KLINISCHES RISIKOMANAGEMENT IN BEZUG AUF ELEKTRONISCHE GESUNDHEITSAKTE

Wrodnigg GH[1], Dorda W[2]

Kurzfassung

Elektronische Gesundheitsakte bieten großes Potential hinsichtlich verbesserter Behandlung und Versorgung von Patienten im intramuralen und extramuralen Gesundheitswesen. Zur Realisierung müssen jedoch komplexe computerisierte Systeme etabliert und vernetzt werden, um die hierfür benötigten Informationen zur Verfügung zu stellen. Sicherheits- und Service-Management-Systeme sollen die Sicherheit und Verfügbarkeit von Informationen gewährleisten. Jedoch ist es auch mit diesen Managementansätzen nicht möglich, komplexe Systeme bis ins kleinste Detail zu beherrschen. Daher ist der Ansatz des Risikomanagements als zentrale Drehscheibe die Methode der Wahl, um so „Hot Spots" zu identifizieren und vorrangig zu behandeln, wodurch ein hinreichendes Maß an Sicherheit und Verfügbarkeit gewährleistet werden soll. In dieser Arbeit wird ein Referenzmodell zum klinischen Risikomanagement in Bezug auf elektronische Gesundheitsakte vorgestellt, damit ein möglicht hohes Maß an Sicherheit und Verfügbarkeit medizinischer Daten zu akzeptablen Kosten realisiert werden kann.

1. Einleitung

Die strategische Planung und Etablierung lebensbegleitender elektronischer Gesundheitsakte (ELGA) im österreichischen Gesundheitswesen wird durch nationale [1] und europäische [2] strategische Zielvorgaben initiiert [3]. Dies bedingt jedoch die Schaffung verteilter Computersysteme. Aufgrund der komplexen Struktur solcher vernetzten Systeme ist es nicht mehr möglich, sämtliche potentiellen Fehler durch umfassendes Testen auszuschließen. Die Sicherheit und Verfügbarkeit medizinischer Daten ist jedoch eine wesentliche Anforderung an elektronische Gesundheitsakte. Ein immer größerer Teil von Behandlunsgfehlern mit Dauerschäden für Patienten ist auf unzureichende oder falsche Information zurückzuführen. In der Literatur sind zahlreiche Beispiele von Zwischenfällen in Zusammenhang mit medizinischen computerisierten Systemen dokumentiert [4][5][6]. Aus diesem Grund wurden Normungsaktivitäten initiiert, um mit dem Ansatz des klinischen Risikomanagements einen Leitfaden zur verbesserten Sicherheit solcher Systeme vorzugeben [7][8].

Ansätze zur technischen Beherrschung dieser Problematik sind das Informations-Sicherheits- bzw. IT-Service-Management. Jedoch sind auch diesen Ansätzen Grenzen gesetzt, denn es ist mit rationalem Aufwand nicht möglich, 100-%ige Sicherheit und Verfügbarkeit zu gewährleisten. Es muss also zwischen schweren und akzeptablen potentiellen Fehlern unterschieden werden, was durch den Ansatz des Risiko-Managements als zentrale Drehscheibe der Managementsysteme ermöglicht

[1] Medizintechnik, TÜV Austria Services GmbH Wien
[2] MIAS, Medizinische Universität Wien

werden soll. Ziel dieser Arbeit ist es, ein Referenzmodell für das klinische Risikomanagement medizinischer Daten zu entwickeln. Dadurch soll eine hinreichende Sicherheit und Verfügbarkeit elektronischer Gesundheitsakte bei akzeptablem Risiko gewährleistet werden. Dabei ist jedoch zu beachten, dass Risiken und Fehler nicht nur während der Entwicklung und Etablierung von IT-Systemen auftreten, sondern in allen Phasen des Lebenszyklus, insbesondere beim Betrieb und auch bei jeglicher Art von Änderungen am System – bis hin zu Risiken in Zusammenhang mit der Stilllegung.

2. Methoden

Die Basis für eine strukturierte Vorgehensweise bei Entwicklung, Etablierung und Betrieb von computerisierten Systemen bildet im Allgemeinen ein Vorgehens- oder Lebenszyklus-Modell. Im thematisch verwandten Bereich der Medizinprodukte-Software werden Lebenszyklus-Management und Validierung inzwischen durch die Novelle der EG-Richtlinie 93/42/EWG explizit vorgeschrieben [10]. Als klassisches Vorgehensmodell hat sich hierbei das so genannte V-Modell bewährt [11]. Die konsequente Weiterentwicklung des V-Modells, welches primär ein Vorgehensmodell für einzelne Projekte ist, führt schließlich zum Lebenszyklus-Modell zum Management des gesamten System-Lebenszyklus (vom Konzept bis zur Stilllegung), welches beispielhaft in *Abbildung 1* dargestellt ist.

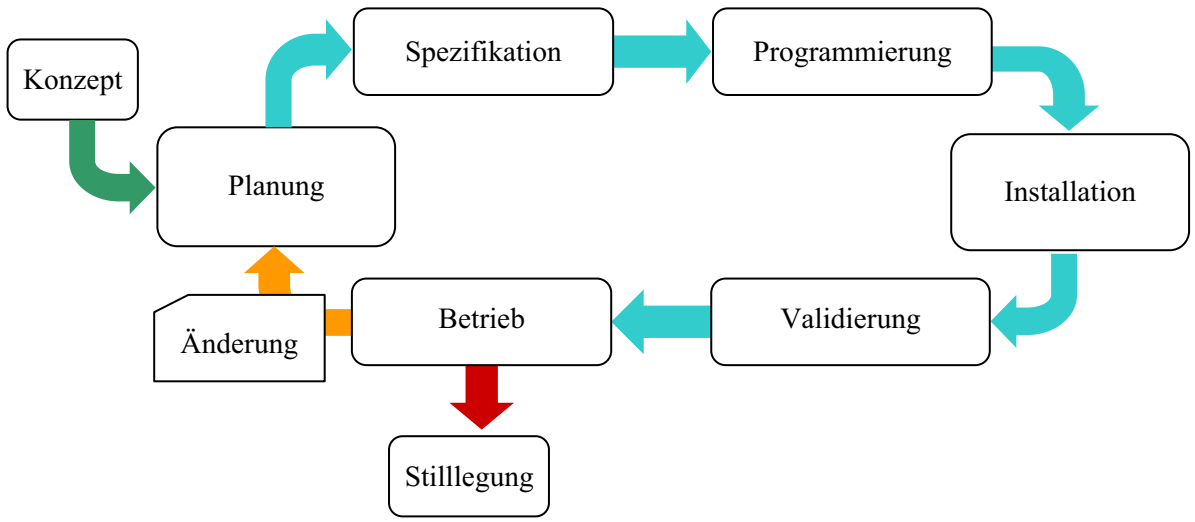

Abbildung 1: Schema des Lebenszyklus-Modells

Zur Verbesserung der Sicherheit von Informationssystemen wurde das so genannte Informations-Sicherheits-Management entwickelt, welches zunächst in den British Standards der Reihe BS 7799-x standardisiert beschrieben wurde. Im Rahmen der internationalen Harmonisierung und zum Zwecke der Zertifizierung solcher Managementsysteme werden die internationalen Standards ISO 2700x auf Basis der British Standards 7799-x veröffentlicht [12], welche zum Teil noch Gegenstand laufender Normungsaktivitäten sind. Für den Bereich der medizinischen Informatik ist ein branchenspezifischer Anwendungsleitfaden (ISO 27799) Gegenstand aktueller Normungsaktivitäten [13].

Neben der Sicherheit von Informationssystemen spielt auch deren Verfügbarkeit eine wesentliche Rolle. Zu diesem Thema wurde die so genannte IT Infrastructure Library (ITIL) entwickelt, eine

Sammlung von Publikationen zur Umsetzung eines IT-Service-Managements. Auch die Konzepte zum IT-Service-Management waren zunächst in britischen Normen (BS 15000) beschrieben, bevor sie im Zuge internationaler Harmonisierung in den Normen der ISO 20000-x [14][15] veröffentlicht wurden.

Die oben genannten Managementsysteme verweisen alle auf das Risiko-Management, welches für die Identifikation, Analyse und Bewertung von Risiken, sowie zur Evaluierung von Maßnahmen zur Risikominimierung eingesetzt wird. In der Medizintechnik ist das Risikomanagement bereits seit Jahren eine regulatorische Anforderung zur Gewährleistung der Sicherheit von Medizinprodukten [16]. War der ursprüngliche Fokus lediglich die initiale Abschätzung von Risiken im Rahmen einer Risikoanalyse [17], so hat sich die Methodik inzwischen zum Management von Risiken weiterentwickelt, was insbesondere die fortgesetzte Bewertung von Maßnahmen hinsichtlich ihrer Eignung zur Reduktion von Risiken und zum kontinuierlichen „Managen“ von Risiken umfasst.

3. Ergebnisse

Aufgrund der Vielfalt der Normungsaktivitäten zum Thema Risikomanagement ist in den letzten beiden Jahren eine gewisse redundante Divergenz an Vorgaben und Konzepten zum Risikomanagement für Informationssysteme entstanden. Als positiver Trend lässt sich ein Übergang von der zumeist einmalig durchgeführten Risikoanalyse zum Risiko-Management feststellen, allerdings ist diese Entwicklung noch nicht abgeschlossen bzw. ist das kontinuierliche Risikomanagement in den aktuellen Normentwürfen noch nicht konsequent umgesetzt. Insbesondere auf die Risiken im Zusammenhang mit Änderungen während der Entwicklung und vor allem beim Betrieb von Informationssystemen wird in den aktuellen Normvorschlägen meist nur am Rande eingegangen. Änderungen an Systemen im Zuge von Wartungsaktivitäten, wie zum Beispiel durch das Einspielen von Patches oder Modulen für zusätzliche Funktionalitäten können gänzlich neue Risiken oder neue Ursachen für bekannte Gefahren in das System einbringen, welche in der ursprünglichen Analyse nicht oder nur unzureichend berücksichtigt worden sind. Daher ist in Zusammenhang mit dem Lebenszyklus- und Risikomanagement ein konsequentes und umfassendes Änderungs-Management unumgänglich.

Als Referenzmodell für das Risikomanagement wird die in *Abbildung 2* dargestellte Systematik vorgeschlagen. Dieses Modell basiert auf den in der Literatur und in Normen dargestellten Konzepten zum Risikomanagement, jedoch wird die Problematik von System-Änderungen explizit berücksichtigt. Der Einstieg in das Modell beginnt mit der Definition des Informationssystems, der verwendeten Methoden für Risiko-Analyse und -Bewertung, sowie der system- oder projektspezifischen Vorgehensweise für das Risikomanagement, welche in einem Risikomanagement-Plan definiert werden.

Die Risiko-Analyse umfasst die Tätigkeiten zur Identifikation und Evaluierung der einzelnen Risiken und Gefahren. Die Risikobeherrschung formt den „inneren Zyklus“ der Risikomanagement-Aktivitäten. Hier erfolgen Präzisierung und Verbesserung der Analyse, die Definition von Maßnahmen zur Risikobeherrschung und die Bewertung dieser Maßnahmen (z.B. ob durch solche Maßnahmen nicht neue Risiken in das System eingebracht werden).

Nach der Prüfung auf Vollständigkeit der Ergebnisse erfolgt die Bewertung der Akzeptanz des Gesamt-Risikos, bzw. ob die verbleibenden Risiken in Bezug auf den Nutzen durch den Einsatz des Systems akzeptiert werden können. Die Ergebnisse des Prozesses werden schließlich in einem Ri-

sikomanagement-Bericht zusammengefasst, der auch eine Vorab-Bewertung und Klassifikation von Risiken in Bezug auf zu erwartende System-Änderungen enthalten sollte.

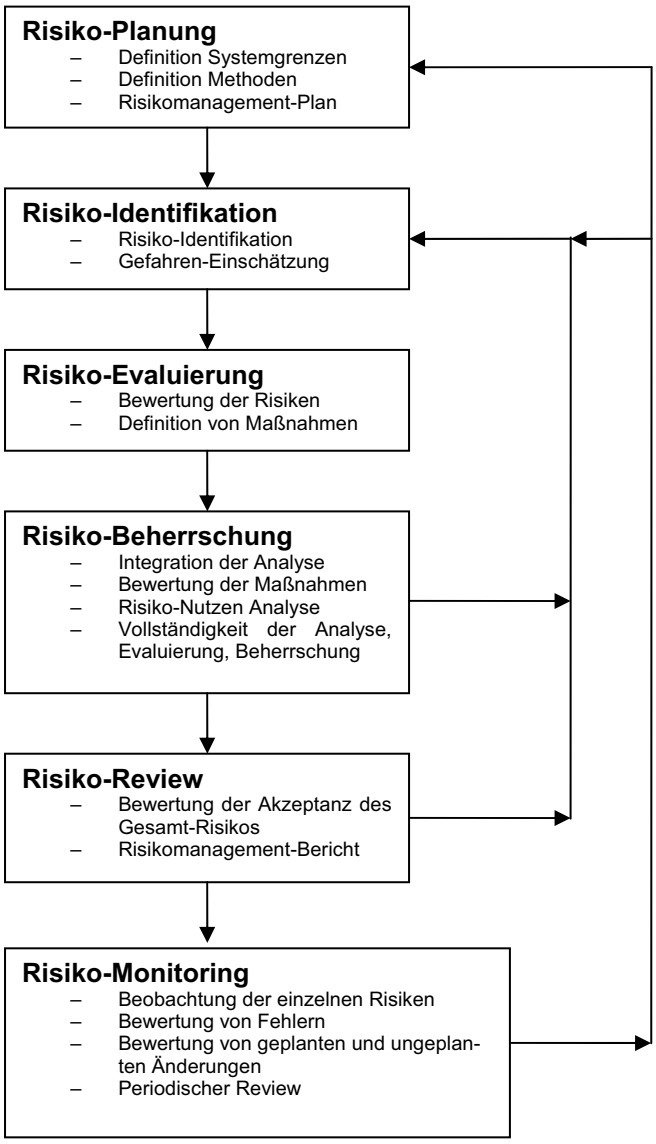

Abbildung 2: Schema eines generischen Risiko-Management-Modells

Der „äußere Zyklus“ des Risikomanagements wird durch das Risiko-Monitoring gesteuert. In dieser operativen Phase erfolgt die laufende Überwachung des Systems (wie z.B. die Auswertung von Logfiles, die Bewertung von Störungen oder unvorhergesehenen Ereignissen). Im Falle von Änderungen am System erfolgt hier der Einstieg in das Management neuer oder veränderter Risiken mit der Entscheidung, ob für diese Änderungen der neue Risikomanagement-Zyklus mit der Phase der Identifikation von Risiken beginnen kann, oder ob die Änderungen so umfassend sind, dass eine neuerliche Planung nach Überarbeitung der Definition der Systemgrenzen erforderlich ist.

Zudem ist ein periodischer Review des Risikomanagement-Plans und -Berichts vorgesehen, um deren Aktualität, Konformität mit dem Stand der Technik, sowie die Berücksichtigung allfälliger neuer oder überarbeiteter regulatorischer Anforderungen zu gewährleisten.

4. Diskussion

Die in der Literatur beschriebenen Risikomanagment-Modelle sind mit unterschiedlichen Zielsetzungen erstellt worden (wie zum Beispiel die Norm 14971:2007 [16] mit dem Fokus auf die Sicherheit von Patienten und Anwendern von Medizinprodukten).

Die aktuell in der Literatur oder in Norm(entwürfen) enthaltenen Konzepte gehen jedoch meist zu wenig auf die Aspekte der Änderung von Systemen ein und fokussieren auf die Entwicklung und Etablierung von Systemen, aber nicht so sehr auf das für den laufenden Betrieb erforderliche Änderungs-Management. Weiters wird die (vorläufige) Außerbetriebnahme von Systemen häufig unterbewertet. Da in solchen Fällen bei vernetzen Informationssystemen die Schnittstellenproblematik schlagend wird, und zudem medizinische Daten über mehrere Jahrzehnte zur archivieren sind, müssen entweder sämtliche Daten migriert, oder durch Bereithalten der operativ abgelösten Infrastruktur im Bedarfsfall verfügbar gemacht werden.

Dieser Problematik wird im dargestellten Referenzmodell dadurch begegnet, dass die kontinuierliche Überwachung der bekannten Risiken, und auch eine Neubewertung im Falle von Änderungen am System vorgesehen sind. Dies erfordert jedoch auch die Implementierung eines Änderungsmanagements im System-Lebenszyklus – sowohl bei der Entwicklung, als auch beim Betrieb von Informationssystemen.

Übertragen auf das komplexe vernetzte System zur Verwaltung und Bereitstellung der elektronischen Gesundheitsakte bedeutet das sicherlich einen gewissen Aufwand für diese Aktivitäten, welche zudem von einem geeigneten Gremium zentral koordiniert werden sollten. Allerdings bedingen Aspekte der Datensicherheit und des Datenschutzes ohnedies teilweise zentralisierte Organisations- und Verwaltungsstrukturen, so dass für den Ansatz des Risikomanagements auf diese Strukturen zurückgegriffen werden kann.

5. Schlussfolgerung / Ausblick

Klinisches Risikomanagement wird der Schlüssel zum Erfolg beim Lifecycle-Management von Informationssystemen für lebensbegleitende elektronische Gesundheitsakte sein, denn andernfalls wird entweder der Aufwand zur Sicherheit und Verfügbarkeit der Systeme vergleichsweise hoch sein, oder unterschätzte bzw. nicht berücksichtigte Risiken können zur Gefährdung oder gar Schädigung von Patienten führen. Aufgrund der Komplexität und der Anzahl der zu etablierenden vernetzten Systeme wird ein umfassendes Management der Risiken erforderlich sein, da nicht nur die einzelnen Informationssysteme zu betrachten sind, sondern die Gesamtheit der institutionsübergreifenden Gesundheitsinformationssysteme.

Mit Hilfe des vorgeschlagenen Referenzmodells zum klinischen Risikomanagement soll eine harmonisierte Basis für die modernen Risikomanagement-Systeme und -Methoden zur Gewährleistung der Sicherheit und Verfügbarkeit medizinischer Daten geschaffen werden.

Bei Planung, Errichtung, Betrieb und Änderung der entsprechenden Informationssysteme sollte ein konsequentes systematisches Vorgehen im Sinne eines Lebenszyklus-Managements mit begleitendem Risiko-Management vorgesehen werden, wie es beispielsweise für qualitätskritische Systeme in der Pharma-Branche gesetzlich vorgeschrieben ist [18].

Im Hinblick auf potentielle Gefahren aufgrund falscher oder fehlender Informationen aus elektronischen Gesundheitsakten sollten für die Etablierung der ELGA-Infrastruktur entsprechende Rahmenbedingungen ebenfalls verpflichtend vorgegeben werden.

6. Literatur

[1] Entwurf für eine österreichische eHealth-Strategie. http://www.bmgfj.gv.at/cms/site/attachments/8/5/3/CH0415/CMS1156950437801/entwurf_fuer_eine_oesterreichische_ehealth_strategie.pdf (accessed 2008-01-30).

[2] Elektronische Gesundheitsdienste - eine bessere Gesundheitsfürsorge für Europas Bürger: Aktionsplan für einen europäischen Raum der elektronischen Gesundheitsdienste, KOM(2004) 356 http://www.bmgfj.gv.at/cms/site/attachments/9/5/4/CH0414/CMS1085493102352/ek-mitt--ehealth-deu.pdf (accessed 2008-01-30).

[3] GALL W, GROSSMANN W, DORDA W, Auswertung Elektronischer Gesundheitsakte für Forschung und Qualitätsmanagement, Tagungsband der eHealth 2007 – Medical Informatics meets eHealth; Vienna, Austria; pp. 53 - 58; 2007.

[4] KOHN IT, CORRIGAN JM, DONALDSON MS, To Err is Human: Building a Safer Health System, USA. Institute of Medicine, National Academy Press, 1999.

[5] An Organisation with a Memory, HMSO, June 2000.

[6] BRENNAN TA, LEAPE II, LAIRD NM, HERBERT I, LOCALIO AR, LAWTHERS AG, Incidents of adverse events and negligence in hospitalised patients: results of the Harvard Medical Practice Study, New England J Med., 324, 1991, pp 370-376.

[7] ISO/PDTS 29321.5.36 – Health Informatics – Application of risk management to the manufacture of health software (Version 5.6), Sept. 2007.

[8] ISO/PDTE 29322.4 – Health Informatics – Guidance on the management of clinical risk relating to the deployment and use of health software systems (Version 3.4), Nov. 2007.

[9] Quality of care: patient safety, Report of the WHO Secretariat, EB 109/9, 5 December 2001.

[10] Richtlinie 2007/47/EG des europäischen Parlaments und des Rates vom 5. September 2007, Amtsblatt der Europäischen Union L 247/21.

[11] DRÖSCHEL W, WIEMERS M, Das V-Modell 97. Der Standard für die Entwicklung von IT-Systemen mit Anleitung für den Praxiseinsatz. Oldenbourg, München 1999.

[12] ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements.

[13] ISO/DIS 27799 – Health informatics – Security management in health using ISO/IEC 17799.

[14] ISO 20000-1 – Service Management: Specification.

[15] ISO 20000-2 – Service Management: Code of Practice.

[16] EN ISO 14971:2007 – Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte.

[17] EN 1441:1997 – Medizinprodukte – Risikoanalyse.

[18] Verordnung der Bundesministerin für Gesundheit und Frauen betreffend Betriebe, die Arzneimittel herstellen, kontrollieren oder in Verkehr bringen (Arzneimittelbetriebsordnung 2005 - AMBO 2005)