

Ausarbeitung von Michael Meier

## **E-Health Scenarios 2020 = Mobility + Ubiquity + Economics, but - Privacy?**

*Diese Ausarbeitung basiert auf dem Vortrag von Prof. Eymann ([http://www.bwl7.uni-bayreuth.de/de/team/001\\_Torsten\\_Eymann/index.html](http://www.bwl7.uni-bayreuth.de/de/team/001_Torsten_Eymann/index.html)) vom 12.06.2006 in Freiburg im Rahmen der Ringvorlesung 'Standort Internet Informatikinnovation' veranstaltet von Prof. Dr. Günter Müller. Dieses Dokument fasst diesen Vortrag zusammen bzw. gibt in verkürzt wieder und ergänzt ihn um einige kritische Anmerkungen.*

Wie sieht das Krankenhaus in der Zukunft aus? Betriebskosten müssen reduziert werden um den Steuerzahler zu entlasten. Die Koordination von Abläufen muss besser optimiert werden, schon um die Nerven von Patienten zu schonen und Wartezeiten zu verkürzen. Die Anzahl der Fehlbehandlungen muss vermindert werden, beispielsweise rühren 10% aller Medikationsfehler daher, dass Patienten verwechselt werden. Jedes Jahr gehen 15%-20% des Equipment (z.B. Infusionspumpen) verloren, weil diese entweder gestohlen werden, oder nicht auffindbar sind zur Wartung (was bei manchen Geräten einem Verlust gleichkommt). Wie könnte die Infrastruktur eines Krankenhauses beschaffen sein, um diese Ziele zu erreichen? Das ist die Frage, welche Prof. Eymann versucht hat zu beantworten. Der vorgestellte Ansatz basiert auf einer Architektur aus vier Ebenen: Identifikation, Intelligence, Integration und Optimierung.

Grundlage des Systems ist die totale Identifikation aller beteiligten Personen und Objekte, also Patienten, Ärzte, Blutkonserven, Infusionspumpen, Betten, Belegung von Betten, etc. Der naheliegende technologische Kandidat hierfür ist RFID. Ärzte mit einem RFID-Armband sind auf dem Krankenhausgelände lokalisierbar, ihre Aktivitäten nachvollziehbar und planbar. Blutbeutel tragen auf ihrem Chip z.B. die Blutgruppe des beinhalteten Blutes. Wenn also während einer Operation ein falscher Blutbeutel zur Hand ist, kann dies vor der Verabreichung festgestellt werden. Dasselbe gilt für Medikamente gemäß dem Motto: richtiger Patient, richtiges Mittel, richtige Dosis, richtige Zeit und richtige Verabreichungsart. Gebrauchsmaterialien müssen nicht langwierig gesucht werden, sondern können direkt lokalisiert werden, was Zeit einspart, welche für andere Tätigkeiten genutzt werden kann. Die psychologische Hürde Material zu entwenden wird erhöht, dadurch dass für Objekte Zonen definiert werden können in welchen sie sich befinden dürfen. Sollte ein Objekt eine solche Zone verlassen, wird ein Alarm ausgelöst, wie z.B. bei einem Diebstahl. Die Entnahme bzw. Rückgabe kann automatisch registriert werden, ohne dass hierfür Arbeitskräfte eingesetzt werden müssen. Medikamente können (halb-) automatisch nachbestellt werden, falls diese nicht mehr ausreichend vorhanden sind im Lager. Nützlicherweise kann die Kommunikation aller RFID-Tags über WLAN erfolgen, d.h. es wird keine separate Kommunikationsstruktur benötigt. RFID-Tags sind damit über alle mobilen Endgeräte, wie z.B. PDAs lokalisierbar bzw. abfragbar nach entsprechender Authentifizierung. Bereits allein durch diese Ebene ist also eine Steigerung der Effizienz zu erwarten. Patienten bekommen Armbänder mit einem inte-

grierten RFID-Chip auf welchem grundlegende Patientendaten, sowie eine Referenz auf eine URL eines Servers, wo detailliertere Informationen zu finden sind. Patienten sind durch das Krankenhauspersonal lokalisierbar und identifizierbar, Verwechslungen von Patienten durch menschliche Fehler werden reduziert. Nun ist das Thema Gesundheit und Krankenhaus, aber ein sensibles Thema und manche Menschen sind möglicherweise nicht gewillt sich einem solch allgegenwärtigen System zu unterwerfen. Deshalb ist es hier besonders wichtig einerseits auf Bedenken der Privacy detailliert einzugehen, was ich erst später tun werde, als auch ganz konkrete Anreize dafür zu schaffen, dass der Patient eine solche Architektur als vorteilhaft empfindet, auch ganz für ihn persönlich. Wenn man beispielsweise das Patientenarmband mit einem Notrufknopf ausstattet, welcher ihm erlaubt, einen Hilferuf in einem Notfall zu senden, kann man sicherlich erreichen, dass die Patienten das System besser annehmen. Patienten können sich potentiell auf dem Krankenhausgelände freier bewegen und brauchen nicht zwingend in ihrem Bett zu bleiben, was auf jeden Fall eine positive psychologische Wirkung haben dürfte, sofern man dem ganzen System Vertrauen schenkt. Außerdem kann man Infoterminals für die Patienten einrichten, an welchen man Informationen über ihre Krankheit, ihren Krankheitsverlauf etc. abfragen kann.

Auf der zweiten Ebene, der Intelligence-Ebene, werden aus dem riesigen Datenvolumen, welches auf der ersten Ebene gesammelt wurde, die wichtigen Daten ausgesondert. Die Daten werden analysiert, verwaltet, in ihren Kontext gestellt und ggf. schnell weiterübermittelt. Wenn sich zwei ähnliche Vorfälle räumlich nahe beieinander registriert werden, könnte man vermuten, dass sie dieselbe Ursache haben, d.h. Information wird in ihren Kontext gesetzt und an die zuständigen Ärzte weitergeleitet. Bei der aktuellen Fußball-Weltmeisterschaft werden z.B. Ärzte mit PDAs ausgestattet und geben so ihre Informationen an eine Einsatzzentrale weiter, wo genau solche Vorgänge stattfinden können. Es ist aber wohl nicht klar, welche Technologien auf dieser Ebene zum Einsatz kommen sollten, was auch für die nachfolgenden Ebenen gilt. Die Schaffung von Standards wird hier eine wichtige und sehr schwierige Aufgabe sein.

Die dritte Ebene sorgt für die Integration verschiedener Datenquellen. Man stelle sich vor, dass ein Patient öfters seinen Hausarzt gewechselt hat oder bereits in einigen Krankenhäusern war. Die Gefahr ist hier sehr groß, dass jede Stelle nur Zugriff auf einen Teil der Krankengeschichte des Patienten hat. Dies kann zu Mehrfachuntersuchungen, der Gabe falscher Medikamente oder gar falschen Diagnosen führen. Wenn ein Patient bewusstlos ins Krankenhaus eingeliefert wird, stehen unter Umständen gar keine Informationen über ihn zur Verfügung. Könnte man ihn mittels eines RFID-Chips identifizieren und seine Krankenakte abrufen, die wohlgerne erst aus verschiedenen Datenquellen zusammengestückt werden muss, dann könnten einige Probleme bei der Behandlung vermieden werden. Ein wesentlicher Problem hier ist, dass zu viele Firmen ihren eigenen Standard für ein solches System verkaufen wollen. Vielleicht wäre es hilfreich, wenn an dieser Stelle der Gesetzgeber eingreifen würde und einen einheitlichen Standard vorgeben würde, wie z.B. gerade bei der Gesundheitskarte geschehen. In den

USA gibt es über 150 sogenannte "Health Information Networks". Diese sind in der Lage innerhalb eines Netzwerkes Patientendaten auszutauschen, indem sie einen einheitlichen Standard zur Datenintegration einsetzen. Krankenhäuser können sich diesen Netzwerken anschließen, bekommen dann Standards vorgeschrieben, erhalten dafür aber wiederum finanzielle Unterstützung, was einen zusätzlichen Anreiz darstellt sich auch wirklich einem solchen Netzwerk anzuschließen.

Auf der vierten und letzten Ebene werden ablaufende Prozesse optimiert. Z.B. können freien Ärzten, abhängig von ihrem aktuellen Aufenthaltsort, neue Aufgaben zugewiesen werden, was es möglich macht die Liste der Aufgaben eines Arztes zu optimieren. So werden ablaufende Prozesse optimiert, was Zeit und Geld einspart. Dasselbe gilt auch für andere Angestellte des Krankenhauses. Patienten können rechtzeitig zu Untersuchungen einberufen werden. Wartezeiten werden so verringert und die Nerven der Patienten geschont.

Laut Prof. Eymann ist das größte Sicherheitsrisiko, neben den konventionellen Risiken in einem Kommunikationssystem, der Verlust von Identifikation. Es können keinerlei Entscheidungen bezüglich eines Patienten getroffen werden, wenn man sich nicht absolut sicher sein kann, dass man auch den richtigen Patienten vor sich hat. Der Verlust der Identifikation kommt hier dem Verlust des Patienten gleich, selbst wenn man ihn physisch vor sich hat. Ein großes Angriffsziel an ein derartiges System ist demnach die Erschwerung der Identifikation. Allein dies zeigt schon, dass die vorgestellte Architektur zwingend mit klassischen Mechanismen integriert werden muss und keinesfalls alleine existieren kann.

Bisher haben wir noch nicht über Privacy gesprochen, es sollte aber klar geworden sein, dass totale Identifikation in einer Krankenhausumgebung entscheidend ist für das Funktionieren der vorgestellten Architektur und damit das Thema Privacy zunächst einmal komplett in den Hintergrund gedrängt wird. Privacy hat aber unmittelbar mit Identifikation zu tun, nämlich insofern, dass man Personen fälschlich identifizieren kann. Beispielsweise sollte nur der behandelnde Arzt und niemand sonst auf die Krankengeschichte eines Patienten zugreifen dürfen. Es darf also keinesfalls passieren, dass jemand anderes als der behandelnde Arzt identifiziert wird. Insofern hat Privacy auch im Krankenhaus seine Berechtigung und 100%ige Identifikation ohne Anonymität bzw. Pseudonymität stellt gerade einen Verlust eben dieser Privatsphäre dar. Es kann aber auch passieren, dass ich aufgrund der Vielzahl der RFID-Chips, welche ich bei mir habe, aus irgendwelchen Gründen nicht identifiziert werden kann. Was tun? Wie kann ich beweisen, dass ich auch wirklich der bin, der ich vorgebe zu sein? Ein Lösungsansatz könnte die vorgestellte Alibi-Maschine sein. Sie kombiniert eine Identifizierung anhand biometrischer Daten, einer signierter Lokation und einer Zertifizierung des Gerätes selbst. Es wird also einfach versucht so viele vertrauenswürdige Informationen in ihr zusammenzutragen, dass es extrem unwahrscheinlich ist, diese alle zusammen fälschen zu können. Identifiziert ein Arzt seinen Patienten anhand der Alibi-Maschine, muss er natürlich Rechtssicherheit

haben, dass aufgrund der von der Alibi-Maschine des Patienten gelieferte Information als verbindlich angesehen werden kann. Interessant wäre hier die Frage, wer haften muss, wenn der Arzt seinem Patienten ein falsches Medikament aufgrund der Identifizierung der Alibi-Maschine gibt, d.h. wenn die Alibi-Maschine den Patienten aus irgendwelchen Gründen nicht korrekt identifiziert bzw identifizieren kann.

Verstärkter Einsatz von IT im Krankenhaus, ein schwieriges Thema. Auch wenn die Vorteile einer funktionierenden IT klar auf der Hand liegen, so ist doch das Stichwort Vertrauen von entscheidender Bedeutung. Jeder hat schon sehr oft erlebt, das ein Computer abstürzt oder davon das Daten von Hackern manipuliert werden. Nun ist das Abstürzen eines PCs an einem Büro-Arbeitsplatz zwar ärgerlich, aber nicht lebensbedrohlich, im Krankenhaus aber potentiell schon. Was passiert wenn das WLAN im Krankenhaus ausfällt? Das ist mit der vorgestellten Architektur allein keinesfalls abgedeckt. Es scheint demnach nicht möglich das Funktionieren eines Krankenhauses vollständig von der IT abhängig zu machen. Eine Integration mit traditionellen Mechanismen scheint unbedingt erforderlich zu sein. Wie das jedoch genau aussehen soll, ist wohl nicht klar. Das müssen Pilotprojekte, wie z.B. in Saarbrücken erst noch erweisen. Der Einsatz neuer Technologien im Krankenhaus scheint vielversprechend zu sein, ansonsten hätte man die RFID-Technologie vom Jacobi Medical Center New York gar nicht erst in Saarbrücken übernommen.

Aber hier besteht auch eine große Gefahr. Nämlich die, das Verantwortung vom Menschen an die IT übertragen wird und so es z.B. dem Patienten schwerer gemacht wird Schadenersatzansprüche gegenüber einem Krankenhaus durchzusetzen. Wie bereits erwähnt: wer haftet, wenn ein Patient aufgrund der IT falsch identifiziert wird und z.B. die falschen Medikamente erhält? Lässt sich das ohne Eingriff des Gesetzgebers realisieren? Ich glaube nein, es gibt einfach zuviel Einzelinteressen von Krankenhausbetreibern und Firmen die Geld einfahren wollen und die Belange der Patienten potentiell vernachlässigen. Der Gesetzgeber sollte allein schon deshalb einschreiten um Inselfösungen zu vermeiden bzw. Anreize dazu geben Inselfösungen zu vereinheitlichen. Dies hätte den Vorteil, dass der Standard von Krankenhäuser vergleichbar gemacht wird und so Wettbewerb zwischen den einzelnen Krankenhausbetreibern entsteht. Jeder Krankenhausbetreiber will sicherlich schlechte Presse vermeiden, ist ja schlecht für das Geschäft, was hoffentlich dem Patienten zu Gute kommt.

Auch ist das Thema Privacy nur mit der fiktiven Alibi-Maschine vertreten, was ja bedeutet, dass in den bisherigen Pilot-Projekten Privacy fast überhaupt keine Rolle spielt. Laut Prof. Eymann sind die bisherigen Projekte an Krankenhäusern, aber immer noch in einer so frühen Phase, dass im Punkte Privatsphäre keine negativen Ereignisse aufgetreten sind. Die Alibi-Maschine braucht von Seite des Gesetzgebers Rechtssicherheit, ansonsten kann ein Arzt keine Entscheidungen aufgrund von ihr treffen. Die Alibi-Maschine ist zwar nach dem Vortrag von Herrn Eymann etwas nebulös geblieben, aber wir brauchen solche Ansätze im Hinblick auf Privacy dringend, bevor wir

unsere Anonymität an der Krankenhausporte abgeben müssen. Ob ein solches System dann später in dieser Form dann auch wirklich eingesetzt wird, ist eine völlig andere Frage, welche die Pilotprojekte und der Gesetzgeber erst noch beantworten müssen.

Es geht mir keineswegs darum den gesamten Ansatz schlecht zu reden, aber es ist doch klar, dass das Thema Gesundheitssystem gesellschaftlich heikel ist und viele Leute mitreden wollen. Und es ist deshalb gerade notwendig einerseits neue Ansätze vorzustellen, als auch diese dann ausführlich zu diskutieren, um hoffentlich schon dadurch eine gewisse Akzeptanz zu schaffen und schlechte Ansätze von vorneherein auszusondern. Schließlich kann ein reales Krankenhaus es sich nicht leisten, nicht leistungsfähig zu sein, weil die IT gerade wieder mal streikt.