überprüfung von Notwendigkeit und Dauer einer stationären Behandlung) legen sogar nahe, dass auch nach Abschluss der Behandlung noch in die Patientenunterlagen eingesehen werden darf. Oft ergeben sich für die Krankenkasse erst bei Erhalt der Krankenhausrechnung Zweifel an der Notwendigkeit oder insbesondere der Dauer des Krankenhausaufenthaltes. Dies kann auch sogar dann noch der Fall sein, wenn die Rechnung bereits beglichen wurde. Wie lang die Frist zu bemessen ist, in der eine Einsichtnahme durch den MDK nach Abschluss der Behandlung noch möglich sein soll, hängt letztlich davon ab, wie viel Zeit Krankenkassen und MDK für die endgültige Bearbeitung der Behandlungsfälle üblicherweise benötigen. Sie darf sich aber nicht nach den Verjährungsvorschriften richten.

Begutachtung nach § 17a KHG

Ein bis heute strittiges Thema zwischen Krankenhäusern und Krankenkassen sind die Befugnisse des MDK bei **Fehlbelegungsprüfungen** nach § 17a Abs. 2 KHG. Nach dieser Vorschrift „wirken die Krankenkassen ... durch gezielte Einschaltung des MDK darauf hin, dass Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden.“ Zu diesem Zweck hat der MDK wiederum ein Einsichtsrecht in Krankenunterlagen und damit Zugang zu Patientendaten.

Während § 276 Abs. 4 SGB V zum Ziel hat, unter anderem die Dauer von Krankenhausaufenthalten einzelner Patienten zu prüfen, ist der Prüfungsumfang bei § 17a KHG weiter, da es hier darum geht, Fehlbelegungen in einem größeren Umfang abzubauen beziehungsweise von vornherein zu vermeiden.

Folgende Voraussetzungen müssen erfüllt sein:

§ 17a Abs. 2 KHG spricht von **gezielter** Einschaltung des MDK. Dieses Erfordernis ist wiederum Ausdruck des Verhältnismäßigkeitsgrundsatzes. „Gezielt“ ist eine Einschaltung des MDK nur dann, wenn ein konkreter Anlass besteht, eine Fehlbelegung zu vermuten. Ein derart konkreter Anlass setzt voraus, dass **bezogen auf bestimmte Behandlungsfälle, einzelne Fachabteilungen, Stationen oder ganze Krankenhäuser** der Verdacht auf Fehlbelegungen besteht. Dabei kann es sich um eine Vielzahl von Patienten einer Station/Abteilung oder des gesamten Krankenhauses handeln. Es ist nicht erforderlich, dass nur Versicherte der prüfenden Krankenkasse betroffen sind. Die Zahl der Patienten muss aber bestimmbar bleiben.

An das Bestehen eines Verdachtes sind keine allzu hohen Anforderungen zu stellen. So kann es beispielsweise ausreichend sein, wenn in einer Abteilung gehäuft montags Patienten entlassen werden. In einem solchen Falle kann der MDK auch eine Vielzahl von Patientenunterlagen dieser Abteilung einsehen. Erforderlich ist es jedoch, dass der Kranken-

kasse mindestens solcherart Verdachtsmomente vorliegen. Die Anknüpfung an bestimmte Auffälligkeiten im Rahmen der Krankenbehandlung muss in jedem Falle erkennbar und plausibel sein. Die Krankenkasse beziehungsweise der MDK sind darüber hinaus verpflichtet, dem Krankenhaus in nachvollziehbarer Weise die konkreten Verdachtsmomente zu benennen. Können sie das nicht, hat das Krankenhaus eine Einsichtnahme in Patientenakten abzulehnen.

Es gilt also wieder der in § 17a Abs. 2 KHG konkretisierte datenschutzrechtliche Grundsatz, dass jeweils aufgrund konkreter Anhaltspunkte zu prüfen ist, ob die Daten zur Fehlbelegungsprüfung **erforderlich** sind. Daraus folgt, dass allgemeine flächendeckende Prüfungen, die einer Ausforschung der Krankenhäuser gleichkommen, von § 17a KHG nicht erfasst und damit in jedem Falle unzulässig sind. Beispielsweise kann eine Krankenkasse durch den MDK nicht alle bei ihr Versicherten, die in einem bestimmten Krankenhaus behandelt worden sind, überprüfen lassen, ohne dass der konkrete Verdacht einer Fehlbelegung besteht. Ebenso unzulässig wäre eine flächendeckende Prüfung, die gar nicht dem primären Zweck des Abbaus von Fehlbelegungen dient, sondern beispielsweise Grundlage für kommende Budgetverhandlungen sein soll. Dies würde dem datenschutzrechtlichen Grundsatz der Zweckbindung widersprechen.

Übermittlung der gutachterlichen Stellungnahme

Der MDK ist nach erfolgter Begutachtung gegenüber der das Gutachten veranlassenden Krankenkasse gemäß § 277 Abs. 1 Satz 1 SGB V verpflichtet, ihr unter anderem das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitzuteilen. Eine Übermittlung an andere als in § 277 Abs. 1 SGB V genannte Stellen ist nicht zulässig.

Datenübermittlungen innerhalb des Krankenhauses

Durch die vermehrte Nutzung des Fachwissens anderer Abteilungen des Krankenhauses und die zunehmende Einbeziehung von Spezialisten in die Behandlung besteht für den Patienten die Gefahr, dass er nicht mehr überblicken kann, wer was wann über ihn gespeichert hat. Daher sind einige grundlegende Dinge zu beachten:

Werden zwischen **Fachabteilungen** Patientendaten übermittelt, so bestimmt § 16 Abs. 3 LKHG M-V, dass dafür § 17 Abs. 1 LKHG M-V entsprechend gilt. Das bedeutet, dass diese Datenübermittlungen genauso zu behandeln sind, wie solche an Stellen außerhalb des Krankenhauses. Einer der häufigsten Fälle dürfte die Datenübermittlung zur Durchführung einer Mit- oder Nachbehandlung sein. Sie ist nach § 17 Abs. 1 Nr. 2 LKHG M-V zulässig. In der Regel werden die Patientenunterlagen von der mit- oder nachbehandelnden Abteilung angefordert. Der behandelnde Arzt dieser Abteilung muss letztlich auch entscheiden, welche Daten er benötigt. Allerdings sind derartige Zugriffe in den Unterlagen entsprechend zu **protokollieren**, um die Datennutzung nachvollziehbar zu machen. Dies ergibt sich zudem aus den berufsrechtlichen Dokumentationspflichten. Dabei spielt es grundsätzlich keine Rolle, ob es sich um konventionelle Patientenakten handelt oder um elektronische. Unterschiedlich ist nur die Art der Protokollierung.

Zu beachten ist vor allem, dass der Patient über eine solche Datenübermittlung zu informieren ist und ihr nach § 17 Abs. 1 Nr. 2 LKHG M-V auch **widersprechen** kann. Eine ausdrückliche Einwilligung ist hingegen nicht erforderlich. Es reicht vielmehr aus, dass der

Patient von der ursprünglich behandelnden Abteilung darauf hingewiesen wird, dass es erforderlich oder zu empfehlen ist, eine andere Abteilung hinzuzuziehen. Ist der Patient mit der eigentlichen Mit- oder Nachbehandlung einverstanden, so ist davon auszugehen, dass er damit auch in die dafür erforderliche Datenübermittlung einwilligt.

In **Notfällen**, wenn der Patient zum Beispiel aufgrund von Bewusstlosigkeit oder Ähnlichem nicht von einer notwendigen Mit- oder Nachbehandlung informiert werden kann, ist zu diesem Zweck auch die Datenübermittlung zulässig. Dies gilt allerdings dann nicht, wenn ein ausdrücklicher (z. B. Patientenverfügung) oder mutmaßlicher entgegenstehender Wille des Patienten bekannt ist. Bestimmte Notfalldaten sollten ohnehin für den ärztlichen Zugriff jederzeit zur Verfügung stehen.

Psychischkrankengesetz – PsychKG M-V

Das Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (PsychKG M-V) ist zeitlich vor dem LKHG M-V in Kraft getreten. Abschnitt IX enthält Regelungen zum Datenschutz und zur Akteneinsicht. Zu beachten ist, dass auch einige andere Paragraphen Bestimmungen mit datenschutzrechtlichem Bezug enthalten, beispielsweise § 41 Verwertung von Erkenntnissen.

§ 43 Personenbezogene Daten

§ 43 Abs. 1 PsychKG M-V

Für die Verarbeitung personenbezogener Daten der Betroffenen oder Dritter gelten die Vorschriften des Landesdatenschutzgesetzes und Landeskrankenhausgesetzes, soweit nicht in den folgenden Absätzen abweichende oder ergänzende Regelungen getroffen werden.

Durch den Verweis auf das DSG M-V und das LKHG M-V wird klargestellt, dass das PsychKG M-V den Umgang mit personenbezogenen Daten nicht abschließend regelt. Lässt sich eine datenschutzrechtliche Frage nach den Bestimmungen des PsychKG M-V nicht beantworten, so ist aus systematischen Gründen zunächst zu prüfen, ob sie anhand des LKHG M-V beantwortet werden kann. Führen auch diese Normen zu keinem Ergebnis, sind die Bestimmungen des DSG M-V anzuwenden, oder gegebenenfalls das BDSG, wenn das DSG M-V auf den Träger des Krankenhauses nicht anwendbar ist (siehe hierzu Seite 12).

§ 43 Abs. 2 PsychKG M-V

Personenbezogene Daten der Betroffenen und Dritter, insbesondere Angehöriger und gesetzlicher Vertreter, dürfen durch die einweisende Behörde, das Sozialministerium, den Sozialpsychiatrischen Dienst, das Gesundheitsamt und die Einrichtung verarbeitet werden, soweit es für die Gewährung von Hilfen, für die ordnungsgemäße Unterbringung und Behandlung einschließlich der staatlichen Aufsicht und der Abwehr von Gefahren für die Sicherheit und das geordnete Zusammenleben in der Einrichtung und für die Wiedereingliederung der Betroffenen nach der Entlassung erforderlich ist. Bei Unterbringung nach § 1 Abs. 1 Nr. 3 Buchstabe b gilt dies auch für das Justizministerium.

Abweichend vom LKHG M-V wird im PsychKG M-V der sonst im Datenschutzrecht übliche Begriff „personenbezogene Daten“ verwendet. Inhaltlich bestehen zwischen den Begriffen „personenbezogene Daten“ und „Patientendaten“ keine wesentlichen Unterschiede. Als **Patientendaten** sind nach der Definition im LKHG M-V auch die Daten von **Angehörigen** oder anderen Bezugspersonen des Patienten sowie sonstigen Dritten zu zählen, die dem Krankenhaus durch die Behandlung bekannt werden. Im PsychKG ist dagegen von Dritten, insbesondere Angehörigen und gesetzlichen Vertretern, die Rede.

Die Daten erhebenden Stellen sind im Absatz 2 abschließend genannt, ebenso die Aufgaben, zu deren Erfüllung personenbezogene Daten erforderlich sein können. Sofern eine Aufgabe ohne personenbezogene Daten erfüllbar ist, dürfen solche weder erhoben noch gespeichert werden.

§ 43 Abs. 3 PsychKG M-V

Im Rahmen der Unterbringung nach § 1 Abs. 1 Nr. 3b sind Ärzte, Psychologen, Gerichte und Behörden befugt, der Einrichtung Strafurteile, staatsanwaltliche Ermittlungssachverhalte, psychiatrische und psychologische Gutachten aus gerichtlichen oder staatsanwaltlichen Verfahren, den Lebenslauf und Angaben über die bisherige Entwicklung sowie Angaben über Krankheiten, Körperschäden und Verhaltensauffälligkeiten des Betroffenen zu übermitteln, es sei denn, dass Rechtsvorschriften außerhalb der allgemeinen Regelungen über die Berufs- und Amtsverschwiegenheit dies untersagen.

Diese Regelung beinhaltet eine eingeschränkte **Übermittlungsbefugnis**. Sie ist nur anwendbar bei einer durch einen Gerichtsbeschluss festgelegten Unterbringung in einer psychiatrischen Einrichtung. Unter diesen Umständen kann es für die Therapie oder andere Maßnahmen erforderlich sein, dass Daten über Verhaltensauffälligkeiten oder Krankheiten aus Urteilen, Ermittlungssachverhalten oder Gutachten verfügbar sind. Aus diesem Grund sind Ärzte, Psychologen, Gerichte und Behörden befugt, der psychiatrischen Einrichtung die erforderlichen Daten mitzuteilen. Unzulässig wäre diese Mitteilung, wenn andere Rechtsvorschriften außer solchen über die Berufs- und Amtsverschwiegenheit (z. B. § 203 StGB) dies untersagen würden.

Ärzte, Psychologen, Gerichte und Behörden sind aber nicht verpflichtet, diese Daten mitzuteilen. Die psychiatrische Einrichtung kann folglich die Stellen nicht dazu zwingen.

Eine Übermittlung personenbezogener Daten von der psychiatrischen Einrichtung an andere Stellen regelt diese Rechtsvorschrift nicht, siehe jedoch Absatz 5.

§ 43 Abs. 4 PsychKG M-V

Im Rahmen der Unterbringung nach § 1 Abs. 1 Nr. 3b darf die Einrichtung listenmäßig erfassen und speichern, welche Personen zu welchem Zeitpunkt und zu welchem Zweck die Einrichtung betreten oder verlassen haben.

Eine von einem Strafgericht angeordnete Unterbringung ist eine Maßregel, die im Zusammenhang mit den Bestimmungen der §§ 37 bis 41 dieses Gesetzes zu sehen ist. Aus diesem Grund ist eine Liste in dem gesetzlich bestimmten Umfang zu führen. Sie dient im Wesentlichen der Überwachung des Betroffenen.

§ 43 Abs. 5 PsychKG M-V

Die beteiligten Stellen dürfen die gemäß Absatz 2 erhobenen und gespeicherten personenbezogenen Daten für die Einleitung oder Durchführung eines Verfahrens nach dem Betreuungsgesetz an die zuständigen Behörden und Gerichte übermitteln, soweit es für das Verfahren erforderlich ist. Insoweit dürfen diese Daten auch für die Erstellung eines psychiatrischen oder psychologischen Gutachtens verwendet werden.

Die Übermittlung personenbezogener Daten an die zuständigen Behörden und Gerichte ist nach dieser Vorschrift nur zulässig, wenn sie nach dem Betreuungsgesetz erforderlich ist, um ein Verfahren durchzuführen oder einzuleiten. Es ist jeweils im Einzelfall zu prüfen, welche Daten für diesen Zweck erforderlich sind. Es dürfen auch nur Daten übermittelt werden, die für Zwecke nach Absatz 2 bereits erhoben worden sind. Die für ein Verfahren nach dem Betreuungsgesetz übermittelten Daten dürfen auch für ein psychiatrisches oder psychologisches Gutachten genutzt werden.

§ 43 Abs. 6 PsychKG M-V

Soweit die nach Absatz 2 gespeicherten Daten nicht in Krankenakten aufgenommen worden sind, sind sie spätestens zwei Jahre nach Beendigung der Unterbringung zu löschen. Nach Absatz 4 gespeicherte Daten sind unmittelbar nach der Entlassung der Betroffenen, auf die sie sich beziehen, zu löschen. Soweit ein solcher Bezug nicht besteht, sind diese Daten spätestens ein Jahr nach der Speicherung zu löschen.

Die festgelegten **Löschfristen** sind unbedingt einzuhalten, insbesondere, da es sich teilweise um Daten Dritter handelt, deren Nutzungszweck eingeschränkt ist, aber auch, weil diese Daten noch sensibler sind als sonstige Gesundheitsdaten. Sofern Daten in Krankenakten aufgenommen werden, ist die Löschfrist des § 19 Abs. 1 LKHG M-V anzuwenden: 30 Jahre nach Abschluss der Behandlung beziehungsweise wenn sie nicht mehr erforderlich sind.

§ 44 Bekanntgabe und Begründung von Anordnungen, Akteneinsicht

§ 44 Abs. 1 PsychKG M-V

Entscheidungen und Anordnungen im Rahmen der Unterbringung sind den Betroffenen unverzüglich bekannt zu geben und, soweit es der gesundheitliche Zustand des Betroffenen zulässt, zu erläutern. Sie sind in den jeweiligen Krankenakten zu vermerken und zu begründen. Soweit Entscheidungen oder Anordnungen schriftlich ergehen, erhalten die jeweiligen gesetzlichen Vertreter eine Abschrift.

Eine Entscheidung oder Anordnung über eine Unterbringung, die ein Betroffener nicht beeinflussen kann, ist ihm zumindest mitzuteilen und – soweit möglich – zu erläutern. Die psychiatrische Einrichtung hat dies in der Krankenakte zu dokumentieren. Dem gesetzlichen Vertreter ist eine Abschrift über eine schriftliche Entscheidung oder Anordnung zu geben.

§ 44 Abs. 2 PsychKG M-V

Die Betroffenen und ihre gesetzlichen Vertreter erhalten auf Verlangen unentgeltlich Auskunft über die zur Person der Betroffenen gespeicherten Daten sowie Einsicht in die über sie geführten Akten. Den Betroffenen können Auskunft und Einsicht verweigert werden, wenn eine Verständigung mit ihnen wegen ihres Gesundheitszustandes nicht möglich ist.

Ist bei einer vollständigen Auskunft oder Einsichtnahme mit schwerwiegenden gesundheitlichen Nachteilen bei dem Betroffenen zu rechnen, so soll der behandelnde Arzt die entsprechenden Inhalte unter Berücksichtigung des Gesundheitszustandes an den Betroffenen vermitteln. Die Verweigerung von Auskunft oder Einsicht ist mit einer Begründung in den Akten zu vermerken.

Das im Datenschutzrecht normierte **Auskunftsrecht** ist hier spezialgesetzlich ausgeformt. Ein Betroffener und sein gesetzlicher Vertreter erhalten danach ein umfassendes Auskunfts- bzw. Einsichtsrecht. Dieses Recht kann gegenüber dem Betroffenen ausgesetzt werden, wenn eine Verständigung mit ihm aus gesundheitlichen Gründen nicht möglich ist. Der Einzelfall kann es erforderlich machen, dass nicht vollständig Auskunft gegeben oder Einsicht gewährt wird, weil anderenfalls mit schwerwiegenden gesundheitlichen Nachteilen für den Betroffenen gerechnet werden müsste, wenn er Kenntnis vom Inhalt der Akte erlangt. In diesem Fall soll der behandelnde Arzt die entsprechenden Inhalte aus Dateien oder Akten unter Berücksichtigung des gesundheitlichen Zustandes an den Betroffenen vermitteln.

Zur (späteren) Prüfung, ob Auskunft oder Einsicht aus medizinischer Sicht zu Recht eingeschränkt oder verweigert wurde, ist dies mit entsprechender Begründung in der Krankenakte zu dokumentieren.

Dienstanweisung zum Datenschutz im Krankenhaus

Vorbemerkung

Die vielen, teilweise sehr detaillierten rechtlichen Grundlagen zum Datenschutz im Krankenhaus sind zwangsläufig abstrakt und oft nicht ohne weiteres in die Praxis vor Ort zu übertragen. Ein Instrument zur Transformation des geltenden Rechts in die praktische Anwendung ist eine Dienstanweisung zum Datenschutz. Ihre Notwendigkeit folgt nicht zuletzt aus dem gesetzlichen Erfordernis, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird, zum Beispiel § 21 Abs. 1 DSG M-V. Die Bedeutung solcher Dienstanweisungen steigt vor allem deshalb, weil sich immer mehr Krankenhäuser beim Umgang mit Patientendaten der elektronischen Datenverarbeitung bedienen. Aktuelle Entwicklungen auf diesem Gebiet sind unter anderem Krankenhaus- oder Klinikinformationssysteme (KIS) oder die Einführung der elektronischen Patientenakte.

Von einer Dienstanweisung zum Datenschutz ist ein Datenschutz- und Datensicherheitskonzept zu unterscheiden. Es enthält vor allem die technischen und organisatorischen Maßnahmen, die nach §§ 21, 22 DSG M-V oder § 9 BDSG erforderlich sind. Ausgehend von möglichen Bedrohungssituationen für die Daten und deren Sicherheit ist zu konzipieren, welche Sicherungsmaßnahmen zu treffen sind.

Wie die bisherigen praktischen Erfahrungen mit Dienstanweisungen generell, aber auch in Krankenhäusern gezeigt haben, bestehen oft Unsicherheiten, wo die inhaltlichen Schwerpunkte zu setzen sind, was einer konkreten Regelung bedarf und wo eine solche entbehrlich ist. Vielfach begegnet man Dienstanweisungen, die lediglich die einschlägigen gesetzlichen Bestimmungen zitieren, ohne konkret auf die Bedingungen des jeweiligen Hauses

einzugehen. Dies hilft dem einzelnen Mitarbeiter, der mit personenbezogenen Daten oder Patientendaten umgeht, in der Regel wenig. Gelegentlich wird die Unsicherheit noch dadurch erhöht, dass gesetzliche Bestimmungen unvollständig zitiert oder solche verwendet werden, die nicht einschlägig sind.

Die Dienstanweisung soll eine konkrete Anleitung für die mit den Patientendaten umgehenden Beschäftigten sein und sie dabei unterstützen, rechtliche Vorgaben in die Praxis umzusetzen. Außerdem sollte geregelt werden, auf welche Art und Weise die Betroffenen ihre gesetzlich normierten Rechte geltend machen können. Gegebenenfalls können aber auch Bestellung, Befugnisse und Pflichten eines internen Datenschutzbeauftragten mit aufgenommen werden.

Im Folgenden werden einige Hinweise gegeben, wie eine Dienstanweisung zum Patientendatenschutz aufgebaut sein könnte.

Gliederung

Bei der Gliederung ist es sinnvoll, sich im Wesentlichen am Aufbau der §§ 15 ff. LKHG M-V zu orientieren, das heißt, nach einer Einleitung in der Reihenfolge Erheben, Speichern, Nutzen, Übermitteln und besondere Verarbeitungsstufen vorzugehen. Danach könnten die Rechte der Betroffenen, Regelungen über Aufgaben und Befugnisse des Datenschutzbeauftragten und Sonstiges aufgenommen werden. Ein Beispiel ist das folgende Schema, das weder verbindlich ist noch Anspruch auf Vollständigkeit erhebt:

I. Allgemeines

1. Einleitung
2. Rechtliche Grundlagen
3. Schweigepflicht; Datengeheimnis

II. Patientendatenschutz im Einzelnen

1. Erheben und Speichern von Daten (§ 15 LKHG M-V)
2. Nutzen und Übermitteln von Daten (§ 16 Abs. 1, 4 LKHG M-V)
3. Grundsätze der Datenübermittlung
4. Übermittlung innerhalb des Krankenhauses (§ 16 Abs. 3 LKHG M-V)
5. Übermittlung an Stellen außerhalb des Krankenhauses
 - a) nach § 17 Abs. 1 Nr. 2 LKHG M-V
 - b) nach § 17 Abs. 1 Nr. 4 LKHG M-V
 - c) nach § 17 Abs. 1 Nr. 5 LKHG M-V
 - d) nach § 17 Abs. 1 Nr. 8 LKHG M-V
 - e) nach § 17 Abs. 1 Nr. 10 LKHG M-V
 - f) an die Sozialversicherungsträger (§ 301 SGB V)
 - g) an den MDK (§§ 275 ff. SGB V)
 - h) nach dem PStG
 - i) nach der BpflV und der KHStatV
6. Datenverarbeitung nach Abschluss der Behandlung (§ 19 LKHG M-V)
7. Datenverarbeitung für Forschungszwecke (§ 20 LKHG M-V)
8. Datenverarbeitung im Auftrag (§ 21 LKHG M-V)

III. Beschlagnahmeschutz

IV. Rechte der Betroffenen (§ 18 LKHG M-V)

V. Datenschutzbeauftragter des Krankenhauses (§ 20 DSG M-V)

Im Folgenden werden zu den einzelnen Gliederungspunkten die wichtigsten Aspekte genannt, auf die es bei einer Dienstanweisung ankommt:

Allgemeines

Einleitung

In einer Einleitung sollte der Anwendungsbereich der Dienstanweisung festgelegt werden. So ist klarzustellen, dass der Umgang mit Patientendaten und nicht der mit personenbezogenen Daten geregelt wird (siehe Begriffsbestimmung in § 14 Abs. 1 Satz 2 LKHG M-V). Zu beachten ist dabei insbesondere, dass nach § 14 Abs. 1 Satz 3 LKHG M-V auch Daten von Angehörigen, anderen Bezugspersonen oder Dritten, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden, zu den Patientendaten zählen.

Der Sozialdatenschutz der §§ 35 SGB I, 67 ff. SGB X gilt nicht für Krankenhäuser, sondern nur für Sozialleistungsträger, zum Beispiel die gesetzlichen Krankenkassen. Diese Vorschriften sollten in einer Dienstanweisung deshalb nicht erwähnt werden.

Bei datenschutzrechtlichen Beratungen wurde festgestellt, dass Dienstanweisungen auf die Tatsache fixiert sind, dass ein Krankenhaus Leistungen nach dem SGB V erbringt. Dies ist zwar überwiegend, aber nicht vollständig der Fall. Das Krankenhaus erbringt auch Leistungen für Selbstzahler beziehungsweise Privatpatienten und Sozialhilfeempfänger. Daher sollten die Aufgaben und die sich daraus ergebenden Datenübermittlungen an die Kostenträger der Krankenhausbehandlung vollständig beschrieben werden.

Rechtliche Grundlagen

Wie bereits erwähnt, ist es aus den genannten Gründen unzweckmäßig, die einschlägigen Rechtsvorschriften seitenweise zu zitieren. Ausreichend ist es, wenn die Vorschriften genannt und – falls erforderlich – als Anhang beigelegt werden.

Unbedingt aufzuführen sind:

- das LKHG M-V, dort insbesondere §§ 14 bis 21,
- das DSGVO M-V bzw. für privatrechtlich geführte Krankenhäuser das BDSG,
- das SGB V, insbesondere §§ 107 ff., 275, 276, 301,
- die BOÄ M-V.

Inwieweit noch weitere Vorschriften unter diesem Punkt der Dienstanweisung genannt werden oder erst weiter unten, wenn es auf sie ankommt, ist letztlich ohne Belang. Dies betrifft:

- §§ 203, 138, 139 StGB,
- §§ 53, 97 StPO,
- §§ 6 ff. IfSG,
- §§ 18, 34 PStG,
- § 6 BestattG M-V,
- § 17 BPfIV,
- die KHStatV,
- § 28 KHG.

Schweigepflicht, Datengeheimnis

Die Mitarbeiter – insbesondere Ärzte und deren Gehilfen – sollten mit dem grundlegenden Inhalt der Vorschriften des § 203 StGB und des § 2 BOÄ M-V vertraut gemacht werden. Ich empfehle, auch darauf hinzuweisen, dass die Schweigepflicht nicht nur gegenüber anderen Patienten oder Personen außerhalb des Krankenhauses gilt, sondern auch innerhalb des Hauses gegenüber anderen Beschäftigten, die nicht in die Behandlung einbezogen sind. **Patientendaten** dürfen nur aufgrund einer Rechtsvorschrift oder, sofern der Patient den Arzt von der Schweigepflicht für einen bestimmten Zweck entbindet, übermittelt werden.

Alle Krankenhausmitarbeiter mit Zugang zu Patienten- oder personenbezogenen Daten sind darüber hinaus auf das Datengeheimnis nach § 6 DSG M-V bzw. § 5 BDSG zu verpflichten. Deren Anwendungsbereiche sind weiter als der des § 203 StGB, denn sie erfassen auch Daten, die nicht der ärztlichen Schweigepflicht unterliegen. Folgerichtig schließt die Verweisungsnorm des § 14 Abs. 2 LKHG M-V die Anwendung von § 6 DSG M-V (bzw. § 9 BDSG) nicht aus. Deshalb sollte die Verpflichtung der Mitarbeiter in der Dienstanweisung geregelt sein. Der Dienstanweisung kann auch ein Muster einer solchen Erklärung beigelegt werden.

Patientendatenschutz im Einzelnen

Erheben und Speichern von Daten (§ 15 LKHG M-V)

In der Dienstanweisung sollte zunächst festgelegt werden, welche Stelle innerhalb des Krankenhauses welche Daten erhebt und speichert. Hierbei ist die Grenze des § 15 Abs. 1 LKHG M-V zu beachten. Bereits bei der Aufnahme des Patienten empfiehlt sich eine organisatorische Trennung zwischen medizinischen Daten und denen, die für die Verwaltung sowie zur Abrechnung erforderlich sind. Durch die organisatorische Trennung der Daten bereits beim Erheben lassen sich beispielsweise Zugriffsrechte leichter festlegen.

Die Mitarbeiter sollten in der Dienstanweisung darauf hingewiesen werden, welche Daten aufgrund von Rechtsvorschriften und welche auf freiwilliger Basis zu erheben sind. Beispielsweise sind Daten wie Religionszugehörigkeit (§ 15 Abs. 1 Nr. 2 LKHG M-V), solche über Angehörige oder die Telefonnummer **freiwillig**. Darüber müssen die Patienten beim Erheben informiert werden. Andere Daten – wie Angaben über den Arbeitgeber – sind nur erforderlich, wenn nicht die Krankenkasse, sondern beispielsweise eine Berufsgenossenschaft die Kosten trägt.

Nutzen und Übermitteln von Daten (§ 16 Abs. 1, 4 LKHG M-V)

Allgemein ist zu beachten, dass – abgesehen von den Ausnahmen in § 16 Abs. 1 S. 2 LKHG M-V – Daten nur für die Zwecke genutzt oder verarbeitet werden dürfen, für die sie erhoben worden sind (siehe § 15 Abs. 1 LKHG M-V). Diese **Zweckbindung** gilt auch mitarbeiterbezogen, deshalb darf jeder Mitarbeiter nur die Daten nutzen oder verarbeiten, die er für seine jeweilige Aufgabe benötigt.

Um dies organisatorisch zu sichern, sollte in der Dienstanweisung festgelegt werden, welche Mitarbeiter beziehungsweise welche Gruppe von Mitarbeitern welche Daten nutzen oder übermitteln dürfen. Auf dieser Grundlage sind dann die **Zugriffsberechtigungen** festzulegen. Dabei ist je nach Mitarbeiter und Aufgabengebiet auch nach der Art der Zugriffsberechtigung (lesender, schreibender oder verändernder Zugriff) zu differenzieren.

In diesem Zusammenhang könnten auch Maßnahmen zur nutzerbezogenen Protokollierung der Zugriffe auf die Datensätze in die Dienstanweisung aufgenommen werden.

Vorab sollte ein **Stammdatensatz** festgelegt werden, auf den jede Fachabteilung des Hauses im Rahmen ihrer Aufgaben zugreifen kann. Dieser Stammdatensatz ist auf den erforderlichen Umfang zu begrenzen. Er könnte beispielsweise den Namen des Patienten, den Aufenthaltsort im Krankenhaus, die behandelnde Abteilung sowie weitere wichtige Angaben enthalten. Der Zugriff auf den Stammdatensatz ist bestimmten – in der Dienstanweisung festzulegenden – Personen beziehungsweise Stelleninhabern einzuräumen. Der Umfang der Zugriffsberechtigung hat sich danach auszurichten, welche Zugriffe zur Aufgabenerfüllung erforderlich sind.

Des Weiteren könnte ein Notfalldatensatz festgelegt werden, auf den jedoch nur ärztliches beziehungsweise pflegerisches Personal Zugriff haben darf.

Die behandelnde Abteilung selbst hat Zugriff auf alle im Zusammenhang mit der Behandlung stehenden Daten. Die Dienstanweisung kann jedoch auch innerhalb der Abteilung differenzieren, welcher Personenkreis welche Zugriffsmöglichkeiten hat. Ein Zugriff auf alle Daten ist in der Regel nur für die in der Abteilung beschäftigten Ärzte (einschließlich Ärzte im Praktikum und zugewiesene PJ-Studenten) erforderlich, die an der Behandlung beteiligt sind. Der Umfang und die Art der Zugriffsberechtigung von Pflegepersonal und sonstigen Beschäftigten ist auf das jeweils erforderliche Maß zu beschränken. Den in der behandelnden Abteilung vorübergehend tätigen Ärzten (z. B. Nacht- oder Wochenenddienste) ist im Einzelfall eine Zugriffsmöglichkeit auf alle für den Zweck erforderlichen Daten zu schaffen. Dies muss nicht in allen Einzelheiten in der Dienstanweisung geregelt werden, sondern kann auch, gerade bei kleineren Häusern, der Entscheidung des Chefarztes der Abteilung vorbehalten bleiben.

Soweit medizinische Daten durch nichtmedizinisches Personal (z. B. durch die Verwaltung für Planungszwecke oder Wirtschaftlichkeits- und Organisationsuntersuchungen) genutzt oder übermittelt werden müssen, sollte die Dienstanweisung festlegen, durch welche **technischen und organisatorischen Maßnahmen** diese Daten vor der Nutzung anonymisiert werden, um der Vorschrift des § 16 Abs. 4 Satz 1 LKHG M-V zu entsprechen. In jedem Fall sollte das medizinische Personal die Daten vorher anonymisieren.

Für die Verarbeitung und Nutzung der eigenen Daten zu **Forschungszwecken** durch die behandelnde Abteilung ist nach § 16 Abs. 1 Satz 2 Nr. 4 LKHG M-V die Vorschrift des § 20 LKHG M-V anwendbar.

Grundsätze der Datenübermittlung

Übermittlungen von Patientendaten sind nach den unterschiedlichsten Rechtsgrundlagen zulässig. Zu unterscheiden ist zwischen **Datenübermittlungen** innerhalb des Krankenhauses nach § 16 Abs. 3 LKHG M-V und solchen an Stellen außerhalb des Krankenhauses, die entweder nach § 17 LKHG M-V oder einer der vielen Spezialvorschriften zulässig sind. Verantwortlich für die Zulässigkeit der Übermittlung ist grundsätzlich das Krankenhaus. Es hat beispielsweise durch vertragliche Vereinbarungen dafür zu sorgen, dass die Daten beim Empfänger mindestens genauso geheim gehalten werden, wie bei ihm selbst; Weiterübermittlungen vom Empfänger an Dritte bedürfen der Zustimmung des Krankenhauses, § 17 Abs. 2 und 3 LKHG M-V.

Die Art und Weise der Datenübermittlung hängt jeweils von den Umständen des Einzelfalls und den Gegebenheiten des Krankenhauses ab. Folgende Grundsätze sind zu beachten:

- Datenübermittlungen sind in jedem Fall zu protokollieren.
- Bei einer Übermittlung per Datenfernübertragung über öffentliche Netze sollten kryptographische Verfahren eingesetzt werden.
- Falls eine Computeranlage ferngewartet wird, sollte die Orientierungshilfe „Forderung an Wartung und Fernwartung“ der Datenschutzbeauftragten des Bundes und der Länder beachtet werden.
- Wegen der erheblichen Gefahren bei einer Datenübermittlung per Telefax (Ankommen beim falschen Empfänger, Kenntnisnahme durch Unbefugte auf der Empfängerseite usw.) sollte diese grundsätzlich unzulässig sein. Eine Ausnahme gilt in Notfällen, soweit eine andere Art der Übermittlung nicht in Frage kommt. Darauf ist in der Dienstanweisung hinzuweisen.
- Schließlich ist entsprechend der Vorschrift des § 16 Abs. 2 LKHG M-V bei den einzelnen Datenübermittlungen festzulegen, welcher Mitarbeiter beziehungsweise welche Mitarbeitergruppe welche Daten entsprechend ihrer jeweiligen Aufgabe und Funktion übermitteln darf.

Datenübermittlung innerhalb des Krankenhauses (§ 16 Abs. 3 LKHG M-V)

Innerhalb des Krankenhauses werden Daten vor allem dann übermittelt, wenn eine andere Fachabteilung zur Mit- oder Nachbehandlung einbezogen wird. Dabei ist zu beachten, dass § 16 Abs. 3 LKHG M-V die entsprechende Anwendung der Regelungen zur Datenübermittlung an Stellen außerhalb des Krankenhauses (§ 17 Abs. 1 LKHG M-V) für diesen Fall vorschreibt. Bei der Mit- oder Nachbehandlung (§ 17 Abs. 1 Nr. 2 LKHG M-V) hat dies zur Folge, dass der Patient über die Datenübermittlung informiert werden muss und ihr auch **widersprechen** kann („soweit der Patient nichts anderes bestimmt hat, ...“). Eine schriftliche Einwilligung ist hingegen nicht erforderlich.

Es gilt auch hier wieder der Grundsatz, dass nur die Daten übermittelt werden dürfen, die **erforderlich** sind, vgl. § 16 Abs. 1 LKHG M-V. Deshalb sind technische und organisatorische Maßnahmen vorzusehen, die sicherstellen, dass diesem Grundsatz Rechnung getragen wird. Die Dienstanweisung sollte auch für diesen Fall die Zugriffsberechtigung regeln. Die (ursprünglich) behandelnde Abteilung wird dabei in der Regel der mit- oder nachbehandelnden Abteilung den Zugriff einräumen. Letzterer können dabei alle erforderlichen Behandlungsdaten übermittelt werden, wobei ein Arzt entscheiden sollte, welche dies sind. Die Übermittlung ist zu dokumentieren.

Wird ein Patient zu einem späteren Zeitpunkt in eine andere **Fachabteilung** des Krankenhauses aufgenommen, ist dieser der Zugriff auf die früheren Behandlungsdaten zu gewähren, soweit ein medizinischer Sachzusammenhang gegeben ist. Die neu aufnehmende Abteilung ist verantwortlich für den Zugriff. Sie muss ihn begründen, und der Zugriff ist zu protokollieren. Im Übrigen ist auch der Patient darüber zu informieren.

Sollen anderen Abteilungen Daten für **Forschungszwecke** übermittelt werden, so sind die Vorschriften der §§ 16 Abs. 3, 17 Abs. 1 Nr. 6 und 20 LKHG M-V anzuwenden. Die behandelnde Abteilung hat sich vor der Übermittlung davon zu überzeugen, dass die Voraussetzungen der genannten Vorschriften vorliegen.

Die Form der Datenübermittlung an andere Leistungserbringer (z. B. Labore) sollte an dieser Stelle ebenfalls geregelt werden.

Datenübermittlung an Stellen außerhalb des Krankenhauses (§ 17 LKHG M-V)

Datenübermittlungen an Stellen außerhalb des Krankenhauses sind entweder nach § 17 Abs. 1 LKHG M-V oder nach anderen speziellen Vorschriften zulässig.

Für Datenübermittlungen nach § 17 Abs. 1 LKHG M-V sollte, zumindest für die häufig wiederkehrenden Fälle, in die Dienstanweisung aufgenommen werden, welche Daten jeweils „erforderlich“ im Sinne dieser Vorschrift sind und welcher Mitarbeiter beziehungsweise welche Mitarbeitergruppe für die Datenübermittlung zuständig ist. So empfehlen sich zumindest für die Nummern 2, 4, 5, 8 und 10 des § 17 Abs. 1 LKHG M-V Konkretisierungen.

a) Datenübermittlungen nach § 17 Abs. 1 Nr. 2 LKHG M-V

Bei der Datenübermittlung zur Mit- oder Nachbehandlung sollte für den wohl häufigsten Fall der ambulanten Nachbehandlung durch den Hausarzt festgelegt sein, dass der Patient die Möglichkeit erhält, einer solchen Nachbehandlung und der damit verbundenen Datenübermittlung zu widersprechen. Das heißt, der Patient muss entsprechend informiert und aufgeklärt werden. Eine ausdrückliche Einwilligung ist nicht erforderlich.

b) Datenübermittlung nach § 17 Abs. 1 Nr. 4 LKHG M-V

Diese Vorschrift regelt die Auskunftserteilung an Angehörige und sollte allein wegen der Häufigkeit von Anfragen auf jeden Fall in der Dienstanweisung konkretisiert werden.

Auskünfte an Angehörige des Patienten sind, soweit es sich um medizinische Daten handelt, grundsätzlich nur mit Einwilligung des Patienten zulässig. Dabei sollte man je nach Art der Auskunft wie folgt differenzieren:

- Auskünfte über den Aufenthaltsort des Patienten im Krankenhaus können von der Aufnahme, Pforte oder Station mitgeteilt werden, wenn ein ausdrücklicher, anders lautender Wille des Patienten dem nicht entgegensteht. Dies ist auch mündlich oder fernmündlich möglich, soweit der jeweilige Mitarbeiter von der Identität eines Angehörigen überzeugt ist und der Patient der Auskunftserteilung nicht widersprochen hat.
- Bei Auskünften über den Gesundheitszustand ist grundsätzlich im Einzelfall die Zustimmung des Patienten einzuholen. Ausgenommen davon ist bei Lebensgefahr die Auskunft an Angehörige, sofern der Patient nicht widersprochen hat oder wenn er bewusstlos und kein gegenteiliger Wille anzunehmen ist. Telefonische Auskünfte sind unzulässig.
- Patientennamen an Zimmertüren, Betten etc. sind nur mit Einwilligung des Patienten anzubringen.

c) Gesetzliche Mitteilungspflichten nach § 17 Abs. 1 Nr. 5 LKHG M-V

- an das Gesundheitsamt nach §§ 6 ff. IfSG

Die Meldepflicht an das Gesundheitsamt bei bestimmten übertragbaren Krankheiten stellt eine Durchbrechung der Schweigepflicht dar. Die damit verbundene Datenübermittlung sollte den behandelnden Ärzten vorbehalten bleiben. Dies kann im Einzelnen in der Dienstanweisung festgelegt werden.

- an das Gesundheitsamt nach § 6 BestattG M-V

Nach § 6 Abs. 2 des BestattG M-V sind Obduktionsscheine an das für den Sterbeort zuständige Gesundheitsamt unverzüglich zu übermitteln. Diese Verpflichtung kann in die Dienstweisung aufgenommen werden, verbunden mit konkreten Verantwortlichkeiten für diese Übermittlung.

- Anzeigepflicht geplanter Straftaten §§ 138, 139 StGB

Die Dienstweisung kann Ausführungen zur Anzeigepflicht bestimmter schwerer Straftaten enthalten. Auch Träger der Schweigepflicht sind danach verpflichtet, die in § 138 StGB genannten Straftaten (schwere Verbrechen wie Mord, Totschlag, Raub, Menschenhandel usw.) anzuzeigen. Melden sie eine solche geplante Straftat nicht, gehen sie dennoch gemäß § 139 Abs. 3 StGB straffrei aus, wenn sie sich ernsthaft bemüht haben, die Tat ihres Patienten abzuwenden, es sei denn, dass es sich um solche Straftaten handelt, die Absatz 3 gesondert aufzählt und aus dem Katalog des § 138 StGB herausnimmt. Diese Straftaten sind immer anzuzeigen, ein Bemühen, die Tat zu verhindern, genügt für eine Straffreiheit nicht. Auf diese gesetzlichen Bestimmungen sollten die Mitarbeiter hingewiesen werden.

d) Datenübermittlungen nach § 17 Abs. 1 Nr. 8 LKHG M-V

Bei der Konkretisierung von § 17 Abs. 1 Nr. 8 LKHG M-V ist genau festzulegen, welche Daten übermittelt werden. Zu beachten ist, dass von dieser Vorschrift nicht nur Datenübermittlungen an privatärztliche Verrechnungsstellen erfasst sind, sondern auch an Sozialhilfeträger für die Abrechnung der in Anspruch genommenen Leistungen von Sozialhilfeempfängern. Bei gesetzlich Versicherten gilt ohnehin § 301 SGB V.

e) Datenübermittlungen nach § 17 Abs. 1 Nr. 10 LKHG M-V

Für den Fall der Übermittlung an Krankenhausseelsorger (§ 17 Abs. 1 Nr. 10 LKHG M-V) ist entweder eine Regelung aufzunehmen, welche Daten übermittelt werden (ausreichend sind Name und Aufenthalt des Patienten im Krankenhaus), oder – falls vorhanden – kann auf eine entsprechende Vereinbarung des Krankenhauses mit der (oder den) Kirche(n) Bezug genommen werden.

f) Datenübermittlung an die Sozialversicherungsträger (§ 301 SGB V)

Aufgrund der sehr detaillierten Regelungen in § 301 Abs. 1 SGB V einerseits und der „Vereinbarung gemäß § 301 Abs. 3 SGB V über das Verfahren zur Abrechnung und Übermittlung der Daten nach § 301 Abs. 1 SGB V (Datenübermittlungs-Vereinbarung)“ andererseits sollte sich die Dienstweisung auf die organisatorischen Maßnahmen im Krankenhaus (insbesondere welche Mitarbeiter Zugriff auf die Abrechnungsdaten haben und wer Daten verarbeiten und übermitteln darf) und das Verfahren der Datenübermittlung beschränken. Auf die Vereinbarung sollte aber zumindest Bezug genommen werden.

g) Datenübermittlung an den MDK

Angesichts der häufigen Unklarheiten, welche Befugnisse der MDK hat, sollte eine Dienstweisung die Mitarbeiter präzise darüber und über die Kompetenzen des MDK aufklären. Wichtig ist insbesondere, dass der MDK nur Prüfungen im Auftrag einer gesetzlichen Krankenkasse vornehmen darf. Wie auch immer geartete Routineprüfungen und/oder Prüfungen ohne konkreten Auftrag einer gesetzlichen Krankenkasse sind nicht zulässig. Deshalb sollte die Dienstweisung regeln, wer im Krankenhaus verantwortlich beurteilt, ob Prüfungen des MDK zulässig sind, und wer befugt ist, die Akteneinsicht nach § 276 Abs. 4 SGB V oder die Übermittlung von Daten nach § 276 Abs. 2 Satz 1 SGB V abzulehnen, wenn die Voraussetzungen nicht erfüllt sind. Außerdem sind die Verträge zwischen der Krankenhausgesellschaft Mecklenburg-Vorpommern (KGMV) und den Spit-

zenverbänden der gesetzlichen Krankenversicherung unter Einbeziehung des MDK zu berücksichtigen.

Im Falle der Datenübermittlung nach § 276 Abs. 2 Satz 2 SGB V, bei Beratungstätigkeit durch den MDK gemäß § 275 Abs. 4 SGB V, ist in der Dienstanweisung darauf hinzuweisen, dass die Daten zu anonymisieren sind.

Schließlich sollte in der Dienstanweisung auch festgelegt sein, wie die Einsichtnahme des MDK in Krankenunterlagen bei Fehlbelegungsprüfungen gemäß § 17a Abs. 2 KHG organisatorisch durchgeführt wird. Siehe insgesamt zum MDK die Erläuterungen Seite 57.

h) Datenübermittlung nach dem PStG

Bei Geburten und Sterbefällen in einem öffentlichen Krankenhaus hat der Leiter der Anstalt oder ein von ihm ermächtigter Mitarbeiter eine ausschließliche Anzeigepflicht an das Standesamt gemäß §§ 18, 34 PStG. In diesem Zusammenhang sollte die Dienstanweisung regeln, wer die Geburt oder den Sterbefall anzeigt.

i) Datenübermittlung zu statistischen Zwecken nach der BPflV und der KHStatV

Zu statistischen Zwecken hat nach § 17 Abs. 4 Satz 4 BPflV der Krankenhausträger auf Verlangen einer Vertragspartei und den nach § 18 Abs. 1 KHG genannten Beteiligten (Sozialversicherungsträger oder Verband) anonymisierte Statistiken zu übermitteln.

Ebenso kann der Krankenhausträger nach § 7 KHStatV Diagnosestatistiken anonymisiert an das Sozialministerium übermitteln. Dazu bedarf es für die Übermittlung von diagnosebezogenen Daten nach § 3 Nr. 14 KHStatV der Zustimmung des Krankenhauses.

Es empfiehlt sich festzulegen, welche Stelle die anonymisierten Daten nach den jeweiligen Vorschriften übermittelt.

Schließlich führt das Statistische Landesamt nach § 1 KHStatV Erhebungen über die Krankenhäuser als Bundesstatistik durch. Erhebungsmerkmale ergeben sich aus § 3 KHStatV. Auch hierbei ist die Anonymisierung zu beachten.

Datenverarbeitung nach Abschluss der Behandlung (§ 19 LKHG M-V)

Nach Abschluss der Behandlung sollte bei automatisierter Speicherung nach einem angemessenen Zeitraum der Kreis der Zugriffsberechtigten verringert werden. Die Daten sind für den Direktzugriff gemäß § 19 Abs. 3 LKHG M-V zu sperren. Die Dienstanweisung sollte regeln, durch welche technischen und organisatorischen Maßnahmen der Vorschrift des § 19 LKHG M-V entsprochen wird.

Bei der **Archivierung** ist darauf zu achten, dass die Datensätze beziehungsweise die Akten getrennt nach Behandlungen gespeichert und abgelegt werden, so dass bei einer späteren Behandlung durch eine andere Abteilung nicht alle Informationen auf einmal ohne weiteres zugänglich sind. Dies dient außerdem der Einhaltung der Vorschrift des § 19 Abs. 2 Satz 4 LKHG M-V, wonach zur Erschließung der Akten ein Nachweis zu führen ist, zu dem andere Bereiche keinen direkten Zugriff haben. Eine Archivierung nach Geburtsdaten und Namen genügt diesen Anforderungen nicht. Querverweise auf das Vorhandensein weiterer Bestände sind selbstverständlich zulässig. Die Mitarbeiter sollten auf die Einhaltung der Vorschrift des § 19 Abs. 2 Sätze 4 und 5 LKHG M-V hingewiesen werden, die die Möglichkeiten der Aufhebung der Sperrung abschließend regelt.

Datenverarbeitung für Forschungszwecke (§ 20 LKHG M-V)

Es sollte auch darauf hingewiesen werden, dass zur **Forschung** mit Patientendaten grundsätzlich die **Einwilligung** erforderlich ist, es sei denn, dass die Voraussetzungen des § 20 Abs. 2 LKHG M-V vorliegen. In jedem Falle sind die Patientendaten so früh wie möglich zu anonymisieren. Patientendaten dürfen für diesen Zweck entsperrt werden, wenn sichergestellt ist, dass die Daten so genutzt werden, dass keinerlei Personenbezug mehr herstellbar ist. Ein verantwortlicher Mitarbeiter hat die Einhaltung dieses Verfahrens zu kontrollieren. Organisatorisch ist außerdem die Einhaltung der Vorschrift des § 20 Abs. 2 Satz 2 LKHG M-V sicherzustellen. Schließlich ist der **Datenschutzbeauftragte des Krankenhauses** bei Übermittlungen zu Forschungszwecken zu beteiligen.

Datenverarbeitung im Auftrag (§ 21 LKHG M-V)

Die Datenverarbeitung im Auftrag sollte – schon wegen des gelockerten Beschlagnahmeschutzes (siehe auch Seite 43) – nur im Ausnahmefall durchgeführt werden. Außerdem sind weitere Vorkehrungen zu treffen, die den Beschlagnahmenschutz gewährleisten. Darüber hinaus sollte die Dienstanweisung organisatorische Maßnahmen vorsehen, die die strikte Einhaltung aller Datenschutzbestimmungen des LKHG M-V sicherstellen. Die Stelle, die Daten im Auftrag verarbeitet, muss sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwerfen. Das Krankenhaus sollte die Beziehungen zur verarbeitenden Stelle so gestalten, dass es jederzeit die Einhaltung der datenschutzrechtlichen Vorschriften kontrollieren kann und die verarbeitende Stelle den Weisungen des Krankenhauses unterworfen ist. Unbedingt ist das Trennungsgebot beachten.

Beschlagnahmenschutz

Bei diesem Punkt ist vor allem die Vorschrift des § 97 Abs. 2 Satz 2 StPO zu nennen, die die Beschlagnahmefreiheit für Krankenhäuser ausdrücklich regelt. Den Mitarbeitern sollte durch einen entsprechenden Hinweis in der Dienstanweisung bewusst werden, dass Beschlagnahmen von Patientenunterlagen durch die Staatsanwaltschaft in der Regel unzulässig sind und Akten nicht herausgegeben werden dürfen (siehe hierzu Seite 7 und die Ausführungen zu § 21 Abs. 6 LKHG M-V, Seite 47).

Rechte des Betroffenen (§ 18 LKHG M-V)

Die Mitarbeiter sind in der Dienstanweisung auf den Umfang und die Beschränkungen des Auskunfts- und Akteneinsichtsrechtes hinzuweisen. Der wesentliche Inhalt von § 18 LKHG M-V sollte dabei dargestellt werden.

Datenschutzbeauftragter des Krankenhauses (§ 20 DSG M-V)

Nach § 14 Abs. 2 LKHG M-V, § 20 DSG M-V bzw. §§ 4f und 4g BDSG hat jedes Krankenhaus einen Datenschutzbeauftragten zu bestellen.

Die Dienstanweisung könnte die Einordnung des Datenschutzbeauftragten in die Hierarchie des Krankenhauses präzisieren und seine Aufgaben und Kompetenzen im Einzelnen festlegen. Hierzu sei auf die ausführlichen Erläuterungen zu § 20 DSG M-V, Seite 48, verwiesen.

Anhang

Datenschutzbehörden in Mecklenburg-Vorpommern

Kontrollbehörde für den öffentlichen Bereich

Postanschrift

Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern
Schloss Schwerin
19053 Schwerin

Hausanschrift

Johannes-Stelling-Straße 21
19053 Schwerin

Telefon: (03 85) 5 94 94-0
Telefax: (03 85) 5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: <http://www.lfd.m-v.de>

Aufsichtsbehörde für den nicht-öffentlichen Bereich

Postanschrift

Innenministerium
Mecklenburg-Vorpommern
II 250
19048 Schwerin

Hausanschrift

Arsenal am Pfaffenteich
Karl-Marx-Straße 1
19055 Schwerin

Telefon: (03 85) 5 88-22 50
Telefax: (03 85) 5 88-29 78
E-Mail: II2vz@im.mv-regierung.de
Internet: <http://www.mv-regierung.de/im/index.htm>

Datenschutzbeauftragte für den kirchlichen Bereich

Für die Evangelisch-Lutherische Landeskirche Mecklenburgs:

Herr Rechtsanwalt Schütte
Am Kamp 5
18209 Bad Doberan

Telefon: (03 82 03) 1 29 47
Telefax.: (03 82 03) 1 29 06
E-Mail: rbr.raeschuette@set.de

Pommersche Evangelische Kirche

Das Konsistorium
Datenschutzbeauftragter
Postfach 31 52
17461 Greifswald

Telefon: (0 38 34) 55 46

Katholische Kirche:

Der Beauftragte für den Datenschutz
der Erzbistümer Berlin und Hamburg,
der Bistümer Hildesheim und Osnabrück und
des Bischöflich Münsterschen Offizialates in Vechta
Herr Lutz Grammann
Plathnerstraße 43

30175 Hannover

Telefon: (05 11) 81 93 15

Telefax: (05 11) 81 21 35

Muster einer Bestellung zur oder zum behördlichen Datenschutzbeauftragten gemäß § 20 DSG M-V in öffentlich-rechtlich geführten Krankenhäusern

Frau/Herr wird mit Wirkung vom zur/zum behördlichen Datenschutzbeauftragten bei [Bezeichnung der Daten verarbeitenden Stelle] bestellt.

Gemäß § 20 DSG M-V (in der Fassung vom , GVOBl. M-V S.) werden ihr/ihm damit folgende Aufgaben übertragen:

1. Sie/Er überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei [Bezeichnung der Daten verarbeitenden Stelle]
2. Bei der Einführung neuer und der Änderung bestehender Datenverarbeitungsmaßnahmen bzw. automatisierter Verfahren wirkt sie/er auf die Einhaltung der Datenschutzvorschriften hin und berät [Bezeichnung der Daten verarbeitenden Stelle] bei der Auswahl und der Gestaltung von Verfahren zur Verarbeitung personenbezogener Daten. Dies betrifft auch Verfahren der Auftragsdatenverarbeitung nach § 4 DSG M-V oder bereichsspezifischen Vorschriften.
3. Sie/Er hat die Beschäftigten mit den Bestimmungen des DSG M-V sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen.
4. Die ihr/ihm von [in der Regel der IT-Abteilung] zur Verfügung gestellten Unterlagen nach § 18 DSG M-V (Verfahrensverzeichnis) führt sie/er in geordneter Form. Sie/Er hält das Verzeichnis gemäß § 20 Abs. 4 DSG M-V zur Einsicht bereit. Dabei hat sie/er die Einschränkungen des § 20 Abs. 4 Satz 2 DSG M-V zu beachten. In Zweifelsfällen ist [in der Regel die Behördenleitung] vor einer Einsichtnahme zu benachrichtigen.
5. Das nach § 18 DSG M-V zu führende Verfahrensverzeichnis ist von ihr/ihm darauf hin zu überprüfen, ob es Hinweise auf systembedingte Verstöße gegen das Datenschutzrecht gibt. Soweit dies der Fall ist und bei Stichprobenprüfungen hat sie/er eine datenschutzrechtliche Bewertung vorzunehmen und[in der Regel die Behördenleitung] über das Ergebnis zu informieren.
6. Sofern ein automatisiertes Verfahren, das die Verarbeitung personenbezogener Daten gemeinsam mit anderen Daten verarbeitenden Stellen (gemeinsames Verfahren) oder die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) ermöglicht, eingerichtet oder geändert wird, sowie bei der Einrichtung und Änderung automatisierter Verfahren, mit denen personenbezogene Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben verarbeitet werden, hat sie/er die Vorabkontrolle gemäß § 19 Abs. 2 DSG M-V durchzuführen.

7. Bei gemeinsamen Verfahren und Abrufverfahren hat sie/er die Protokolldatenbestände daraufhin zu prüfen, ob sie Hinweise auf Datenschutzverstöße enthalten. Diese Prüfung ist innerhalb von [maximal 12 Monaten] zu wiederholen und das Ergebnis zu dokumentieren.
8. Sie/Er hat allen Angelegenheiten des Datenschutzes nachzugehen, die von den Beschäftigten der/des [Bezeichnung der Daten verarbeitenden Stelle] oder von Betroffenen an sie/ihn herangetragen werden. Auf die Einhaltung des Dienstweges darf dabei nicht bestanden werden.
9. Sie/er kann sich jederzeit an den Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, Schloss Schwerin, 19053 Schwerin, Telefon (03 85) 5 94 94-0 wenden und dessen Beratung in Anspruch nehmen.
10. Stellt sie/er Verstöße gegen die Vorschriften des DSGVO M-V oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bei [Bezeichnung der Daten verarbeitenden Stelle] fest, fordert sie/er die jeweils zuständigen Mitarbeiterinnen oder Mitarbeiter zur Mängelbeseitigung auf. Mit der Feststellung von Mängeln sollten Vorschläge zu ihrer Beseitigung und zu sonstigen Verbesserungen des Datenschutzes verbunden werden. Über alle ihr/ihm bedeutsam erscheinenden datenschutzrechtlich relevanten Sachverhalte sollte sie/er [in der Regel die Behördenleitung] unmittelbar informieren.
11. Sie/Er hat sich so aus- und fortzubilden, dass sie/er die für die Erledigung der übertragenen Aufgaben erforderliche Fachkunde besitzt.
12. Neben der Tätigkeit als behördliche(r) Datenschutzbeauftragte(r) übt sie/er keine weiteren Aufgaben aus.
oder
Neben der Tätigkeit als behördliche(r) Datenschutzbeauftragte(r) übt sie/er die im jeweils gültigen Geschäftsverteilungsplan ausgewiesenen Aufgaben aus.
13. Sollten sich hierdurch oder aus anderen Gründen Konfliktsituationen (im Sinne des § 20 Abs. 1 Satz 3 DSGVO M-V) oder Beeinträchtigungen der Tätigkeit als behördliche(r) Datenschutzbeauftragte(r) (im Sinne des § 20 Abs. 1 Satz 2 DSGVO M-V) ergeben, ist dies bei [in der Regel der Behördenleitung] anzuzeigen.

Frau/Herr ist bei der Ausübung des Amtes weisungsfrei. Ihre/Seine Kontroll- und Einsichtsrechte ergeben sich insbesondere aus § 20 Abs. 1 Sätze 4 und 5, Abs. 3 DSGVO M-V. Die Art und der Umfang der zur Erfüllung der Aufgaben notwendigen Mittel ist bei[in der Regel der Behördenleitung] anzu-melden.

Sie/Er kann jederzeit von dem Amt zurücktreten.

Ort, Datum
Unterschrift der Leitung der Daten verarbeitenden Stelle

Orientierungshilfe „Forderung an Wartung und Fernwartung“

des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der ständigen
Konferenz der Datenschutzbeauftragten des Bundes und der Länder
(Stand März 1993)

Die speichernde Stelle ist für alle Daten und Verfahren selbst verantwortlich. Sie hat dafür Sorge zu tragen, dass der Einzelne davor geschützt wird, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Die speichernde Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, Datenschutz und Datensicherheit zu gewährleisten.

Hersteller von DV-Anlagen, externe Software-Ersteller und Wartungsfirmen dürfen daher nur auf konkrete Weisung der speichernden Stelle tätig werden. Art und Umfang dieser Service-Tätigkeit bestimmt stets die speichernde Stelle. Sie unterscheidet, ob und in welcher Weise Dritte auf dem DV-System tätig werden können. In einem solchen Falle legt die speichernde Stelle schriftlich fest, dass die Wartungsarbeiten möglichst ohne Kenntnisnahme personenbezogener Daten durchgeführt werden.

Ist dies nicht möglich,

- ist die Kenntnisnahme personenbezogener Daten externen Dritten nach vorheriger Risikoabschätzung nur in dem Umfang erlaubt, wie dies für die konkreten Arbeiten im Einzelfall unerlässlich ist,
- kann das Zugänglichmachen personenbezogener Daten nur in besonderen Ausnahmefällen erfolgen, wobei die offenbarten Daten einer strengen Zweckbindung unterliegen und eine Weitergabe an Dritte untersagt ist.

Die speichernde Stelle hat technisch und organisatorisch sicherzustellen, dass eine Wartung oder Fernwartung (Fernbetreuung) nur mit ihrem Einverständnis und im Einzelfall erfolgen kann.

Die speichernde Stelle hat ferner sicherzustellen, dass sie kontrollieren kann, was bei einer Wartung oder Fernwartung im Einzelnen geschieht, insbesondere, welche Zugriffe auf personenbezogene Daten erfolgen. Bei Systemen mit sensiblen personenbezogenen Daten hat sie diese Kontrolle in jedem Einzelfall durchzuführen. Das hat jedoch zur Folge, dass eigenes Personal vorhanden und entsprechend geschult ist, um diese Aufgabe zuverlässig erledigen zu können.

Schließlich muss die Fernwartungszentrale angemessene technische, organisatorische und personelle Sicherheitsanforderungen erfüllen.

Sicherheitsmaßnahmen für Wartung und Fernwartung:

1. Maßnahmen zur Zugangskontrolle

- 1.1 Die Personen, die die Wartungsarbeiten an der DV-Anlage durchführen, müssen sich den gleichen strengen Zugangskontrollprüfungen unterziehen wie das eigene Personal.
- 1.2 Bei der Fernwartung muss der Verbindungsaufbau stets durch den Kunden erfolgen, so dass Wartungsarbeiten nur mit Wissen und Willen des Kunden beginnen können.

- 1.3 Der Kreis des autorisierten Wartungspersonals ist festzulegen; ohne genaue Identifikation dürfen keine Wartungsarbeiten beginnen.
- 1.4 Der Kunde muss das Wartungspersonal als autorisiert identifizieren können.
- 1.5 Um zu verhindern, dass ein unbefugter Teilnehmer Zugriff auf das DV-System erhält, ist die Verbindung vom DV-System aus aufzubauen. Die Anschlussnummern der zulässigen Partner, einschließlich Fernwartungszentrale, sind einzuprogrammieren, so dass ein Anwählen einer anderen Nummer unmöglich wird.
- 1.6 Der Kunde muss die Fernwartungsarbeiten jederzeit abbrechen können.

2. Organisation der Datenträgerkontrolle

- 2.1 Bevor ein Datenträger mit Kundendaten den DV-Bereich zu Wartungszwecken oder zur Fehleranalyse verlässt, ist die Genehmigung einer vom Kunden dafür autorisierten Person einzuholen. Auf einem Begleitschein sind die Art der Daten und des Datenträgers zu vermerken. Für die Rücklaufkontrolle muss eine Kopie beim Kunden verbleiben.
- 2.2 Wenn personenbezogene Daten an die Fernwartungszentrale übertragen werden müssen, ist vorher die Erlaubnis durch eine vom Kunden autorisierte Person einzuholen.
- 2.3 Die Übertragung von Daten aus dem DV-System des Kunden an die Fernwartungszentrale ist nur bei gleichzeitiger Protokollierung der übertragenen Daten zuzulassen.
- 2.4 Die Kontrolle der protokollierten Daten ist DV-technisch durch geeignete Kommandos oder Dienstprogramme zu unterstützen.
- 2.5 Es ist sicherzustellen, dass das Wartungspersonal nicht mit den eigenen mitgebrachten Datenträgern die Wartung durchführt, sondern ausschließlich mit Duplikaten arbeitet, die an der DV-Anlage des Kunden zu erstellen und dort dann für Kontrollzwecke für einen bestimmten Zeitraum (in der Regel ein Jahr) aufzubewahren sind.
- 2.6 Es ist darauf zu achten, dass Wartungstechniker keine am DV-System benützten Datenträger ungelöscht mitnehmen.
- 2.7 Alle Wartungs- und Übertragungsaktivitäten müssen an der Kundenkonsole zum Mitlesen sichtbar gemacht werden.

3. Maßnahmen zur Speicherkontrolle

- 3.1 Der Betreiber der DV-Anlage muss alle Programme durch Passworte schützen, soweit diese bei der Wartung physisch im Zugriff bleiben.
- 3.2 Das Wartungspersonal muss sich einer Anmeldeprozedur unterwerfen. Diese muss aus einer Identifikation (Benutzerkennung) und einer Authentifikation (Passwort) bestehen. Die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalterprivilegien einschließt.
- 3.3 Werden Test- und Service-Programme des Herstellers auf der DV-Anlage gespeichert, sind diese unter der Wartungskennung abzuspeichern.
- 3.4 Der Zugriffsschutz muss hinreichend differenziert sein.
- 3.5 Ist für Wartungszwecke ein Zugriff auf Kundendaten erforderlich, ist zu prüfen, ob sensible personenbezogene Kundendaten aus dem direkten Zugriff zu entfernen sind. Im Rahmen der Fernwartung ist der Zugriff auf Kundendaten grundsätzlich zu verhindern. Dabei ist denkbar, die Laufwerke, auf denen diese Daten gespeichert werden, vom DV-System physikalisch abzutrennen, soweit dies technisch möglich ist.
- 3.6 Ein Einspielen von Änderungen ins Betriebssystem, in systemnahe Software oder Anwendungsfremdsoftware im Rahmen der Fernwartung ist nicht zuzulassen. Die Änderungen sind ausschließlich vor Ort entweder vom Kunden selbst oder nach Freigabe durch eine vom Kunden dafür autorisierte Person vom Software-Hersteller in die entsprechende Software zu übernehmen. Dasselbe gilt für die Fehlerbehebung.

- 3.7 Wartungs- und Diagnosearbeiten im laufendem Betrieb, insbesondere, wenn sie die Software betreffen, sind unter ständiger Kontrolle eines sachkundigen Kundenmitarbeiters durchzuführen.
- 3.8 Es muss ausgeschlossen werden, dass vom Kunden erstellte Software und Kundendateien durch die Wartung verändert werden können.
- 3.9 Es ist auszuschließen, dass Anwendungsprogramme durch die Fernwartung aktiviert werden können, solange Kundendateien im direkten Zugriff stehen.

4. Maßnahmen zur Zugriffskontrolle

- 4.1 Für den Fall, dass in einem Wartungsvorgang ein Zugriff auf Dateien mit Kundendaten notwendig ist, sind nach Abschluss der Wartungsarbeiten die der Wartung offenbarten Passworte unverzüglich zu ändern.
- 4.2 Alle Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festgehalten werden, sind zu überprüfen und zur Beweissicherung mindestens ein Jahr aufzubewahren. Die Verpflichtung des beim Kunden für das DV-System Verantwortlichen, den Wartungsvorgang am Bildschirm zu verfolgen und gegebenenfalls zu unterbrechen, bleibt davon unberührt.

5. Maßnahmen zur Transportkontrolle

- 5.1 Beim Transport von Datenträgern sind der Transportweg und die am Transport beteiligten Personen festzulegen.
- 5.2 Es ist zu prüfen, ob beim Versand von Datenträgern für Wartungszwecke die Versandart angemessen und ausreichend ist.
- 5.3 Die Vollständigkeit der Unterlagen ist zu prüfen. Der Transport muss ausschließlich mit Begleitpapieren erfolgen.

6. Maßnahmen zur Organisationskontrolle

- 6.1 Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Kundenpersonal zu treffen. Art und Umfang der Wartung (Hard- und Software) sind schriftlich festzulegen.
- 6.2 Das Wartungspersonal ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten.
- 6.3 Eine Weitergabe von Daten, die dem Wartungspersonal übergeben oder bei der Fernwartung übertragen wurden, an Dritte ist vertraglich zu untersagen. Diese Daten sind ausschließlich für Zwecke der Wartung zu verwenden und nach Abschluss der Wartungsarbeiten oder der Fehlersuche unverzüglich zu löschen. Für eventuell weitergegebene Listen mit personenbezogenen Daten ist eine Rückgabe nach Abschluss der Wartungsarbeiten zu vereinbaren.
- 6.4 Hinsichtlich der Fernwartung wird empfohlen, einen separaten Vertrag abzuschließen, in dem Sicherheitsmaßnahmen festgelegt werden und die Kontrolle der Einhaltung aller Maßnahmen geregelt wird.
- 6.5 Zur DV-Revision ist der Betreiber der DV-Anlage gehalten, das Wartungs- bzw. Fernwartungskonzept schriftlich zu dokumentieren.
- 6.6 Die Systemverantwortlichen beim Kunden sind regelmäßig bezüglich der Möglichkeiten der Fernwartung zu schulen.
- 6.7 Die Einhaltung der getroffenen Sicherheitsmaßnahmen ist regelmäßig zu überprüfen.

Weiterführende Informationen und Literatur

Allgemeine Informationen und Verweise

<http://www.datenschutz.de>

Kostenlose Broschüren, Faltblätter, Orientierungshilfen und weitere Informationen des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern

<http://www.lfd.m-v.de>

Ergebnisse der Konferenzen der Datenschutzbeauftragten des Bundes und der Länder

<http://datenschutz-berlin.de/doc/de/konf/index.htm>

Adressen der Landesbeauftragten für den Datenschutz

<http://datenschutz-berlin.de/sonstige/behoerde/lfdauf.htm>

Adressen der Aufsichtsbehörden für den Datenschutz

<http://datenschutz-berlin.de/sonstige/behoerde/aufsicht.htm>

Fundstellen für Rechtsverordnungen und Gesetze im Internet

Bundesrecht

<http://bundesrecht.de>

<http://jurcom5.juris.de/bundesrecht/index.html>

<http://datenschutz-berlin.de/gesetze/bund.htm>

Landesrecht

<http://www.mv-regierung.de/laris/>

Abkürzungsverzeichnis

Abs.	Absatz
AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BestattG M-V	Bestattungsgesetz Mecklenburg-Vorpommern
BGB	Bürgerliches Gesetzbuch
BOÄ M-V	Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern
BPfIV	Bundespfllegesatzverordnung
DKI	Deutsches Krankenhausinstitut
DSG M-V	Datenschutzgesetz Mecklenburg-Vorpommern
GG	Grundgesetz
HeilBerG	Heilberufsgesetz
IfSG	Infektionsschutzgesetz
KGMV	Krankenhausgesellschaft Mecklenburg-Vorpommern
KHG	Krankenhausfinanzierungsgesetz
KHStatV	Krankenhausstatistik-Verordnung
KrebsRAG MV	Krebsregisterausführungsgesetz Mecklenburg-Vorpommern
LfD	Landesbeauftragter für den Datenschutz
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
MDK	Medizinischer Dienst der Krankenversicherung
PStG	Personenstandsgesetz
PsychKG M-V	Psychischkrankengesetz Mecklenburg-Vorpommern
SGB I	Sozialgesetzbuch Erstes Buch
SGB V	Sozialgesetzbuch Fünftes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
SQS	Servicestelle Qualitätssicherung
ZPO	Zivilprozessordnung

Stichwortverzeichnis

Akteneinsicht	32, 74
Archivierung	43, 73
Aufbewahrungsfrist.....	34
Aufsichtsbehörde	39
Auskunft.....	32, 65, 74
Behandlungsvertrag	16, 26
Beschlagnahme	6, 46, 74
Beschlagnahmeverbot.....	6
Beschwerde.....	7, 30
Daten	
Anonymisierte Daten.....	42
Archivierung	43, 73
Dritter.....	32, 67
Entsperrung.....	36
Erforderlichkeit.....	7, 16, 25, 61
Erheben	16, 68
Löschung	34, 64
Nutzung	21, 24, 68
Patientendaten.....	5, 13, 63
Pseudonymisierte Daten	38
Speichern	16, 68
Sperrung.....	34
Sperrvermerk	35
Übermittlung.....	22, 25, 31, 63, 69
Verarbeitung im Auftrag	42, 74
Daten Dritter	13
Datengeheimnis.....	12
Datenschutzbeauftragter	39, 47, 74
Aufgaben	48
Bestellung	48
Interessenkollision.....	51
Personalrat	50
Rechtsstellung.....	51
Verschwiegenheit	48
Vertreter.....	49
Datenverarbeitung im Auftrag	42
Dokumentation.....	10, 14, 23, 32, 39
Durchsuchung	6
Einwilligung.....	5, 6, 17, 18, 37, 61
Einsichtsfähigkeit	19
Freiwilligkeit	18, 37
Minderjährige	19
Schriftform.....	18
Widerruf.....	19
Erforderlichkeit der Daten	7, 16, 25, 61
Erlaubnisvorbehalt	4
Ermessensspiel	9
Ersuchen.....	7
Fachabteilung	5, 23, 60, 70

Forschung.....	37, 74
Fremdbefunde	58
Gefahr für Leben und andere Rechtsgüter	8, 27
HIV	8
Krankenhausträger	11
Krankenhauswanderer.....	9
Krankenkasse	16, 22
Krankenversicherung	29
Landesbeauftragter für den Datenschutz	42, 45
Leistungsabrechnung	17
Leistungserbringer	57
Leistungsträger.....	57
Maßnahmen, technische und organisatorische	4, 11, 12, 31, 37, 54, 69, 79
Medizinischer Dienst der Krankenversicherung (MDK).....	55, 72
Begutachtung und Stellungnahmen	56
Fehlbelegungsprüfung	60
Fremdbefunde	58
Meldepflicht.....	71
Meldepflichten	10
Mikroverfilmung.....	43
Minderjährige.....	8
Notstand, rechtfertigender.....	8
Offenbarungsbefugnis.....	8
Offenbarungspflicht	10
Patientendaten	5, 13, 63
Patienteninformation.....	18
Patientenverfügung	23
Persönlichkeitsrecht	4
Qualitätssicherung.....	30
Recht auf informationelle Selbstbestimmung.....	4, 13, 18, 19, 58
Rechtsform des Krankenhausträgers.....	12
Schadensersatz	13, 17, 29
Schweigepflicht.....	4, 5
Schweigepflichtentbindung.....	7
Seelsorge	17, 29
Statistik	14
Telefax	25
Tod des Betroffenen.....	9
Übermittlungsersuchen	57
Widerruf.....	19
Widerspruch.....	10, 17, 23
Zeugnisverweigerungsrecht	5
Zugangsbeschränkung.....	14
Zugriffsbeschränkung	14
Zweckbindung.....	16, 20, 30, 45, 68