Risikomanagement- und Fehlermeldesysteme nach dem Patientenrechtegesetz: datenschutzrechtliche Grenzen?

Benedikt Buchner

I. Risikomanagement- und Fehlermeldesysteme – Grundlagen

1. Rechtliche Verortung

Risikomanagement- und Fehlermeldesysteme sind Instrumente der Qualitätssicherung nach §§ 135 ff. SGB V. § 135a Abs. 1 S. 1 SGB V verpflichtet die Leistungserbringer „zur Sicherung und Weiterentwicklung der Qualität der von ihnen erbrachten Leistungen" und § 135 a Abs. 2 Nr. 2 SGB V verpflichtet konkret zur Einführung und Weiterentwicklung eines einrichtungsinternen Qualitätsmanagements. Zu diesem Qualitätsmanagement wiederum zählen insbesondere auch die sog. Risikomanagementsysteme: So soll nach der Qualitätsmanagementvereinbarung für Krankenhäuser das Prinzip des umfassenden Qualitätsmanagements auch das Element „Fehlervermeidung und Umgang mit Fehlern" beinhalten.[1] Ähnlich ist in der Qualitätsmanagement-Richtlinie vertragsärztliche Versorgung davon die Rede, dass ein Instrument des Qualitätsmanagements das „Erkennen und Nutzen von Fehlern und Beinahe-Fehlern zur Einleitung von Verbesserungsprozessen" sein soll.[2]

2. Begrifflichkeiten

Risikomanagementsysteme können allgemein definiert werden als Systeme, die darauf angelegt sind, Risiken zu erkennen und zu analysieren, um dann aufbauend auf diesem Risikowissen Strategien zu entwickeln, wie für die Zu-

---

1 Vereinbarung des Gemeinsamen Bundesausschusses gemäß § 137 Abs. 1 Satz 3 Nr. 1 SGB V über die grundsätzlichen Anforderungen an ein einrichtungsinternes Qualitätsmanagement für nach § 108 SGB V zugelassene Krankenhäuser vom 21.6.2005. Präambel.

2 Richtlinie des Gemeinsamen Bundesausschusses über grundsätzliche Anforderungen an ein einrichtungsinternes Qualitätsmanagement für die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Psychotherapeuten und medizinischen Versorgungszentren vom 18.10.2005, § 4.

kunft solcherlei Risiken ausgeschaltet oder zumindest minimiert werden können.[3] Zentrales Instrument, um ein solches Risikowissen zu schaffen, sind die sog. Fehlermeldesysteme, d. h. Systeme, die es ermöglichen, innerhalb eines bestimmten organisatorischen Rahmens Fehler zu melden. Fehler werden dabei definiert als Vorkommnisse, die planwidrig, mit falschem Plan oder auch ganz ohne Plan abgelaufen sind, wobei es in diesem Zusammenhang zunächst einmal keine Rolle spielt, ob ein solcher Fehler auch zu einem Schaden geführt hat oder möglicherweise nur hätte führen können (sog. „Beinaheschaden"/„near miss").[4] Neben Fehlern mit Schadensfolge können entsprechend auch Beinaheschäden und so genannte „kritische Ereignissen" („critical incidents") berichtet werden, weshalb sich für Fehlermeldesysteme auch die Bezeichnung „CIRS" – „Critical Incident Reporting System" etabliert hat.[5] Beide Bezeichnungen werden regelmäßig und auch in den folgenden Ausführungen synonym verwendet.

3. Grundkonzeption

Die Idee, die hinter diesen Fehlermeldesystemen steht, ist ebenso einfach wie einleuchtend: Je mehr Fehler kommuniziert werden, desto mehr Wissen um mögliche Risiken sammeln wir und desto größer ist auch die Chance, auf solche Risiken zu reagieren und ihnen künftig vorzubeugen. Die Idee ist nicht neu, sondern schon seit langem aus einem anderen „Hochsicherheitsbereich", dem Bereich der Luftfahrt, bekannt und von dort für den Bereich der Medizin übernommen worden.[6]

---

3 Vgl. *Wiederkehr/Züger*, Risikomanagement im Unternehmen, 2010, S. 18; *Pampel/Glage*, in: Hauschka (Hrsg.), Corporate Compliance, 2. Aufl. 2010, § 5 Rn. 21; *Grützner/Jakob*, Compliance von A-Z, 2010, Stichwort „Risikomanagementsystem (RMS)".

4 *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf/Thomeczek*, CIRS – Gemeinsames Lernen durch Berichts- und Lernsysteme, in: Herbig/Poppelreuter/Thomann (Hrsg.), Qualitätsmanagement im Gesundheitswesen, 31. Aktualisierung 2013, S. 2; *Rohe/Sanguino Heinrich/Weidringer/Thomeczek*, Critical-Incident-Reporting-System (CIRS), Notfall Rettungsmedizin 2012, 25 (26).

5 Erfasst werden mithin alle Ereignisse, die subjektiv als sicherheitsrelevant aufgefasst werden, vgl. *Thüß*, Rechtsfragen des Critical Incident Reportings in der Medizin, 2012, S. 8. Zu den Begrifflichkeiten vgl. *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf/Thomeczek* (Fn. 4), S. 2.

6 Dazu *Knoch*, Aus der Luftfahrt lernen – Patientensicherheit durch gesetzlich verpflichtende OP-Checklisten, RDG 2012, 94; *Gunkel/Rohe/Sanguino Heinrich/Weid-*

Betrieben werden können solcherlei Fehlermeldesysteme in zwei Varianten:

- als *einrichtungsinterne* Fehlermeldesysteme, die lediglich innerhalb einer Praxis, Abteilung oder Klinik betrieben und nur von den dort tätigen Personen genutzt werden
- oder auch als *externe* Systeme, die einrichtungsübergreifend betrieben, also von einer Vielzahl von Gesundheitseinrichtungen genutzt werden und damit auch einem entsprechend weiten, teils auch unbegrenzten Nutzerkreis offenstehen.[7]

Eines der bekanntesten Beispiele für letztere externe Fehlermeldesysteme in Deutschland ist CIRSmedical.de, das Fehlermeldesystem der deutschen Ärzteschaft. CIRSmedical.de richtet sich an alle Mitarbeiter des Gesundheitswesens: Alle in irgendeiner Form sicherheitsrelevanten Ereignisse können über ein Berichtsformular online gemeldet werden, diese Meldungen werden dann von Mitarbeitern des ÄZQ gelesen und entsprechend aufbereitet, um auf CIRS Medical.de veröffentlicht zu werden.[8]

4. Patientenrechtegesetz

Das Patientenrechtegesetz hat sich u. a. zum Ziel gesetzt, eine solche Kultur der Fehlervermeidung mittels Fehlermeldesystemen nochmals zu fördern. Krankenhäuser und vertragsärztliche Praxen sollen, so die Begründung des Gesetzentwurfs, „zukünftig verstärkt Maßnahmen zur Verbesserung der Patientensicherheit und Fehlervermeidung durchführen."[9]

Konkret soll dies dadurch erreicht werden, dass

- der Gemeinsame Bundesausschuss verpflichtet wird, in seinen Richtlinien zum Qualitätsmanagement Mindeststandards für Fehlermeldesysteme festzulegen (§ 137 Abs. 1 d S. 1 SGB V),

---

ringer/Thomeczek (Fn. 4), 26; vgl. auch *Lauterbach*, Gesundheitsökonomie, Management und Evidence-based Medicine, 3. Aufl. 2009, S. 379; *Thüß* (Fn. 5), S. 4.

7 Vgl. *Rohe/Heinrich/Thomeczek*, Netzwerk für Patientensicherheit, DÄBl. 2011, 92 (93); *Thüß* (Fn. 5), S. 6; *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf/Thomeczek* (Fn. 4), S. 5 f.

8 Siehe im Einzelnen http://patientensicherheit-online.de/cirs, zuletzt abgerufen am: 27.11.2013.

9 Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten, BTDrs. 17/10488, 12.

- sich Interessierte über die Umsetzung dieser Maßnahmen zukünftig auch in den Qualitätsberichten der Krankenhäuser informieren können (§ 137 Abs. 1 d S. 2 SGB V),
- für Krankenhäuser im Krankenhausfinanzierungsgesetz ein finanzieller Anreiz gesetzt wird, sich künftig an einrichtungsübergreifenden Fehlermeldesystemen zu beteiligen (§ 137 Abs. 1 d S. 3 SGB V).

II. Datenschutzrechtliche Grenzen der Implementierung von Fehlermeldesystemen

Es stellt sich die Frage, welche rechtlichen, insbesondere datenschutzrechtlichen Hürden der praktischen Umsetzung solcher Fehlermeldesysteme entgegenstehen. Der Begriff der „datenschutzrechtlichen Hürden" ist in diesem Zusammenhang weit zu verstehen und bezieht sich nicht nur auf den Datenschutz, wie er im Bundes- und den Landesdatenschutzgesetzen normiert ist, sondern auch auf den spezifischen „Patientendatenschutz", wie er in § 203 StGB seine Ausprägung gefunden hat.

1. Der Ausgangskonflikt

Der Ausgangskonflikt lässt sich zunächst relativ einfach skizzieren: Es geht um „möglichst viel erzählen" versus „möglichst wenig erzählen":

Auf der einen Seite stehen die Fehlermeldesysteme, deren Effektivität gerade davon abhängt, dass möglichst viel und möglichst genau erzählt wird und dies eben gerade auch von Personen – vom Patienten, seiner Krankheitsgeschichte und Behandlung, aber auch vom Behandelnden, dessen Maßnahmen und insbesondere auch dessen Fehlern.

Auf der anderen Seite steht der Datenschutz, dessen Erfolg in erster Linie davon lebt, dass möglichst wenig erzählt wird und möglichst wenig personenbezogene Daten kommuniziert werden. Maxime des Datenschutzrechts ist die Datensparsamkeit, wie sie in § 3a S. 1 BDSG als Leitidee auch explizit so normiert ist:

> „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen."

2. Anonymisierung als Lösung?

Allerdings gibt es auch einen Ausweg aus diesem Zielkonflikt zwischen „möglichst viel" und „möglichst wenig erzählen" und zwar dergestalt, dass alle in Fehlermeldesysteme eingemeldeten Daten umfassend anonymisiert werden, also ihr Bezug auf eine individualisierbare Person aufgehoben wird.[10]

Sämtliche Fehlermeldesysteme sind so konzipiert, dass zum einen der Meldevorgang als solcher anonym erfolgt und zum anderen auch die eigentlichen Fehlerberichte in einer Form abstrahiert werden, die keine Rückschlüsse auf individualisierbare Personen, weder die betroffenen Patienten noch die behandelnden Personen bzw. sonstige Beteiligte, erlaubt. Beispielhaft sei hier auf die Handlungsanleitung des ÄZQ für CIRS-Systeme verwiesen.[11] Danach sind in Fehlermeldungen alle Angaben, die Rückschlüsse auf eine Identität erlauben, zu löschen bzw. zu verändern, insbesondere im Hinblick auf

- Namen und Adressen
- Alter und Geschlecht
- Datumsangaben
- Stations-/Abteilungs-, Fach-, Hierarchiebezeichnungen
- die spezifische Beschreibung des Patienten z. B. durch mehrere Krankheiten, seltene Krankheiten usw.[12]

Fehlermeldesysteme nehmen mit einer dergestalt vorgenommenen, umfassenden Anonymisierung zunächst einmal eben das auf, was auch das Datenschutzrecht als Mittel erster Wahl für Datensparsamkeit vorsieht. Auch nach § 3a S. 2 BDSG soll Datensparsamkeit insbesondere durch das Instrument der Anonymisierung (und Pseudonymisierung) erreicht werden:

> „Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."

3. Das Problem der (rechts-)sicheren Anonymisierung

In der Praxis lässt sich dieser Gleichklang zwischen Risikomanagement und Datenschutz allerdings nicht ohne Weiteres herstellen, tatsächlich ist die Un-

---

10 Vgl. dazu auch die Legaldefinition des § 3 Abs. 6 BDSG.

11 *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf Thomeczek* (Fn. 4), S. 13 ff.

12 *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf Thomeczek* (Fn. 4), S. 18.

sicherheit darüber, ob Fehlerberichte auch wirklich ausreichend anonym sind und anonym behandelt werden, eine der zentralen Hürden für die erfolgreiche Umsetzung von Fehlermeldesystemen.

Exemplarisch sei hier auf folgende Fehlermeldung aus CIRSmedical.de verwiesen – keine typische Fehlermeldung, die über ein medizinisches Ereignis berichtet, sondern vielmehr eine Meldung, die eine Art von Systemfehler offenbart, der jedem CIRS innewohnt:

Fall-Nr. 37477 Drucken Kommentieren Zurück
Fall

Titel:	**CIRS-Nutzung**
Zuständiges Fachgebiet:	
Altersgruppe des Patienten:	
Geschlecht des Patienten:	
Wo ist das Ereignis passiert ?	Krankenhaus
Welche Versorgungsart:	
In welchem Kontext fand das Ereignis statt ?	
Was ist passiert ?	Bei einem Gespräch unter Pflegenden über Missstände im Krankenhaus wurde auch das Thema CIRS-Meldungen angesprochen. Es stellte sich heraus, dass kaum eine(r) der KollegInnen von der Möglichkeit Gebrauch macht, kritische Situationen an das CIRS zu berichten, obwohl sehr viele Fehler, gefährliche Situationen und Missstände im Krankenhausbetrieb wahrgenommen werden.
Was war das Ergebnis ?	Das CIRS bildet wahrscheinlich nicht das tatsächliche Ausmaß der gefährlichen Pflege in den Krankenhäusern ab. Kritische Situationen werden als Ausnahmefälle wahrgenomen, obwohl sie regelhaft auftreten. Nicht gemeldete Fehler können nicht ausgewertet, Verbesserungsmaßnahmen nicht eingeleitet werden
Wo sehen Sie Gründe für dieses Ereignis und wie hätte es vermieden werden können ?	Die Gründe die dafür genannt wurden, dass nicht berichtet wird waren: - Angst, dass Anonymität nicht wirklich gewährleistet ist. Dass IP-Adressen von Berichtenden gespeichert werden oder man aus der Beschreibung des Falles doch Rückschlüsse auf den Berichtenden ziehen kann. Man weiß nicht, wer alles Zugriff auf die nicht öffentlichen CIRS-Daten hat.

Abbildung 1: CIRS Fehlermeldung, Fall-Nr.: 37477[13]

Gemeldet wird hier der „Fehler", dass kaum jemand von der Möglichkeit Gebrauch macht, kritische Situationen an Fehlermeldesysteme zu berichten, obwohl es offensichtlich viele Vorfälle zu berichten gäbe. Interessant ist dann vor allem der allererste Grund, der für diese Zurückhaltung angeführt wird, nämlich die „Angst, dass Anonymität nicht wirklich gewährleistet ist. Dass IP-Adressen von Berichtenden gespeichert werden oder man aus der Beschreibung des Falles doch Rückschlüsse auf den Berichtenden ziehen kann. Man weiß nicht, wer alles Zugriff auf die nicht-öffentlichen CIRS-Daten hat."

13 Fehlerbericht abrufbar unter: https://www.cirsmedical.de, Fall-Nr.: 37477, zuletzt abgerufen am 27.11.2013.

Diese Unsicherheit hinsichtlich einer sicheren Anonymisierung beschränkt sich keineswegs auf die Anwenderebene, sondern setzt sich auf der Rechtsebene bei der Frage fort, wann von einer rechtssicheren Anonymisierung auszugehen ist. Seit jeher ist es im Datenschutzrecht ein ungelöster Konflikt, wann tatsächlich von anonymisierten Daten ausgegangen werden kann.

Gemäß § 3 Abs. 6 BDSG soll eine Anonymisierung dann anzunehmen sein, wenn Daten derart verändert worden sind,

> „dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten, Arbeitskraft einer bestimmten oder bestimmbaren persönlichen Person zugeordnet werden können."

Problematisch ist diese Frage einer ausreichenden Anonymisierung vor allem, wenn man die absolute Sichtweise der Datenschutzbehörden zugrundelegt, nach der sich Daten einer bestimmten Person immer schon dann zuordnen lassen, wenn „irgendjemand" eine Information, eine Geschichte oder wie hier eine Fehlermeldung einer bestimmten Person zuordnen kann.[14]

Aber selbst wenn man den Personenbezug nicht in einem absoluten Sinne, sondern nur relativ, also mit Blick auf den Kenntnisstand der jeweiligen Empfänger solcher Fehlermeldungen beurteilt, ist eine rechtssichere Anonymisierung zuweilen nur schwer zu gewährleisten.[15] Nimmt man das Beispiel der einrichtungsinternen Fehlermeldesysteme, ist dort zwar einerseits der Empfängerkreis der Berichte überschaubar, andererseits werden aber gerade bei solchen Systemen viele potentielle Leser als „Insider" über ein Zusatzwissen verfügen, das es für sie dann doch wieder möglich macht, einen an sich anonymisierten Fehlerbericht im Ergebnis einer bestimmten Person zuzuordnen und damit die Anonymität des Fehlerberichts aufzuheben.

Tatsächlich ist daher die datenschutzrechtliche Hürde der Anonymisierung allenfalls dann überwindbar, wenn zumindest ein gewisses stets vorhandenes Restrisiko einer Individualisierung bei Fehlermeldesystemen als systemimmanent akzeptiert wird und die Anforderungen an eine Anonymisierung nicht zu sehr überspannt werden. Dies ist im Übrigen eine Forderung, die ebenso für andere datenschutzrechtlich relevante Bereiche gilt, insbesondere wenn es um Forschung mit personenbezogenen bzw. anonymisierten Daten geht. Auch hier stellt sich oftmals das Problem, dass sich eine 100%ige Anonymisierung niemals sicher gewährleisten lässt.

---

14 Vgl. *Pahlen-Brandt*, Datenschutz braucht scharfe Instrumente – Beitrag zur Diskussion um personenbezogene Daten, DuD 2008, 34; *Weichert*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 3 Rn. 47.

15 Zu dieser relativen Theorie siehe etwa *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rn. 10.

4. Datenverarbeitung durch CIRS-Betreiber

Leichter überwinden lässt sich demgegenüber eine zweite datenschutzrechtliche Hürde, die der Zulässigkeit einer Datenverarbeitung durch die CIRS-Betreiber selbst. Auch wenn es grundsätzlich Vorgabe aller CIRS-Systeme ist, dass bereits sämtliche Einmeldungen von vornherein keine personenbeziehbaren Informationen enthalten sollen, ist davon auszugehen, dass sich in einer Vielzahl von Meldungen gleichwohl noch solcherlei personenbeziehbare Angaben finden lassen. Eben deshalb sind Fehlermeldesysteme so konzipiert, dass für die letztendliche Anonymisierung von Fehlerberichten vor deren Weitergabe und Veröffentlichung stets die Systembetreiber verantwortlich sind. Diese nehmen die Berichte entgegen, überprüfen sie und unterziehen sie soweit noch erforderlich einer Anonymisierung. Jedenfalls diejenigen, die als verantwortliche Personen innerhalb eines CIRS die Fehlermeldung entgegennehmen, erhalten damit also auch immer wieder personenbezogene Daten – im datenschutzrechtlichen Sinne werden personenbezogene Daten an diese Personen übermittelt, von ihnen erhoben, gespeichert und verändert.

All diese Datenverarbeitungsprozesse sind datenschutzrechtlich erlaubnispflichtig. Allein der Umstand, dass die bearbeitenden Personen regelmäßig als „Vertrauenspersonen" bezeichnet werden, auf das Datengeheimnis verpflichtet werden und, soweit sie Ärzte sind, auch unter die ärztliche Schweigepflicht fallen, ändert nichts daran, dass jeder Datenverarbeitungsprozess datenschutzrechtlich eines spezifischen Erlaubnistatbestands bedarf.[16] Wie „vertrauenswürdig" ein Datenempfänger ist, spielt aus datenschutzrechtlicher Perspektive zunächst einmal keine Rolle, ebenso wenig wie es auch bei § 203 StGB für die Befugnis einer Datenpreisgabe relevant ist.[17]

Allerdings findet sich im BDSG mit § 28 Abs. 7 BDSG ohnehin ein gesetzlicher Erlaubnistatbestand, der die Übermittlung personenbezogener Daten an die Systembetreiber zulässt.[18] § 28 Abs. 7 BDSG bezieht sich gerade auf die

16 Nach § 4 Abs. 1 BDSG gilt ein Verbotsprinzip mit Erlaubnisvorbehalt; danach dürfen personenbezogene Daten nur verarbeitet werden, wenn entweder der Betroffene in die Verarbeitung eingewilligt hat oder ein gesetzlicher Erlaubnistatbestand besteht.

17 Siehe für § 203 StGB: BGH NJW 1991, 2955 (2957); BGH NJW 1992, 737 (739); *Gramberg-Danielsen/Kern*, Die Schweigepflicht des Arztes gegenüber privaten Verrechnungsstellen, NJW 1998, 2708 (2709) m.w.N.; *Huster/Rux*, Kindeswohl und Datenschutz – Rechtslage und Reformüberlegungen am Beispiel von RISKID, NWVBl. 2008, 455 m.w.N.; *Lilie*, Datenfernwartung – Ein Beitrag zur Reform des § 203 StGB, in: Dannecker/Langer/Ranft/Schmitz/Brammsen (Hrsg.), FS Otto, S. 679 m.w.N.

18 Das BDSG ist in seinem Anwendungsbereich jedenfalls für Arztpraxen und Privatkrankenhäuser eröffnet, da es sich bei ihnen um nicht-öffentliche Stellen im Sinne des § 1 Abs. 2 Nr. 3 BDSG handelt. Soweit es um die Datenverarbeitung in öffentlichen

sog. besonderen Arten personenbezogener Daten und damit Gesundheitsdaten und lässt eine Datenverarbeitung u. a. zum Zweck der Gesundheitsvorsorge jedenfalls dann zu, wenn zwei Voraussetzungen erfüllt sind:

1. die Datenverarbeitung bewegt sich im Rahmen des Erforderlichen und
2. die verantwortlichen Personen unterliegen einer entsprechenden Geheimhaltungspflicht.

5. Verwendungsverbot

Abschließend sei noch auf einen weiteren Aspekt eingegangen, der bei Fehlermeldesystemen auch von datenschutzrechtlicher Relevanz ist – zumindest im weiteren Sinne, soweit man auch vom Datenschutz als „Täterschutz" sprechen möchte.

Die Maxime der Anonymisierung von Daten im Rahmen von CIRS gilt gerade nicht nur mit Blick auf die Patienten, über deren Behandlung berichtet wird, sondern auch mit Blick auf diejenigen, die möglicherweise Fehler gemacht haben. Aus deren Perspektive wiederum birgt der Umstand, dass eine vollständige Anonymisierung im Rahmen von CIRS nicht immer sicher gewährleistet ist, nicht nur das Problem fehlender Vertraulichkeit, sondern damit einhergehend auch oder sogar in erster Linie das Risiko einer möglichen Haftung und strafrechtlichen Verantwortlichkeit.

Die Gefahr, dass der Erfolg von Fehlermeldesystemen daran scheitert, dass aus Angst vor solchen haftungs- und strafrechtlichen Konsequenzen nichts bzw. nichts Erhebliches berichtet wird, hat auch der Gesetzgeber gesehen und daher durch das Patientenrechtegesetz mit § 135a Abs. 3 SBG V eine Art Beweisverwertungsverbot eingefügt, welches besagt, dass Berichte aus Risikomanagement- und Fehlermeldesystemen im Rechtsverkehr „nicht zum Nachteil des Meldenden" verwendet werden dürfen.

Krankenhäusern geht, ist zu differenzieren: Stehen diese in Trägerschaft des Bundes, gilt auch für sie das BDSG, § 1 Abs. 2 Nr. 1 BDSG. Für Krankenhäuser in Trägerschaft der Länder sowie der Kommunen sind vorrangig die datenschutzrechtlichen Regelungen des Landesrechts zu beachten, § 1 Abs. 2 Nr. 2 BDSG. Dabei ist zunächst zu überprüfen, ob die spezifischen Landeskrankenhausgesetze Erlaubnistatbestände für eine Datenverarbeitung enthalten. Falls ein solches fehlt oder aber keine Regelungen zum Datenschutz enthält, ist auf das jeweilige Landesdatenschutzgesetz zurückzugreifen. Dieses wiederum tritt seinen vorrangigen Geltungsanspruch teilweise wieder an das BDSG ab, da es sich bei Krankenhäusern um öffentliche Stellen handelt, die am Wettbewerb teilnehmen.

Selbst wenn also im Rahmen von Fehlermeldesystemen trotz an sich erfolgter Anonymisierung haftungsrelevantes und vor allem personenbeziehbares Wissen vorhanden ist, darf dieses Wissen nicht verwendet werden – zumindest nicht, wie es § 135a Abs. 3 SGB V vorsieht, zulasten des Meldenden. Damit ist aber zugleich auch schon das wesentliche Defizit dieses Verwendungsverbots angesprochen: Es ist eben auch nur dieser „Meldende" selbst, der keine Nachteile mehr zu befürchten hat, wohl aber müssen Dritte, über deren Fehler möglicherweise auch oder sogar ausschließlich berichtet wird, solcherlei Nachteile befürchten.

Diese Dritten (Behandler, Mit-Behandler, Gehilfen etc.) werden nach der bisherigen Konzeption des Patientenrechtegesetzes nicht davor geschützt, dass Berichte aus Risikomanagement- und Fehlermeldesystemen zu ihrem Nachteil verwendet werden.[19] Problematisch ist dieses nur punktuelle Verwendungsverbot nicht nur deshalb, weil die tatsächliche Akzeptanz dieser Systeme im Alltag darunter leiden wird, sondern vor allem auch deshalb, weil man durch den Verzicht auf ein umfassendes Verwertungsverbot diese Fehlermeldesysteme konzeptionell in die Nähe einer ganz anderen Art von Meldesystemen rückt, nämlich die der Whistleblower-Meldesysteme.[20] Im Rahmen solcher Whistleblower-Meldesysteme mag es typisch sein, dass zwar der Meldende geschützt werden soll, gerade nicht aber derjenige, über dessen Fehlverhalten etwas berichtet wird. Eben weil aber medizinische Fehlermeldesysteme eine gänzlich andere Zielsetzung haben, nämlich das möglichst umfangreiche Sammeln und Auswerten von Risikowissen ohne Blick auf persönliche Verantwortung, kann hier der Regelungsansatz des Patientenrechtegesetzes nicht überzeugen.

Es geht – um dies abschließend noch einmal hervorzuheben – bei Fehlermeldesystemen eben gerade nicht um „naming, blaming, shaming", also persönliche Vorwürfe und individuelle Verantwortung, sondern allein um das „Aus Fehlern lernen"[21], und eben diese Zielsetzung muss auch durch datenschutzrechtliche Regelungsvorgaben entsprechend flankiert und abgesichert werden.

---

19 Kritisch dazu auch: *Schwarze*, Patientenrechtegesetz – Die Sichtweise des Rechtsanwalts, S. 9, abrufbar unter: http://anaesthesie.uk-koeln.de/de/zielgruppen/lehre-und-fortbildung/fortbildung/kolloquium/vortraege-anaesthesiekolloquien, zuletzt abgerufen am 27.11.2013.

20 Vgl. allgemein zum Begriff des Whistleblowers: *Tinnefeld/Rauhofer*, Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten?, DuD 2008, 717.

21 *Gunkel/Rohe/Sanguino Heinrich/Hahnenkampf/Thomeczek* (Fn. 4), S. 3, 5; vgl. auch *Rohe/Thomeczek*, Risikomanagement in der Arztpraxis, KVH-Journal 2011, 5 (6).