20 Datenschutz als Persönlichkeitsschutz in der Notfallmedizin

Matthias Jaster

Das grundgesetzlich geschützte informationelle Selbstbestimmungsrecht ist ein persönliches Gut sehr hohen Ranges. Die effektive Gewährleistung des Datenschutzes stellt dabei eine grundlegende Verpflichtung und in einer zunehmend digitalisierten Gesellschaft auch tägliche Herausforderung für jede Daten verarbeitende Stelle dar. Auch und gerade die an der Notfallmedizin Beteiligten müssen daher ein gesteigertes Interesse daran haben, die personenbezogenen Daten der Patienten zu schützen und nur dann zu verarbeiten, wenn datenschutzrechtliche Anforderungen berücksichtigt sind. Jeder Fehler kann nicht nur zu aufsichtsbehördlichen Maßnahmen bis hin zu Bußgeldern, sondern auch zu strafrechtlichen Sanktionen gemäß § 203 StGB führen.

20.1 Allgemeines

In der Notfallmedizin geht es wie in kaum einem anderen medizinischen Bereich oft darum, innerhalb möglichst kurzer Zeit Maßnahmen zu ergreifen. Jede noch so kleine zeitliche Verzögerung kann schwere gesundheitliche Schäden hervorrufen oder gar zu einer ernsten Lebensbedrohung für den betroffenen Patienten werden. Die Beschreibung zum Begriff der Notfallmedizin in der (Muster-)Weiterbildungsordnung der Bundesärztekammer verdeutlicht diese lebenswichtige und lebensrettende Funktion:

> *„Die Zusatz-Weiterbildung Notfallmedizin umfasst die Erkennung drohender oder eingetretener Notfallsituationen und die Behandlung von Notfällen sowie die Wiederherstellung und Aufrechterhaltung akut bedrohter Vitalfunktionen."*

Dabei macht Notfallmedizin nicht an den Grenzen einer einzelnen Abteilung Halt. Sie erfordert zum einen die interdisziplinäre Zusammenarbeit verschiedener Fachbereiche zur bestmöglichen Behandlung des Patienten; über diesen innerklinischen Teil hinaus stellt auch der präklinische Rettungsdienst einen wesentlichen Teil der Rettungskette dar.

Der Datenschutz steht oft in dem Ruf, Prozesse kompliziert zu machen; steht da der Datenschutz in einem derart zeitkritischen wie auch lebenswichtigen Arbeitsumfeld nicht eigentlichen den Zielen der Notfallmedizin im Wege? Nein: Der Datenschutz verhindert keine erforderlichen Informationsflüsse. Vielmehr geht es um den Schutz der Persönlichkeit und damit eines Grundrechtes: das **Recht auf informationelle Selbstbestimmung**. Dabei sind die im medizinischen Bereich anfallenden Gesundheitsdaten als besonders schützenswerte Informationen zu qualifizieren. Hier muss darauf geachtet werden, dass die Daten des Patienten nur im Einklang mit datenschutzrechtlichen Anforderungen erhoben, verarbeitet und genutzt werden dürfen. Gerade im medizinischen Leistungsbereich tritt hierneben die berufsrechtliche Verschwiegenheitspflicht, deren Verletzung in § 203 StGB unter Strafe gestellt ist.

Was aber genau beinhaltet das Recht auf informationelle Selbstbestimmung und wie sieht das Nebeneinander von Datenschutz und berufsrechtlicher Verschwiegenheitspflicht aus? Erst mit diesen Kenntnissen ist es möglich, einzelne konkrete Aspekte der gesamten Rettungskette zu betrachten.

20.2 Datenschutzrechtliche Grundlagen

Mit seinem wegweisenden Urteil vom 15.12.1983 – dem Volkszählungsurteil – hat das Bundesverfassungsgericht den Grundstein für den grundgesetzlichen Schutz personenbezogener Daten gelegt. Es entschied im 1. Leitsatz:

> *„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*
>
> *Bundesverfassungsgericht (Urteil vom 15.12.1983, BVerfGE 65, 1 – Volkszählung)*

Mit dieser grundlegenden Entscheidung stehen zwei wesentliche Elemente des Datenschutzes fest: Selbstbestimmung und Grundrechtsschutz. Das Recht eines jeden Einzelnen, selber entscheiden zu können, wer wann welche Informationen über ihn erhalten darf, ist als Bestandteil des grundgesetzlich geschützten allgemeinen Persönlichkeitsrechtes anerkannt. Diese Befugnis, grundsätzlich selber über die Preisgabe der einen selbst betreffenden Informationen zu bestimmen, wird auch bereits durch seinen Namen selbst beschrieben: das Recht auf **informationelle Selbstbestimmung**. Dieses Recht leitet sich aber nicht bloß aus einer einfachgesetzlichen Regelung ab; der Schutz des einzelnen geht vielmehr unmittelbar auf die Verfassung und den in ihr verankerten Grundrechtsschutz zurück. Allerdings gilt auch dieser Grundrechtsschutz nicht uneingeschränkt, wie das Bundesverfassungsgericht in seinem o.g. Urteil weiter im 2. Leitsatz entschied:

> *„Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen*

Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken."

Bundesverfassungsgericht (Urteil vom 15.12.1983, BVerfGE 65, 1 – Volkszählung)

Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten greift somit in dieses Grundrecht auf informationelle Selbstbestimmung ein. Ein solcher Eingriff kann aber gerechtfertigt sein aufgrund einer gesetzlichen Regelung oder durch eine (selbstbestimmte) Einwilligung des Betroffenen, die in der Regel schriftlich erteilt werden muss. Es gilt somit:

Das informationelle Selbstbestimmungsrecht stellt ein grundsätzliches Verbot mit Erlaubnisvorbehalt dar, personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.

20.2.1 Datenschutz und berufsrechtliche Verschwiegenheitspflicht

Einfachgesetzlich finden sich Regelungen zum Datenschutz einerseits in unterschiedlichen spezialgesetzlichen Regelungen (z.B. Krankenhausgesetze und Rettungsdienstgesetze der Länder) und andererseits grundlegend im Bundesdatenschutzgesetz bzw. den Datenschutzgesetzen der Länder; seit dem 24.10.1995 kommt die Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) hinzu. In dieselbe Schutzrichtung führt auch die berufsrechtliche Verschwiegenheitspflicht, wie sie exemplarisch in § 9 der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte niedergeschrieben ist. Berufsrecht und Datenschutzrecht stehen dabei selbständig nebeneinander; die Anforderungen beider Rechtsmaterien müssen beachtet und eingehalten werden.

Sowohl Datenschutz als auch berufsrechtliche Verschwiegenheitsverpflichtung müssen parallel beachtet werden.

20.2.2 Personenbezogene Daten

Zentraler Begriff des Datenschutzes sind die **personenbezogenen Daten**. Im Kern gemeinsam ist allen Definitionen, dass es sich hierbei um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt (vgl. z.B. § 3 Absatz 1 Bundesdatenschutzgesetz). Dabei genießen gerade auch Gesundheitsdaten einen besonderen Schutz, da sie in erheblicher Weise geeignet sind, den Einzelnen z.B. in Anbetracht einer bestimmten Krankheit zu stigmatisieren oder aber auch in ihrer Gesamtheit ein ggf. sogar umfassendes Profil über die körperliche und geistige Verfassung des jeweils betroffenen Patienten darzulegen.

Entscheidend ist hierbei, dass nicht nur diejenigen Informationen den datenschutzrechtlichen Anforderungen unterliegen, die ausdrücklich mit dem Namen des Pa-

tienten verbunden sind; auch Daten, die einer **bestimmbaren** Person zugeordnet werden können, unterliegen dem grundgesetzlichen Schutz. Dabei ist es unerheblich, ob diese Zuordnung z.B. mittels eines Pseudonyms oder anhand der konkretisierenden Inhalte erfolgt (vgl. Artikel 2 Buchstabe a EG-Datenschutzrichtlinie). Ebenfalls irrelevant ist, ob im Falle pseudonymisierter Daten gerade der Empfänger unmittelbar in der Lage ist, das Pseudonym zu entschlüsseln; die EG-Datenschutzrichtlinie stellt insoweit in Erwägungsgrund 26 klar, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, die vernünftigerweise „entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten" eingesetzt werden könnten, um die betreffende Person zu bestimmen. Es geht also zentral um den Personenbezug bzw. die Personenbeziehbarkeit. Im Gegensatz dazu können hinreichend sicher pseudonymisierte Daten ggf. gewährleisten, dass die berufsrechtliche Verschwiegenheit gewahrt ist, weil berufsrechtlich – insbesondere mit Blick auf § 203 StGB – das „Offenbaren des Geheimnisses" im Mittelpunkt steht; entscheidend ist insoweit dann aber, dass der Empfänger den konkreten Patienten nicht ermitteln kann.

> *Personenbezogene Daten sind nicht nur Informationen, die einer bestimmten Person zugeordnet sind, sondern auch solche, die einer bestimmbaren Person zugeordnet werden können.*

20.2.3 Geheimnischarakter

Anders als im Berufsrecht kommt es im Datenschutzrecht grundsätzlich nicht auf den Geheimnischarakter der betreffenden Informationen an. Selbst wenn der Empfänger die Information bereits kennt, die an ihn weitergegeben wird, braucht der Übermittelnde entweder eine gesetzliche Grundlage oder die Einwilligung des Betroffenen, damit er nicht gegen datenschutzrechtliche Normen verstößt; berufsrechtlich könnte es jedoch ggf. wiederum an einer Offenbarung fehlen.

20.2.4 Grad der Sensibilität

Ferner ist zu berücksichtigen, dass jede Einzelangabe über persönliche oder sachliche Verhältnisse unter den Datenschutz fällt, unabhängig von deren Sensibilität. Gerade im medizinischen Bereich müssen sich die Akteure, die tagein tagaus ausschließlich besonders schützenswerte Daten verarbeiten, immer wieder bewusst machen, dass nicht erst die jeweilige medizinische Diagnose den Schutz des informationellen Selbstbestimmungsrechtes genießt. Bereits schon die Tatsache, dass eine bestimmte (oder bestimmbare) Person sich in einem Krankenhaus aufhält, stellt eine solche Einzelangabe dar und unterliegt dem Datenschutzrecht.

20.2.5 Grundsatz der Erforderlichkeit

Ein weiteres datenschutzrechtliches Prinzip ist der Grundsatz der Erforderlichkeit; eine Datenerhebung, -verarbeitung oder -nutzung darf sich – vorbehaltlich weitergehender rechtlicher Befugnisse – grundsätzlich zunächst einmal nur auf die für die

Behandlung **erforderlichen Daten** beziehen. Dieser ebenfalls aus dem Verfassungsrang des informationellen Selbstbestimmungsrechtes hergeleitete Grundsatz der Erforderlichkeit findet sich auch in den Krankenhaus- und Rettungsdienstgesetzen vieler Länder sowie grundlegend in den einschlägigen allgemeinen datenschutzrechtlichen Gesetzen.

> *Auf der Grundlage datenschutzrechtlicher Erlaubnisnormen können nur diejenigen Informationen erhoben, verarbeitet und genutzt werden, die für die Erfüllung der Aufgabe erforderlich sind.*

20.3 Präklinische Notfallmedizin

In der Notfallmedizin ist meistens Eile geboten. In datenschutzrechtlich Hinsicht kommt oftmals hinzu, dass die Betroffenen nicht in der Lage sind, ihre Wünsche zu äußern geschweige denn nach entsprechender Aufklärung eine datenschutzrechtlich wirksame Einwilligung nebst eventuell erforderlicher Schweigepflichtentbindung zu erklären. In erster Linie bedarf es daher gesetzlicher Grundlagen, um einen Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen.

20.3.1 Aufzeichnung des Notrufes

Oftmals wird die Rettungskette mit einem Anruf in der Notrufzentrale in Gang gesetzt. Derjenige, der den Notruf absetzt, ist nachvollziehbarerweise sehr aufgeregt, weil er sich in einer bei weitem nicht alltäglichen Situation wiederfindet und ggf. zusätzlich auch noch selber familiär betroffen ist. Sooft es zuvor in der Theorie auch gelernt sein mag: An einer strukturierten Darstellung des Vorfalles, der Beteiligten und deren Verfassung fehlt es nicht selten. Hier stellt sich die Frage, ob der Anruf aufgezeichnet werden kann, um z.B. bei Unklarheiten im Nachgang die Meldung erneut anhören und prüfen zu können, ob die eingeleiteten Maßnahmen korrekt sind.

Die Aufnahme eines Telefonanrufes stellt einen Eingriff in das informationelle Selbstbestimmungsrecht dar, da die aufgezeichneten Informationen personenbezogene Daten des Anrufers bzw. der zu rettenden Person enthalten. Eine Einwilligung wiederum scheidet aus, da die Einleitung der Rettungsmaßnahmen hierdurch verzögert werden würde. Bei der Suche nach einer entsprechenden gesetzlichen Grundlage, die die Aufzeichnung des Notrufes erlaubt, finden sich in sehr vielen Ländern entsprechende Regelungen in den Rettungsdienstgesetzen oder in den Sicherheits- und Ordnungsgesetzen. Soweit eine solche gesetzliche Regelung nicht existiert, wird zum Teil vorgebracht, dass ein solcher Notruf als öffentlich gesprochenes Wort anzusehen sei und deshalb nicht unter den Schutz des Grundgesetzes bzw. des Strafgesetzbuches falle. Allerdings wird hierbei verkannt, dass auch die Eilbedürftigkeit eines Notrufes nichts daran ändert, dass sich der Anrufer gerade nicht an die Öffentlichkeit wendet, sondern an die zuständige Stelle; insoweit ist ein solcher Notruf auch nicht anders zu bewerten als ein sonstiger Anruf bei einer Behörde.

Der Grund für die Aufzeichnung des Anrufes ist nachvollziehbar und dient ggf. sogar dem Wohlergehen der Betroffenen. Ziel kann es daher nur sein, dass die hierfür er-

forderlichen formellen Grundlagen geschaffen werden und gesetzliche Vorschriften diese Form der Datenverarbeitung legitimieren.

20.3.2 Schutz vor Voyeurismus

Wird der Rettungsdienst zu einem Einsatz im öffentlich zugänglichen Bereich (z.B. zu einem Verkehrsunfall) gerufen, lassen leider Schaulustige nicht allzu lange auf sich warten. Fotografierende oder filmende Passanten sind dabei ebenfalls keine Seltenheit mehr. Abgesehen davon, dass die Rettungsmaßnahmen hierdurch ggf. sogar behindert werden, ist hier auch nach dem Schutz der Daten des Betroffenen zu fragen: Man kann ggf. die betroffene Person sehen und erkennen, die gerade notfallmäßig behandelt wird; das KFZ-Kennzeichen ist schon aufgrund der gesetzlichen Definition in § 45 Satz 2 Straßenverkehrsgesetz als personenbezogenes Datum anzusehen; angesichts der durch den Rettungsdienst ergriffenen Maßnahmen lassen sich Rückschlüsse auf den Gesundheitszustand des Betroffenen ziehen, wenn er z.B. mit einer Schaufeltrage oder einer Vakuummatratze transportiert wird.

Nordrhein-Westfalen hat als erstes Bundesland auf die hiermit in Zusammenhang gebrachten steigenden Unfallzahlen wegen Unachtsamkeit im Straßenverkehr reagiert und mobile Sichtschutzwände angeschafft. Losgelöst von der Frage, ob den Rettungsdienst in Situationen der Notfallrettung überhaupt eine Garantenpflicht auch zum Schutz des Verunfallten in datenschutzrechtlicher Hinsicht trifft und ob hier entsprechende Maßnahmen datenschutzrechtlich gefordert werden müssen, sind Maßnahmen gegen Voyeurismus und zur Unfallvermeidung jedenfalls auch datenschutzfreundlich, da die Sicht auf den Betroffenen und die Möglichkeit der Informationsbeschaffung unterbunden wird. Auf jeden Fall aber muss darauf geachtet werden, dass parallel zur oder im Anschluss an die konkrete Behandlung Schaulustigen keine personenbezogenen Daten des Betroffenen preisgegeben werden, da für eine solche Datenübermittlung regelmäßig eine rechtliche Grundlage fehlen dürfte.

20.3.3 Information über spezifische Keimbelastungen

Ein Notfalleinsatz kann auch in einer Einrichtung, z.B. einem Alten- und Pflegeheim beginnen. Hier stellt sich aus datenschutzrechtlicher Sicht immer wieder die Frage, ob und in welchem Umfang der Rettungsdienst erfahren darf, welche bestehende Infektion bzw. Keimbesiedelung des Patienten besteht. Gerade im Hinblick auf das im Infektionsschutzgesetz niedergelegte Ziel der Verhütung und Bekämpfung von nosokomialen Infektionen und Krankheitserregern mit Resistenzen (vgl. § 23 Infektionsschutzgesetz) stellt dies ein nachvollziehbares Informationsbedürfnis dar. Bei der Vielzahl unterschiedlicher Keime treten zunehmend auch wirtschaftliche Gesichtspunkte in den Vordergrund: Ausgehend von der Situation, dass dem Rettungsdienst ein unspezifischer Hinweis auf eine bestehende Keimbelastung gegeben wurde, wird nunmehr zunehmend dargestellt, die Information über den konkreten Keim sei wesentlich, da sich die Desinfektionsmaßnahmen und -zeiten je nach Keim unterscheiden, der Rettungswagen also ggf. wieder früher einsatzbereit ist.

Allerdings muss auch hierbei berücksichtigt werden, dass es wiederum um personenbezogene Daten geht. Dabei handelt es sich keineswegs **nur** um eine Diagnose. Gerade eine solche Diagnose stellt – abgesehen von dem grundlegenden erhöhten Schutz-

bedarf von Gesundheitsdaten – eine Information höchster Sensibilität dar. Rechtliche Grundlagen für einen Informationsaustausch gibt es in vielen unterschiedlichen Zusammenhängen. Hier kommen insbesondere erneut die Rettungsdienstgesetze der Länder oder auf § 23 Infektionsschutzgesetz beruhende Verordnungen in Betracht. Auch bei einem derartigen institutionsübergreifenden Informationsaustausch greift aber der Grundsatz der Erforderlichkeit. Nur diejenigen Informationen, die zur Verhütung und Bekämpfung erforderlich sind, können unter solche Erlaubnistatbestände fallen. Dies kann z.B. danach differenzieren, welche Körperteile mit Keimen besiedelt sind. So können bei einer Besiedelung von Nasen- und Rachenraum andere Schutzmaßnahmen erforderlich werden als in anderen Fällen. Insgesamt muss hier genau darauf geachtet werden, was die jeweiligen gesetzlichen Vorschriften erlauben. Insbesondere Alten- und Pflegeheime werden hiervon bisher ggf. nicht umfasst.

20.4 Innerklinische Notfallmedizin

Innerhalb eines Krankenhauses kommen Notfallsituationen in verschiedensten Ausgestaltungen vor. Allen gemeinsam ist auch hier die zeitliche Enge, in der Maßnahmen eingeleitet werden müssen. Je größer und detaillierter hierbei die Informationsgrundlage ist, desto höher sind die Chancen für die Betroffenen, unbeschadet die Notfallsituation zu überstehen. Bei allem Verständnis für Befürworter einer insoweit möglichst offenen und damit einfachen Informationskultur innerhalb eines Hauses sind zum Schutz der grundgesetzlichen Rechte eines jeden Patienten dennoch datenschutzrechtliche Anforderungen zu berücksichtigen; dies geht aber auch ohne Verhinderung der erforderlichen Informationsflüsse und ohne Beschränkung der medizinischen Maßnahmen. Grundsätzlich gilt auch hier, dass eine Datenerhebung, -verarbeitung oder -nutzung nur zulässig ist, wenn entweder eine gesetzliche Vorschrift dies erlaubt oder der Betroffene seine Einwilligung erteilt hat; speziell für Notfälle scheidet jedoch oftmals die Möglichkeit, eine Einwilligung erklären zu können, aus.

20.4.1 Notfall auf dem Krankenhausgelände

Gerade in einem Krankenhaus halten sich Menschen auf, die in ihrer gesundheitlichen Verfassung eingeschränkt sind. Hier ist nicht ausgeschlossen, dass ein Patient außerhalb seiner Station in eine akute Notfallsituation gerät. Um hier richtige und sachgerechte Hilfe zu leisten, könnte ein Zugriff auf elektronisch gespeicherte Daten dieses Patienten sehr hilfreich sein. Hieraus könnten sich immerhin nützliche Erkenntnisse z.B. über bestimmte Erkrankungen, Krankheitskonstellationen, erforderliche Medikamente oder Allergien usw. ergeben, deren Unkenntnis für den Patienten zu gefährlichen Folgen führen könnte.

Allerdings greift der Grundsatz der Erforderlichkeit auch innerhalb eines Krankenhauses. Das bedeutet, dass der jeweilige Mitarbeiter bzw. eine bestimmte Rolle von Mitarbeitern auch nur Zugriff auf diejenigen Daten haben darf, die er für die Erfüllung seiner Aufgaben benötigt. So dürften sich grundsätzlich die Zugriffsberechtigungen von ärztlichem und nicht-ärztlichem Personal unterscheiden; auch die Zugriffsmöglichkeiten unterschiedlicher Abteilungen bzw. Kliniken müssten differenziert vergeben sein. Im Hinblick auf Krankenhausinformationssysteme haben die

Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zur Nutzung der elektronischen Patientenakte herausgegeben, der sowohl die rechtlichen Grundlagen als auch die technischen und organisatorischen Maßnahmen entnommen werden können, die zur Gewährleistung des Datenschutzes zu ergreifen sind.

Trotz eines aus datenschutzrechtlicher Sicht erforderlichen Zugriffsberechtigungskonzeptes darf in Notfallsituationen der Zugang zu erforderlichen Informationen auch für einen an sich nicht zuständigen Arzt nicht verschlossen sein. Hier sollte technisch vorgesehen werden, dass im Rahmen eines Notzugriffes z.B. ausschließlich für das ärztliche Personal der Zugriff auf alle Patientendaten ermöglicht wird; entscheidend für die Durchsetzung datenschutzrechtlicher Anforderungen ist dann aber die Kontrollmöglichkeit solcher Zugriffe. Dies setzt z.B. voraus, dass die Zugriff nehmenden Ärzte einen kurzen Grund für diesen Zugriff hinterlegen müssen, dass sie auf die Tatsache des Notzugriffes und die diesbezügliche Protokollierung hingewiesen werden und dass vor allem diese Protokollierung der Notzugriffe anschließend in regelmäßigen Abständen ausgewertet wird. Sollte es hier zu Unstimmigkeiten kommen, müssen diese weiter aufgeklärt werden.

20.4.2 OP und Notfallambulanz

Der OP bzw. die Notfallambulanz sind die Kernbereiche innerklinischer Notfallmedizin. Die eingangs bereits dargestellte interdisziplinäre Zusammenarbeit verschiedener Fachbereiche einerseits und die klinik- bzw. abteilungsübergreifende Zuständigkeit andererseits bedeuten, dass ein der beruflichen Rolle oder dem Fachbereich entsprechendes Zugriffsberechtigungskonzept zu Informationsdifferenzen führen würde, wohingegen eine einheitliche Datengrundlage und ein einheitliches Vorgehen aller an einer Operation Beteiligten notwendig für das Gelingen der Behandlung ist.

In Teil I Ziffer 19 der Orientierungshilfe Krankenhausinformationssysteme der Datenschutzbeauftragten des Bundes und der Länder (März 2014) wurde auch diese besondere Situation berücksichtigt:

> *„Beschäftigte des Krankenhauses mit fachrichtungsübergreifender Funktion (z.B. Anästhesie, … OP-Personal …) sollten den Daten-Zugriff entweder durch individuelle Zuweisung oder mit dem/durch den Patientenkontakt erhalten. Die Zugriffsbefugnisse haben sich an der Erforderlichkeit für die jeweilige Aufgabenerfüllung zu orientieren.“*

Durch eine derart ausgestaltete Technik, fachrichtungsübergreifenden Abteilungen gezielt den Zugriff auf die Patientendaten des jeweils Betroffenen zu ermöglichen, werden die medizinischen Maßnahmen einerseits nicht behindert und dem Datenschutz andererseits dennoch ausreichend Rechnung getragen. Berücksichtigt werden muss hier selbstverständlich aber auch der Grundsatz der Erforderlichkeit. Nicht datenschutzrechtlichen Anforderungen entspricht es daher, wenn OP-Mitarbeiter uneingeschränkt Zugriff auf die Daten sämtlicher Patienten des Krankenhauses haben.

20.4.3 Prominente Patienten

Immer wieder befinden sich auch Prominente zur ärztlichen Behandlung in einem Krankenhaus. Das mediale Interesse an Behandlungsmaßnahmen, Hintergründen und Informationen ist entsprechend groß. Trotzdem unterliegt ein Krankenhaus als

Daten verarbeitende Stelle auch bei solchen Patienten datenschutzrechtlichen Anforderungen; die Tatsache, dass die Gesundheitsinformationen dieses Patient als Prominenter von journalistischem Interesse sein mögen, rechtfertigt es nicht, ohne Rücksicht auf das informationelle Selbstbestimmungsrecht dieses Patienten Rede und Antwort zu stehen. Mangels einer entsprechenden Rechtsgrundlage kommt hier eine Preisgabe personenbezogener Patientendaten über den Prominenten nur in Betracht, wenn er hierzu seine Einwilligung erteilt hat.

Ein weiterer Aspekt im Zusammenhang mit prominenten Patienten ist das hausinterne Interesse an der Krankengeschichte. Entgegen einem dem Erforderlichkeitsgrundsatz entsprechenden Zugriffsberechtigungskonzept haben ggf. auch Mitarbeiter, die nicht an der Patientenbehandlung beteiligt sind, ein allein sensationsbedingtes Bedürfnis, Zugriff auf diese Patientendaten nehmen zu wollen. Zum einen sollte im Falle einer elektronischen Patientenakte die Protokollierung der Zugriffe auf die Daten solcher Patienten mit besonderem Augenmerk ausgewertet werden und zum anderen kommt auch eine Aufnahme unter fiktivem Namen in Betracht – vgl. Teil I Ziffern 41f. der Orientierungshilfe Krankenhausinformationssysteme der Datenschutzbeauftragten des Bundes und der Länder (März 2014). Auf diese technische Weise kann die auch für den Datenschutz letztlich verantwortliche Krankenhausleitung den Missbrauch solcher Patientendaten einzudämmen versuchen.

Literatur

Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2014) Orientierungshilfe Krankenhausinformationssysteme der Datenschutzbeauftragten des Bundes und der Länder. Stand: März 2014. URL: https://www.datenschutz-hamburg.de/uploads/media/Orientierungshilfe_Krankenhausinformationssysteme_2.Fassung.pdf

Bundesverfassungsgericht (Urteil vom 15.12.1983, BVerfGE 65, 1 – Volkszählung) 1 BvR 209, 269, 362, 420, 440, 484/83

Matthias Jaster

Studium der Rechtswissenschaften an der Rheinischen Friedrich-Wilhelms-Universität Bonn. Von 2005 bis 2007 Tätigkeit als Rechtsanwalt und Leitung der Dezernate für Medizinrecht und Verwaltungsrecht in einer alteingesessenen Kanzlei; Absolvierung der Fachanwaltslehrgänge Medizinrecht und Verwaltungsrecht. Mitglied des Deutschen Anwaltvereins (DAV) und der Arbeitsgemeinschaft Verwaltungsrecht des DAV. Ab 2007 Tätigkeit in einer norddeutschen Klinikgruppe u.a. als betrieblicher Datenschutzbeauftragter. Seit 2013 juristischer Fachreferent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit für die Bereiche: Gesundheitswesen und medizinische Forschung, Sozialwesen, Schule und Bildungswesen sowie Grundsatzfragen des Hamburgischen Datenschutzgesetzes; derzeit kommissarischer Leiter des Referates „Sicherheit, Demokratie und Daseinsvorsorge“. Mitglied des Arbeitskreises Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Autor und Referent zu datenschutzrechtlichen Themen im Gesundheitswesen und Sozialwesen.