Fehler als Freunde betrachten

Der CIRS-Gedanke in der Krankenhaus IT

Meist ist die erste Frage nach einem kritischen Ereignis: Wer ist Schuld? Diese „Schuldkultur" führt dazu, dass Fehler verschwiegen werden. Ein Umdenken ist nötig: Dr. med. Rainer Röhrig, Justus-Liebig-Universität Gießen, skizziert Berichtssysteme, an die anonym kritische Ereignisse und Beinahe-Behandlungsfehler berichtet werden können, und die Herausforderungen im Bereich der Krankenhaus-IT.

Vor fast 15 Jahren erschien der amerikanische Bericht „To Err is human – Building a Safer Health System" [1]. Die Schätzung, dass in Amerikanischen Krankenhäusern jährlich 98.000 Patienten durch medizinische Fehler versterben stellte die Renaissance des historischen Grundsatzes „primum non nocere" und damit des Begriffs der Patientensicherheit dar. Auch wenn man über die Zahl ebenso kritisch wie über die Schätzung der jährlichen 19.000 Todesfälle durch Behandlungsfehler in deutschen Krankenhäusern diskutieren kann [2], was bleibt ist die Erkenntnis, dass Fehler im Gesundheitswesen zu thematisieren und strukturelle Konzepte zur Fehlervermeidung zu entwickeln und umzusetzen sind. Eine wesentliche Voraussetzung zur Fehlervermeidung ist die richtige Information zur richtigen Zeit am richtigen Ort der richtigen Person im richtigen Kontext richtig zu präsentieren um so medizinische Entscheidungen und Prozesse zu unterstützen und zu verbessern. Damit ist klar, dass die medizinische Informationsverarbeitung und damit Healthcare IT und „intelligente" Medizintechnik Schlüsselbausteine darstellen.

Doch in der Medizin gilt: Es gibt keine Wirkung ohne Nebenwirkung: Der Einsatz von Software als Informationssystem oder integriert in Medizintechnik ist ebenfalls mit Nebenwirkungen behaftet und kann bei Konstruktionsfehlern, aber auch durch Fehler bei der Implementierung, beim Betrieb oder der Anwendung zu Patientenschäden führen [3-7].

Damit hat auch der GBA-Beschluss vom 23.01.2014, die „grundsätzlichen Anforderungen an ein einrichtungsinternes Qualitätsmanagement für nach §108 SGB V zugelassene Krankenhäuser" um die Forderung nach einem abteilungs- und berufsgruppenübergreifenden Fehlermeldesystems zu erweitern [8], Konsequenzen für die Krankenhaus-IT. Zum einen wird sofort nach einem „IT-System" zur Umsetzung verlangt, zum anderen fallen auch Fehler mit einer Beteiligung von Krankenhaus-IT unter die „Meldepflicht". Das Ziel ist aus Fehlern zu lernen.

Bei der Implementierung von Fehlermeldesystemen gilt es zwischen Beinahe-Behandlungsfehlern (Near Misses) und unerwünschten Ereignissen (UE, auch Adverse Events (AE) zu unterscheiden (siehe Abbildung 1). Unerwünschte Ereignisse, also Ereignisse mit einem (Patienten-) Schaden, können straf- und zivilrechtliche Verfahren zur Haftungsfrage nach sich ziehen und sind daher gesondert zu betrachten. Hierzu gibt es auch verschiedene juristische Empfehlungen [10].

Critical Incident Reporting-Systeme (CIRS) sind Berichtssysteme, an die anonym kritische Ereignisse und Beinahe-Behandlungsfehler berichtet werden können. Die Meldungen sollten danach bewertet und ggf. in einem Risikomanagementprozess weiterbearbeitet werden.

Anmerkung: Bei der Anwendung von Medizinprodukten (einschl. Software wie PACS oder ggf. PDMS) gilt die Medizinprodukte-Sicherheitsplanverordnung (MPSV), in der Vorkommnisse und Meldepflichten explizit geregelt sind [11]. Diese gilt ebenso wie die Meldepflicht bei unerwünschten Arzneimittelwirkungen. Diesen Meldepflichten ist zusätzlich zu einer CIRS-Meldung nachzukommen.

Technische Umsetzung

Die meisten Häuser haben bereits ein CIRS implementiert. Dies erfolgt häufig papierbasiert, kann aber auch durch eine IT-Unterstützung erfolgen. Es stehen jedoch auch verschiedene Webportale wie CIRSmedical (www.CIRSmedical.de) der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung, das Krankenhaus-CIRS-Netz (KH-CIRS-Nezt, www.kh-cirs.de/"http://www.kh-cirs.de/) des Aktionsbündnis Patientensicherheit, der Deutschen Krankenhausgesellschaft (DKG) und des deutschen Pflegerates oder CIRS AINS (www.CIRS-AINS.de) der Deutschen Gesellschaft für Anästhesie und Intensivmedizin (DGAI) und des Berufsverbandes Deutscher Anästhesisten (BDA) zur Verfügung. Der Vorteil dieser Lösungen ist, dass man auch von den Fehlern anderer Einrichtungen/Kliniken lernen kann und ggf. eine höhere Anonymität erreicht werden kann.

Die Forderung des GBA nach einer einfachen Verfügbarkeit von Fehlermeldesystemen für die Mitarbeiter stellt damit keine technische Herausforderung dar.

Organisatorische Umsetzung

Die Herausforderungen bei der Implementierung eines CIRS-Systems liegen also mehr im organisatorischen Bereich. Hier gilt es in der Klinik eine Methodenkompetenz aufzubauen und entsprechende Prozesse zur Bewertung und zum Risikomanagement zu etablieren sowie eine Veränderung im Bewusstsein der Mitarbeiter und damit der Unternehmenskultur zu entwickeln.

Meist ist die erste Frage nach einem kritischen Ereignis: Wer ist Schuld? Diese „Schuldkultur" führt dazu, dass Mitarbeiter aus Furcht vor persönlichen (dienstrechtlichen) Konsequenzen oder Ansehensverlust Fehler eher verschweigen. Mitarbeiter werden nur dann Fehler berichten, wenn ihnen keine negativen Konsequenzen drohen. Dies ist durch ein anonymes Meldesystem, eine Unabhängigkeit der CIRS-Stelle sowie durch eine Erklärung des Klinikumsvorstandes zum Mitarbeiterschutz sicherzustellen. Dies sollte mit einer Systemischen und mit einer Fehlerursachenanalyse gekoppelt werden. Führend ist die Frage, „Wie konnte der Fehler entstehen? (Fehlerkultur.) Darauf basierend gilt es Maßnahmen zu ergreifen und Verhaltensregeln zu erstellen, die zukünftig das Risiko minimieren können. Führend ist die Frage „Warum kann dies bei uns (nicht mehr) passieren?" (Sicherheitskultur).

Umsetzung in der Krankenhaus-IT

Neben den allgemeinen organisatorischen Herausforderungen bei der Etablierung eines CIRS-Systems müssen im Bereich der Krankenhaus-IT auch spezifische Besonderheiten beachtet werden:

Prof. Dr. med. Markus A. Weigand, Direktor der Klinik für Anaesthesiologie, Operative Intensivmedizin, Schmerztherapie (Direktor Univ.-Prof. Dr. M. A. Weigand), Justus-Liebig-Universität Gießen

- **Die Anonymität kann nicht sichergestellt werden**

Bei Fehlern mit Beteiligung von IT-Systemen erfolgt in der Regel eine Fehlermeldung über ein Service Desk (Hotline, Single Point of Communication, SPOC), wo der Fehler in einem Support-Ticketing-System (Issue-Tracking-System) dokumentiert wird. Darüber hinaus ist häufig ein Mitarbeiter für die Administration eines IT-System's, bzw. eines KIS-Moduls zuständig. Häufig werden in Kliniken die Administratoren auch von Anwendern untrennbar mit dem IT-System verbunden. Damit ist der Vorgang immer mit Personen verbunden. Daraus erhöht sich die Bedeutung eines erklärten und gelebten Mitarbeiterschutzes. Für Leitungsfunktionen bedeutet dies, dass Mitarbeitern vermittelt werden muss, dass Fehler(meldungen) als Freunde betrachtet werden müssen, deren Meldung gerne gesehen wird und die einem helfen Schaden abzuwenden. Dass ein Mitarbeiter mehr Fehler meldet, heißt nicht dass er mehr Fehler macht, er trägt aber auf jeden Fall mehr zur Patientensicherheit bei.

- **Service Desk + Meldung an Hersteller + CIRS = redundante Dokumentation**

Durch die Nutzung von Support-Ticketing-Systemen an dem Service Desk steht bereits ein Fehlerdokumentationssystem. Eine zusätzliche Dokumentation in einem CIRS wird damit als redundanter und damit unnützer Dokumentationsaufwand empfunden.

Die Lösung kann ein abgestuftes Vorgehen sein: Fehlermeldungen werden standardmäßig im Incident Management einer Fehlerursachenanalyse unterzogen und bewertet. Wenn sich dabei herausstellt, dass aus dem Fehler eine Gefährdung resultiert und dieser auch in anderen Systemen/Abteilungen/Kliniken auftreten könnte, sollte dieser zusätzlich in einem CIRS gemeldet werden. Da Softwarefehler immer systemisch sind, ist dies ein weiteres Argument für die Verwendung eines öffentlich verfügbaren CIRS wie CIRSmedical (s.o.).

Unabhängig von der internen Dokumentation in einem Support-Ticketing-System und CIRS ist auch der Hersteller zu informieren, damit dieser im Rahmen seiner Verkehrssicherungspflicht andere Betreiber und Anwender aktiv über Risiken informieren und korrektive und organisatorische Maßnahmen ergreifen oder empfehlen kann.

- **Komplexität**

Kritische Ereignisse mit IT-Beteiligung unterliegen häufig einer hohen Komplexität [12]. Es gilt u.A. Aspekte des Nutzungskontext, Softwareergonomie, hart kodierten (Programmierung durch Hersteller) und parametrierten (von oder für Betreiber individualisierten) Funktionalitäten, der Interoperabilität mit anderen IT-Systemen oder Geräten und der eigenen Organisationsstruktur zu beachten. Um zukünftige Schäden zu vermeiden und nicht einfach ein „Ticket zu schließen“, ist es wichtig, der Sache auf den Grund zu gehen: Es reicht nicht aus, den Auslöser für ein kritisches Ereignis zu identifizieren, man muss die Ursache(n) finden und benennen können. Dies ist häufig nur unter Einbeziehung von Anwendern und Herstellern möglich.

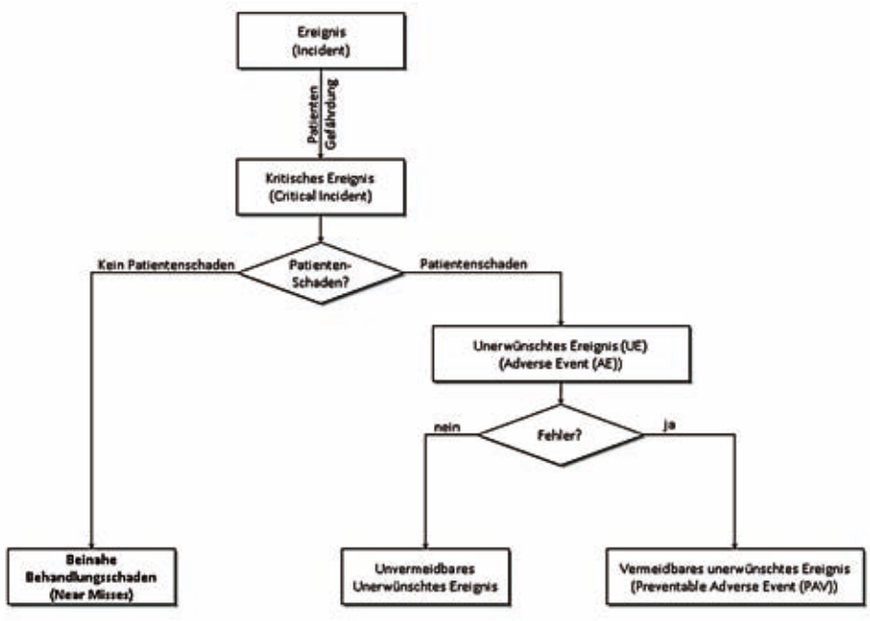
Um den Prozess der Fehleranalyse effizient und sicher gestalten zu können sind Klassifikationssysteme zu entwickeln, die eine Risikobewertung standardisieren und vereinfachen können.

Kommunikation zwischen Hersteller und Klinik

Aus den Ausführungen wird klar, dass auch bei Herstellern von Krankenhaus-IT noch ein Umdenken von einer „Schuldkultur“ im Sinnen eines Abwehrens von Verantwortung hin zu einer Fehler- und Sicherheitskultur stattfinden muss. Beinahe-Behandlungsfehler sollten herstellerseitig zu einem konstruktiven Dialog mit Anwendern und Betreibern genutzt werden. In einem Schadensfall fehlt dem Dialog vor Gericht die konstruktive Komponente.

Aber auch Kliniken müssen bei der Bewertung der Hersteller umdenken: Fehler- und Risikomeldungen durch Hersteller lassen nicht zwangsläufig auf ein schlechteres Produkt schließen. Sie zeugen aber von einer Fehler- und Sicherheitskultur im Sinne der Patientensicherheit.

Folgen eines kritischen Ereignisses modifiziert nach Thomeczek [9].



Dr. med. Rainer Röhrig, Leiter der Sektion Medizinische Informatik in Anaesthesiologie und Intensivmedizin, Klinik für Anaesthesiologie, Operative Intensivmedizin, Schmerztherapie (Direktor Univ.-Prof. Dr. M. A. Weigand), Justus-Liebig-Universität Gießen

Literatur
[1] Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson, Editors; Committee on Quality of Health Care in America, Institute of Medicine: To Err Is Human: Building a Safer Health System. Washington, DC: The National Academies Press, 2000
[2] Richter-Kuhlmann E:Patientensicherheit: Gefährliche Zahlenspielchen Dtsch Arztebl 2014; 111(5): A-147 / B-127 / C-123
[3] Han YY, Carcillo JA, Venkataraman ST, Clark RS, Watson RS, Nguyen TC, Bayir H, Orr RA.: Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. Pediatrics. 2005 Dec;116(6):1506-12.
[4] Koppel R, Leonard CE, Localio AR, Cohen A, Auten R, Strom BL.: Identifying and quantifying medication errors: evaluation of rapidly discontinued medication orders submitted to a computerized physician order entry system. J Am Med Inform Assoc. 2008 Jul-Aug;15(4):461-5
[5] Stürzlinger H, Hiebinger C, Pertl D, Traurig P.: Computerized Physician Order Entry - Wirksamkeit und Effizienz elektronischer Arzneimittelverordnung mit Entscheidungsunterstützungssystemen. Schriftenreihe Health Technology Assessment 2013 (86). 10.3205/hta000069L
[6] Magrabi F, Ong MS, Runciman W, Coiera E.: An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc. 2010 Nov-Dec;17(6):663-70
[7] Bowman S.: Impact of electronic health record systems on information integrity: quality and safety implications. Perspect Health Inf Manag. 2013 Oct 1;10:1c. eCollection 2013.
[8] Gemeinsamer Bundesausschuss: HYPERLINK "https://www.g-ba.de/downloads/39-261-1919/2014-01-23_KQM-RL_137-1d.pdf"https://www.g-ba.de/downloads/39-261-1919/2014-01-23_KQM-RL_137-1d.pdf (Zuletzt abgerufen am 12.04.2014]
[9] Thomeczek C, Rohe J, Ollenschläger G: Das unerwünschte Ereignis in der Medizin. In Madea B, Dettmeyer R (Hrsg.): Medizinschadensfälle und Patientensicherheit. Deutscher Ärzteverlag Köln. 2007. S. 13-20.
[10] Ulsenheimer K, Bock RW: Der juristische Notfallkoffer – Verhalten nach einem Zwischenfall. Anästh Intensivmed 2013;54:2-1. Online: HYPERLINK "http://www.bda.de/downloads/22_2-11JuristischerNotfallkoffer.pdf"http://www.bda.de/downloads/22_2-11JuristischerNotfallkoffer.pdf (Zuletzt abgerufen 14.04.2014)
[11] Medizinprodukte-Sicherheitsplanverordnung vom 24. Juni 2002 (BGBl. I S. 2131), die zuletzt durch Artikel 3 der Verordnung vom 10. Mai 2010 (BGBl. I S. 555) geändert worden ist
[12] Ahlbrandt J, Dettmeyer R, Brammen D, Seggewies C, Johner C, Röhrig R: Fehleranalysen und Verantwortlichkeiten bei kritischen Ereignissen durch Krankenhaus-IT - Ein Fallbericht. GMDS 2013. 58. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS). Lübeck, 01.-05.09.2013. Düsseldorf: German Medical Science GMS Publishing House; 2013. DocAbstr.280 Online: http://dx.doi.org/10.3205/13gmds078