

Aus Fehlern lernen: Risikomanagement mit Fehlerberichtssystemen*

Incident-Reporting-Systeme im Gesundheitswesen können einen spezifischen Beitrag zum Risikomanagement leisten und das systematische Lernen aus Fehlern sowie die Sicherheitskultur fördern. Je nach Einsatzort und Zielsetzung eines Fehlerberichts- und Lernsystems kann dieses unterschiedlich ausgestaltet sein und dadurch typische Vorteile nutzen. Im folgenden Beitrag werden Hintergrund, Entwicklung und unterschiedliche Eigenschaften von Berichtssystemen dargestellt und erläutert.

1. Hintergrund

Behandlungsschäden und Fehler in der Medizin sind kein neues Thema. Schon der Hippokrates zugeschriebene Wahlspruch „primum non nocere“ (etwa 5. Jahrhundert v. Chr.) drückt den Wunsch aus, dem Patienten „zuerst einmal nicht zu schaden“ (Gehring und Mattli 2001). Im vergangenen Jahrhundert wurden dann unter anderem „Morbiditykonferenzen“ und Obduktionen dazu genutzt, um unerwünschte, möglicherweise fehlerhafte Verläufe von Eingriffen zu untersuchen und daraus zu lernen. Dennoch wurde erst durch Untersuchungen in den letzten 15 Jahren erkannt, dass Behandlungsschäden und Fehler in der Medizin ein relativ häufiges Problem sind und auch Todesfälle verursachen.

Der im Jahr 2000 erschienene Bericht des US-amerikanischen Institute of Medicine postuliert, basierend auf den Forschungsergebnissen von Brennan und Leape aus dem Jahr 1991, dass jährlich 44.000 bis 98.000 Todesfälle in US-amerikanischen Kliniken durch Fehler verursacht werden (Institute of Medicine 2000; Brennan 1991; Leape 1991). Von diesen Berechnungen und ähnlichen Ergebnissen anderer

Wissenschaftler aufgerüttelt (Thomas et al. 2000; Vincent et al. 2001; Wilson et al. 1995), begann man auch in Deutschland das Thema Patientensicherheit systematischer als bisher zu bearbeiten. Weltweit wurden Institutionen zur Förderung der Patientensicherheit gegründet und vielfältige Maßnahmen zur Vermeidung von Behandlungsfehlern ergriffen. Eine davon ist die Einführung so genannter Fehlerberichts- und Lernsysteme, auch Incident-Reporting-Systeme (IR-Systeme; im weiteren Text auch Berichtssysteme) genannt. Der Kerngedanke dieser Systeme ist das Berichten von eigenen oder beobachteten sicherheitsrelevanten Ereignissen, sodass diese systematisch analysiert werden können und man selbst, aber auch Andere daraus lernen können.

2. Umgang mit Fehlern

Im Rahmen der Aktivitäten zur Verbesserung der Patientensicherheit wurde deutlich, dass der bisherige Umgang mit Fehlern im medizinischen Alltag nicht zielführend ist. Im Gesundheitswesen ist die traditionelle, personenorientierte Perspektive bis heute weit verbreitet. Immer noch werden Ärzte und Pflegepersonal, wenn ihnen ein Fehler unterläuft, persönlich beschuldigt (Wie konnte Ihnen das passieren? Warum passen Sie nicht auf?), gelegentlich vor Kollegen oder Patienten gemaßregelt beziehungsweise bestraft oder zumindest angewiesen „besser aufzupassen“. Schulungen und Fortbildungen der „Schuldigen“ werden nur in seltenen Fällen als Verbesserungsmöglichkeit gesehen. Ein solcher Umgang mit Fehlern zielt darauf, durch Veränderungen beim Einzelnen die Sicherheit insgesamt zu verbessern. Es wird dabei jedoch außer acht gelassen, dass die Fehlleistungen Einzelner häufig durch Sicherheitslücken im System (mit-)verursacht werden und es daher nur eine Frage der Zeit ist, bis einem(r) Kollegen(in) aufgrund der immer noch bestehenden Sicherheitslücke ein ähnlicher Fehler passiert (Reason 2000; Leape et al. 1998).

* Der Beitrag basiert auf dem Kapitel „Incident Reporting Systeme - in jedem Zwischenfall ein Fehler?“, aus dem Buch „Medizinschadensfälle und Patientensicherheit“, herausgegeben von Burkhard Medea and Reinhard Dettmeyer, Deutscher Ärzte-Verlag, Köln 2007, Seiten 169-176 sowie GGW 2008 Risikomanagement mit Fehlerberichtssystemen, Jg. 8, Heft 1: 18-25

Verschiedene Forscher postulierten daher die Notwendigkeit, eine systemorientierte Sichtweise im Gesundheitswesen - analog zu der in Hochrisikoindustrien üblichen - zu entwickeln und anzuwenden. Diese Perspektive geht grundsätzlich davon aus, dass Menschen fehlerbar sind, und dass das System selbst (zum Beispiel ein Krankenhaus oder eine Arztpraxis) in seinen Strukturen und Prozessen sicher angelegt sein muss, um Fehler und daraus resultierende Behandlungsschäden zu vermeiden. Das bedeutet, dass beispielsweise organisatorische Prozesse, Geräte und Medikamentenverpackungen derart gestaltet sein müssen, dass die Fehlermöglichkeiten gering sind und Fehler, die dennoch gemacht werden, keine dramatischen Auswirkungen für die Patienten haben (Reason 2000; Leape 1994). Diese Sichtweise findet sich in Incident-Reporting-Systemen insofern wieder, als diese versuchen, systematisch aus Fehlern und unerwünschten Ereignissen zu lernen und bei der Analyse der Ereignisse der Schwerpunkt auf die systematische Ursachenforschung gelegt wird.

2.1. Vorbild aus der Luftfahrt

In risikoreichen Industriezweigen (kommerzielle Luft- und Seefahrt, Atomenergie) wurde schon zu einem viel früheren Zeitpunkt erkannt, dass die systematische Aufarbeitung von Fehlern und kritischen Ereignissen wertvolle Hinweise auf Sicherheitslücken in den jeweiligen Systemen liefern kann. Das bekannteste Berichtssystem ist vermutlich das „Aviation Safety Reporting System“ (ASRS) der Federal Aviation Administration in den USA¹. Seit 1975 werden alle Piloten, das gesamte Bord- und Bodenpersonal, Mechaniker und andere in der Luftfahrt beteiligte Personen aufgefordert, tatsächlich oder potenziell gefährliche Situationen per Post oder Internet an das ASRS zu berichten (tatsächliche Unfälle dürfen

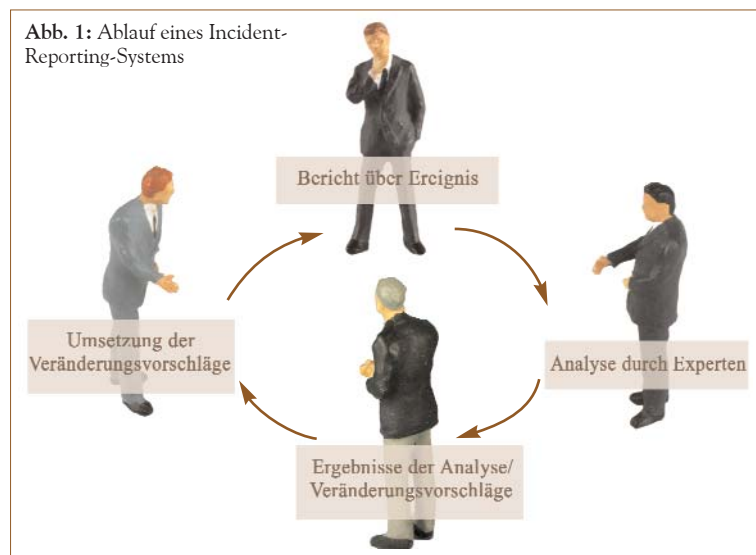
nicht berichtet werden). Die Berichte sind streng vertraulich, und den Berichtenden ist Immunität vor möglichen Sanktionen garantiert, wenn sie ihren Bericht binnen zehn Tagen nach dem Ereignis einreichen.

Bisher sind beim ASRS rund 715.000 Berichte eingegangen. Die Analysen der geschilderten Ereignisse zeigen Probleme und Schwachstellen in den Flugsicherheitssystemen und Sicherheitsprozeduren auf und tragen zu deren Verbesserung bei. Außerdem dienen die Ergebnisse als Datenbasis für die Entwicklung neuer Richtlinien oder neuer Ausrüstung in der Luftfahrt.

Zwei regelmäßig erscheinende Publikationen („Callback“ und „Directline“) fassen jeweils Berichte und Schlussfolgerungen zu bestimmten Themen (zum Beispiel plötzliche Störungen während des Abarbeitens von Checklisten) zusammen und sind zentrale Instrumente, um die in der Luftfahrt arbeitenden Menschen zu informieren³.

3. Berichtssysteme in der Medizin

In den letzten Jahren wurden weltweit verschiedene medizinische Incident-Reporting-Systeme entwickelt. Über sie werden im Gesundheitswesen Tätige aufgefordert, über sicherheitsrelevante Ereignisse aus ihrem Umfeld zu berichten (Abbildung 1). Anschließend werden die Be-



richte von Experten analysiert und die Ergebnisse beziehungsweise Veränderungsvorschläge an die Nutzer des Systems zurückgegeben. Mit „Experten“ ist eine Arbeitsgruppe (fachspezifisch oder berufsgruppenübergreifend) gemeint, die über ein besonderes Wissen, Können oder Training in der systematischen Analyse sicherheitsrelevanter Ereignisse verfügt.

Die Nutzer der Incident-Reporting-Systeme können dann die Veränderungsvorschläge umsetzen. Trotz ihres verbindenden Grundgedankens - nämlich „Aus Fehlern lernen“ - sind die medizinischen Incident-Reporting-Systeme zum Teil sehr verschieden aufgebaut. Auf die relevantesten Unterschiede der verwendeten Berichtssysteme wird in den nachfolgenden Abschnitten eingegangen.

Analog zu den Vorbildern in sicherheitsorientierten Industrien und in der Medizin im Ausland (zum Beispiel England und Schweiz) wurden in den letzten Jahren auch in Deutschland Incident-Reporting-Systeme aufgebaut^{4,5}. Neben verschiedensten institutsinternen Systemen finden sich mehrere internetbasierte, institutsübergreifende und teilweise fachspezifische Systeme. Eine ausführliche Anleitung (nebst Hilfsmitteln und Praxistipps) zur Einführung von Incident-Reporting-Systemen im Krankenhaus wurde von einer Arbeitsgruppe des Aktionsbündnisses Patientensicherheit e. V. erarbeitet (Aktionsbündnis Patientensicherheit e. V. 2006; Aktionsbündnis Patientensicherheit e. V. 2007).

3.1. Intern oder extern

Ein Berichtssystem kann innerhalb einer Institution, zum Beispiel im Krankenhaus, intern (also lokal) betrieben werden oder auch institutionsübergreifend (also extern) sein. Je nach Art des Berichtssystems sind unterschiedliche Möglichkeiten der Berichtsabgabe, des Feedback beziehungsweise der Verbesserungsstrategien gegeben. Grundsätzlich haben beide Arten der Berichtssysteme spezifische Vorteile, die je nach Anwendungsbereich und Zielvorgabe des Berichtssystems genutzt werden sollten.

Der Typ des Berichtssystems bestimmt häufig die Art der Berichtsabgabe. Externe Systeme greifen meist auf ein internetbasiertes Formular

zurück, wodurch viele Menschen unabhängig von Ort und Zeit berichten können. Interne Systeme arbeiten häufig mit Formularen im Intranet der Institution und auch mit handschriftlichen Berichten auf vorgedruckten Formularen. Die Papier-Formulare werden dabei eher von jenen verwendet, die im Rahmen ihrer Arbeit keinen Zugang zum Computer haben (zum Beispiel Transport- oder Reinigungspersonal). Einige Incident-Reporting-Systeme lassen beide Arten der Berichtsabgabe zu.

Interne Berichtssysteme haben den Vorteil, dass der „Kreislauf des Berichtssystems“ (siehe Abbildung 1) vollständig innerhalb der Institution abläuft. Ein internes Analyseteam kennt die spezifischen Umstände in einem Krankenhaus oder in einer Abteilung und kann diese bei der Formulierung von Verbesserungsvorschlägen berücksichtigen. Außerdem können die Mitarbeiter der Abteilung bei der Entwicklung von Verbesserungsvorschlägen maßgeblich mitwirken. Deren Umsetzung kann dann wiederum durch die Experten des Analyseteams unterstützt werden. Des Weiteren können die Mitarbeiter im Rahmen eines aktiv betriebenen internen Incident-Reporting-Systems leichter ein Zugehörigkeitsgefühl entwickeln, welches sich zum Beispiel in reger Berichtstätigkeit und in konstruktiven Verbesserungsvorschlägen zeigt.

Externe Systeme können sich bei den Analysen ausschließlich auf den vorliegenden Bericht beziehen, und die Ergebnisse beziehungsweise Verbesserungsvorschläge des externen Analyseteams können folglich meist nur von allgemeiner Natur sein. Die Anpassung und Umsetzung dieser Vorschläge muss dann eigenständig in der Institution erfolgen. Externe Berichtssysteme haben jedoch den Vorteil, dass sie einer größeren Zielgruppe zur Verfügung stehen und dass die Berichte von sehr vielen Menschen gelesen werden können. Dies kann bei einem Bericht über ein spezifisches Problem mit einem bestimmten technischen Gerät von großer Wichtigkeit sein (zum Beispiel, wenn ein Defekt oder Fehler eines Narkosegeräts unabhängig voneinander in mehreren Krankenhäusern auftritt). Auch können Institutionen voneinander lernen. Fehlervermeidungsstrategien können in ei-

nem Krankenhaus erprobt und entwickelt werden, ein anderes Krankenhaus kann diese Strategie dann „lernen“. Ein weiterer Vorteil externer Berichtssysteme ist die Tatsache, dass die Anonymität noch größer ist und daher nicht nur über Beinahe-Schäden, sondern auch über tatsächliche Schäden berichtet werden kann (siehe auch Abschnitt 3.3 „Definition, was berichtet werden soll“). Berichtete Ereignisse können theoretisch überall auf der Welt passiert sein; eine Rückverfolgung der beteiligten Personen oder der Institution ist dabei unmöglich. Nicht zuletzt bieten externe Systeme dem ambulanten Sektor eine gute Möglichkeit, an einem Berichtssystem teilzunehmen, denn für eine kleine Arztpraxis würde es sich nicht lohnen, ein internes Incident-Reporting-System aufzubauen.

3.2. Freiwillig oder verpflichtend

Es existieren sowohl freiwillige als auch verpflichtende Berichtssysteme. Es ist jedoch umstritten, ob die Verpflichtung zu berichten tatsächlich höhere Berichtszahlen bewirkt oder eher abschreckt. Meist wird die Freiwilligkeit als erfolgsfördernde Eigenschaft beschrieben (Leape 2002). Grundsätzlich muss man davon ausgehen, dass auch nominell verpflichtende Systeme in der Praxis fast immer freiwillig sind. Dies liegt daran, dass Fehler und Beinahe-Schäden oft nur einer einzigen Person auffallen und dass es daher im Ermessen dieses Menschen liegt, ob das Ereignis berichtet oder „vergessen“ wird.

3.3. Definition, was berichtet werden soll

Einige Berichtssysteme erfassen - meist aus rechtlichen Gründen - ausschließlich Ereignisse, die keinen Schaden verursacht haben (so genannte Near-miss-Ereignisse beziehungsweise Beinahe-Schäden). Dies ist im deutschsprachigen Raum fast immer in Krankenhäusern der Fall, da die Krankenhausleitung aus haftungsrechtlichen Gründen keine Berichte über tatsächliche Schäden in einer den Mitarbeitern und gegebenenfalls Anderen zugänglichen Datenbank sammeln möchte. Wirkliche Schadensfälle müssen ja auch in Hinblick auf den Umgang mit Patienten und andere Beteiligte auf anderen Wegen bearbeitet werden.

Andere (meist externe) Systeme können durch ihre Sicherheitsstruktur auch Ereignisse mit Schadensfolge aufnehmen. Die Fehlerhaftigkeit (Vermeidbarkeit) des Ereignisses spielt - hinsichtlich der Definition, was berichtet werden soll - meist nur eine untergeordnete Rolle. Dies ist vor allem deshalb so, weil die Vermeidbarkeit oft nicht einwandfrei festzustellen ist und auch unabhängig davon aus Ereignissen gelernt werden kann. Insofern kann nicht davon ausgegangen werden, dass in jedem Bericht tatsächlich auf einen Fehler im Sinne eines vermeidbaren fehlerhaften Plans beziehungsweise einer vermeidbaren fehlerhaften Handlung, also auf ein vermeidbares Ereignis, hingewiesen wird. Wenige Berichtssysteme fordern die Nutzer auch dazu auf, positive Ereignisse zu berichten, zum Beispiel kritische Situationen, die besonders gut gemeistert worden sind.

3.4. Anonym oder vertraulich

Die meisten Berichtssysteme arbeiten ausschließlich mit vollständig anonymen Berichten, ohne die Identität des Berichtenden zu erfassen. Wenige sind streng vertraulich. Diese haben den Vorteil, dass gegebenenfalls Rückfragen an den Berichtenden zu Details des Ereignisses möglich sind und dass die Analysen dadurch genauer sein können. Die Daten der Berichtenden werden niemals an Dritte weitergegeben. In diesem Zusammenhang muss auf das Problem der Anonymität in kleinen Abteilungen hingewiesen werden. Hier ist es oft - trotz vollständiger Anonymisierung des Berichts - nicht möglich, eine wirkliche Anonymität der beteiligten Personen zu gewährleisten, da das Ereignis zum Beispiel ohnehin schon bekannt ist oder aber bestimmte (nicht löschbare) Details des Berichts Rückschlüsse auf die Beteiligten zulassen. Hier ist es bei der Analyse des Berichts besonders wichtig, die systemorientierte Perspektive nicht zu verlassen (Fragen nach „Was ist passiert? Warum ist es passiert?“ Und NICHT: „Wem ist es passiert? Wer hat was getan?“) und eine vertrauensvolle Kultur des Fehlermanagements zu etablieren.

3.5. Freitext oder Kategorien

Die verschiedenen Berichtssysteme unterscheiden sich bezüglich des Anteils der Fragen, die

mit Freitext beziehungsweise in vorgegebenen Antwortkategorien zu beantworten sind. Die Erfahrung zeigt, dass eigentlich nur der geschriebene Bericht in Freitextfeldern ein Verstehen des Ereignisses und der spezifischen Umstände zulässt, während die zusätzlichen Klassifikationen mittels Auswahlfeldern allenfalls Randinformationen liefern. Mehrere Freitextfelder mit unterschiedlichen Fragen können darüber hinaus zu einem detaillierten Bericht mit eigenen Analysen und Verbesserungsvorschlägen führen. Auch in der internationalen Diskussion zu Fehlerberichtssystemen wird die Wichtigkeit der Freitextfelder betont (World Health Organization 2005). Eine Zusammenfassung erfolgsfördernder Eigenschaften von Incident-Reporting-Systemen zeigt die Tabelle.

4. Möglichkeiten und Grenzen medizinischer Berichtssysteme

Im Vergleich zu Maßnahmen des letzten Jahrhunderts wie zum Beispiel „Morbiditätskonferenzen“ und Obduktionen bieten Incident-Reporting-Systeme neue Möglichkeiten der Risikoanalyse. Im Rahmen eines (internen oder externen) Incident-Reporting-Systems kann über Fehler, Zwischenfälle und unerwünschte Ereignisse berichtet und aus diesen gelernt werden, ohne dass die Identität der Beteiligten offenge-

legt werden muss (Einschränkung bei internen Incident-Reporting-Systemen: Bei schwerwiegenden oder typischen Ereignissen sind die Beteiligten häufig allgemein bekannt). Diese Anonymität erleichtert die Meldungen über sicherheitsrelevante Ereignisse und ermöglicht damit das systematische Lernen aus Einzelereignissen, aber auch aus einer größeren Anzahl von Berichten.

4.1. Möglichkeiten

Da die Analyse auch Berichte ohne oder mit nur geringer Schadensfolge umfasst, können chronische Schwachstellen in Abläufen oder Verfahren aufgedeckt werden, bevor schwerwiegende Schäden an genau diesen Stellen entstehen. Bei „Morbiditätskonferenzen“ geht und ging es meist nur um schwerwiegende Ereignisse und Schäden.

Seltene Ereignisse, zum Beispiel ein spezifischer technischer Defekt eines medizinischen Geräts, können durch externe, institutionsübergreifende Incident-Reporting-Systeme bekannt werden und für alle beteiligten Institutionen publik gemacht werden.

Externe Incident-Reporting-Systeme bieten auch kleinen Institutionen des Gesundheitswesens, zum Beispiel Arztpraxen mit nur einem Arzt und ein bis zwei Mitarbeiterinnen, die

Tabelle: Eigenschaften von erfolgreichen Berichtssystemen	
Eigenschaft	Erklärung
sanktionsfrei	Es gibt keinerlei Sanktionen für Berichtende und Nutzer.
anonym oder streng vertraulich	Die Identität des Berichtenden, des Patienten oder der Institution ist entweder vollständig anonym oder streng vertraulich. Die vertraulichen Daten werden niemals an Dritte weitergegeben.
freiwillig	Die Abgabe eines Berichtes ist freiwillig.
unabhängig	Das Berichtsprogramm ist von jeglicher Autorität, die Berichtende oder Nutzer bestrafen könnte, unabhängig.
Analyse durch Experten	Die Berichte werden von Experten analysiert, die die klinische Situation verstehen und zugrunde liegende Systemfehler erkennen können.
zeitnahe Rückmeldung und Umsetzung	Die Berichte werden schnell analysiert und die Ergebnisse bzw. Empfehlungen zügig umgesetzt (bei internen Incident-Reporting-Systemen) bzw. für Berichtende und Nutzer veröffentlicht.
systemorientiert	Die Empfehlungen fokussieren auf Veränderungen von Systemen, Prozessen oder Produkten.
einfach	Das Berichtsformular ist einfach und für jeden zugänglich.
Freitextfelder	Das Berichtsformular basiert vor allem auf Freitextfeldern.

Chance, sich einfach und anonym mit Kollegen über Zwischenfälle und Vermeidungsstrategien auszutauschen.

Incident-Reporting-Systeme können also das Risikobewusstsein der im Gesundheitswesen Tätigen fördern und die Sicherheitskultur stärken.

4.2. Grenzen

Die Grenzen von Incident-Reporting-Systemen sind vielfältig und je nach Art des Systems unterschiedlich bedeutsam. Im Folgenden soll auf die wichtigsten Beschränkungen von Incident-Reporting-Systemen eingegangen werden.

Die reine Bereitstellung oder Einführung von externen oder internen Berichtssystemen hat keinen Einfluss auf die Patientensicherheit. Nur „lebendige“ Berichtssysteme mit adäquaten Berichtszahlen, systemorientierten Analysen und sinnvollen Verbesserungsstrategien können die Sicherheitskultur stärken und die Patientensicherheit möglicherweise erhöhen. Der tatsächliche Nachweis, dass Berichtssysteme die Patientensicherheit erhöhen, konnte bisher nicht erbracht werden. Die Schwierigkeit dieses Nachweises liegt darin, dass die Messung aller sicherheitsrelevanten Ereignisse in einer bestimmten Einheit des Gesundheitswesens (zum Beispiel Abteilung eines Krankenhauses oder Arztpraxis) extrem aufwändig ist. Jede Messmethode (zum Beispiel retrospektive Aktenanalyse, Beobachtung, Berichte der Beteiligten oder Betroffenen) kann immer nur einen Teil aller Ereignisse aufdecken. Zudem ist die Kausalität zwischen Einführung eines Berichtssystems und Veränderung der Anzahl der sicherheitsrelevanten Ereignisse fast niemals eindeutig zu klären.

Incident-Reporting-Systeme eignen sich nicht dafür, Aussagen zur Epidemiologie sicherheitsrelevanter Ereignisse zu machen. Es werden ja lediglich jene Ereignisse betrachtet, die erstens selbst bemerkt oder beobachtet werden und die zweitens auch berichtet werden. Man geht davon aus, dass aus einer Vielzahl von Gründen (zum Beispiel Wahrnehmung von Ereignissen; Angst, ein Ereignis zu berichten; Zeitmangel, um Berichte abzugeben) nur ein Bruchteil aller sicherheitsrelevanten Ereignisse gemeldet wird (Billings 1998).

Es darf auch nicht außer Acht gelassen werden, dass die Analyse der Berichte immer vor dem Problem des „hindsight bias“ („Rückschaufehler“ beziehungsweise das Problem des „Hinterher ist man immer schlauer“) steht. Das heißt, zum Zeitpunkt der Analyse liegen Informationen zum Ablauf und Ergebnis des Ereignisses vor, die der Handelnde während des Ereignisses nicht hatte. Diese Informationen werden aber bei der Beurteilung des Ereignisses herangezogen. Dieser Effekt muss ganz besonders bei der Formulierung zukünftiger Vermeidungsstrategien beachtet werden.

5. Fazit

Incident-Reporting-Systeme können einen wichtigen Beitrag zum Risikomanagement im Gesundheitswesen leisten. Für die erfolgreiche Einführung und Anwendung eines Berichtssystems sind vielfältige Kriterien zu beachten, wobei der Erfolg immer mit der Glaubwürdigkeit des Systems zusammenhängt. Die Mitarbeiter, die Berichte schreiben sollen, müssen davon überzeugt sein, dass sie selbst und ihre Kollegen keine Nachteile aus der Aufarbeitung der Berichte haben. Darüber hinaus müssen sie erfahren, dass die Mühe, die sie für einen Bericht aufwenden, gut investiert ist, weil aus den Berichten sinnvolle Veränderungen im Krankenhaus, und damit für die eigene Arbeit, abgeleitet werden. Hierfür ist es essenziell, dass die Klinik- oder Abteilungsleitung hinter den Zielen und der Einführung des Berichtssystems steht und die Umsetzung von Verbesserungsvorschlägen fördert.

Ein Incident-Reporting-System kann letztlich nur in Verbindung mit einer aktiven und „gelebten“ Sicherheits- und Fehlermanagementkultur die Patientensicherheit fördern.

Literatur und Web-Quellen bei den Verfassern oder im Internet unter www.aerzteblatt-sh.de

Dr. Julia Rohe, MPH, Fachärztin für Allgemeinmedizin und Gesundheitswissenschaftlerin, E-Mail rohe@azq.de

Dr. Christian Thomeczek, Facharzt für Allgemeinmedizin, Flugmedizin und Notfallmedizin, Qualifikation als leitender Notarzt, Ausbildung als Verkehrsflugzeugführer, E-Mail thomeczek@azq.de

Nachdruck aus GGW 1/2008 mit freundlicher Genehmigung des KomPart-Verlags