

DER WEG VON EHEALTH ZU MHEALTH – KOMPLEXE FUNKTIONALE UND SICHERHEITSANFORDERUNGEN IN DER WELT MOBILER MEDIZINISCHER GERÄTE

Pharow P¹, Blobel B¹, Aschenbrenner S²

Kurzfassung

Mobilität ist ein vielseitig genutzter Begriff. Er schließt Personen und Objekte genau so ein wie die verteilte Information. Im Gesundheitswesen sind die mobilen Geräte als Teil der Infrastruktur für viele Prozesse inzwischen unverzichtbar geworden. Für die Beteiligten spielen dabei Themen wie Sicherheit, Zugriff, Zugang, Datenschutz und Wahrung der Privatsphäre eine zunehmend wichtige Rolle. Existierende Sicherheitsdienste müssen daher angepasst und erweitert werden. Dies führt von eHealth zu einem mobilen Gesundheitswesen, auch Mobile Health oder mHealth genannt.

1. Einführung

Alle entwickelten Länder der Welt stehen vor der Herausforderung einer adäquaten Sicherung der Gesundheitsversorgung für die Bevölkerung unabhängig von gegebenen zeitlichen, örtlichen oder anderen Beschränkungen und ungeachtet der demografischen Entwicklung. Dies trifft zunehmend auch für sich entwickelnde Länder zu. Die Erwartungen der Bevölkerung hinsichtlich einer verbesserten Lebensqualität und die fast schon selbstverständliche Inanspruchnahme von hochtechnischen und zeitaufwändigen Gesundheitsleistungen nehmen parallel ebenfalls zu. Als bevorzugte Lösung für das wachsende Verfügbarkeitsproblem kristallisiert sich ein beginnender Paradigmenwechsel von organisationszentrierter über prozessorientierte (eHealth) hin zu personenzentrierter Gesundheitsversorgung heraus [1]. In dem Kontext spielen Themen wie Prävention, Wellness und Lifestyle sowie das aktive (Gesundheits)-Monitoring der Bürger eine zunehmend wichtige Rolle. Da im Versorgungsprozess neben dem ambulanten und dem stationären Bereich der häusliche und der Heimbereich einen immer höheren Stellenwert erlangen, kommt der Mobilität der Daten und der dahinter liegenden Technologie mobiler Geräte eine wachsende Bedeutung zu. Personal Health bzw. pHealth als neue, strikt personenbezogene Form von eHealth wird auf diesem Wege zu Mobile Health bzw. mHealth. Dies muss aber stets im Einklang mit geltendem Recht und unter Einsatz bestmöglicher technologischer Lösungen geschehen. Ein weiterer, wichtiger Aspekt sind Bewusstsein (*Awareness*) und Vertrauen (*Confidence*) und die daraus erwachsende Akzeptanz (*Acceptance*) aller Beteiligten und Betroffenen in die implementierten technischen und organisatorischen Lösungen. Letztlich beruht die gesundheitliche Betreuung der Bürger seit Jahrtausenden auf den Prinzipien von Vertrauen, Vertraulichkeit und Vertrauenswürdigkeit. Der Eid des Hippokrates, die ärztliche Schweigepflicht und die Aspekte medizinischer Ethik sollen hier nur als Beispiel stehen [2].

¹ eHealth Competence Center, Universitätsklinikum Regensburg, Deutschland

² Biomedizintechnik, Fraunhofer-Institut für Integrierte Schaltungen IIS Erlangen, Deutschland

2. Material und Methoden

Basis für alle Dienste im Gesundheits- und Sozialbereich ist stets die konkrete Situation und die damit verbundenen konkreten Erfordernisse aller Betroffenen. Zur Gewährleistung einer flexiblen Verknüpfung verschiedener Gesundheitsdomänen über lokale, regionale und oft auch nationale Grenzen hinaus sowie zur Individualisierung (Personalisierung) der begleitenden Prozesse müssen die unterstützenden Systeme der Informations- und Kommunikationstechnik (IKT) ebenfalls extrem flexibel und adaptierbar sein. Alle Bereiche des gesellschaftlichen Lebens und alle Medien bzw. Modalitäten für Monitoring, Diagnose, Betreuung und Therapie sowie Nachsorge und Rehabilitation sind dabei in den Workflow einzubeziehen. Trotz der immer weiter gehenden – und gewollten – Technisierung der Domäne Gesundheits- und Sozialwesen (GSW) dürfen Sicherheit (*Safety* und *Security*), Datenschutz (*Data Protection*), Ethik und Moral sowie die Wahrung der Privatsphäre (*Privacy*) aller Betroffenen (Bürger, Patienten, Angehörige, Heilberufler usw.) dabei aber nicht vernachlässigt werden. Daher ist bei jeder mobilen Art der Kommunikation (dies betrifft nicht nur die bekannten Mobiltelefone, sondern zunehmend jede Art mobil einsetzbarer Medizin- und Biomedizintechnik) auf Kommunikations- und Anwendungssicherheit zu achten [3]. Existierende und in Entwicklung befindliche Konzepte für Netzwerke, Protokolle und Mechanismen der mobilen Welt (z.B. WLAN, ZigBee, Bluetooth, WEP, WPA, WPA2) müssen auf ihre Tauglichkeit (*Adoption*) und ihre Anpassbarkeit (*Adaptation*) für die sichere mobile Kommunikation von Gesundheitsdaten analysiert und bewertet werden [4].

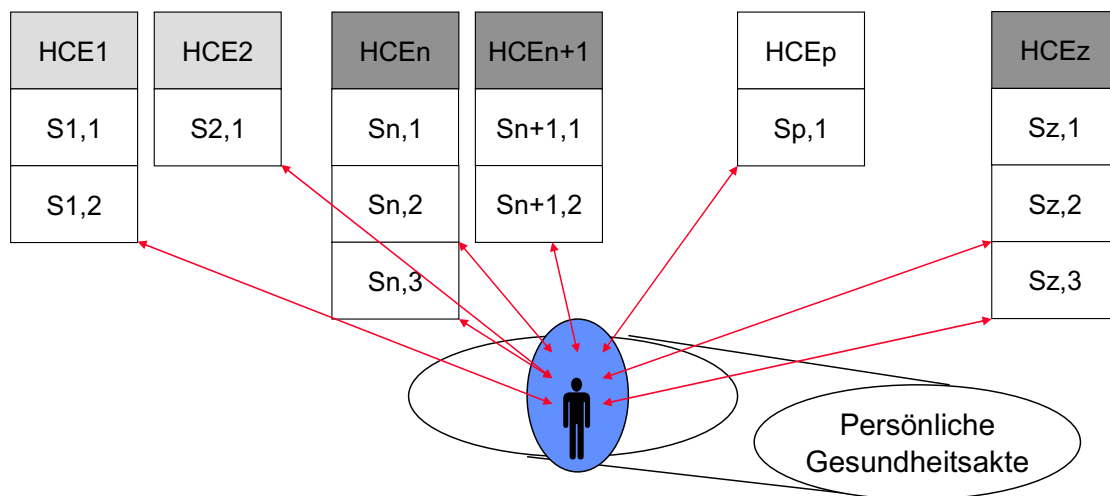


Abbildung 1. Beim Personal Health (pHealth) steht der Bürger im Mittelpunkt aller Aktivitäten

Beim Einsatz personalisierter Gesundheitsdienste (*Personal Health*) steht der Bürger bzw. der Patient im Mittelpunkt des gesamten Workflows. Alle Aktivitäten laufen bei ihm zusammen, er initiiert die erforderlichen Prozesse, unterstützt durch die Heilberufler. Alle am Workflow beteiligten Organisationen stellen die erfassten Informationen bereit, um eine sichere, vertrauenswürdige, lebenslange persönliche elektronische Gesundheitsakte zu generieren [5], die nicht nur den Versorgungsprozess selbst, sondern auch viele vorbeugende Maßnahmen (*Prevention*) beinhaltet. Bereits existierende internationale Standards unterstützen diese Entwicklung, ohne bereits den Anspruch auf Vollständigkeit zu erheben [6]. Neben der eigentlichen Gesundheitsversorgung (*Medical and Clinical Care*) stehen mehr und mehr die sozialen Aspekte (*Welfare*) und die Gesundheitsunterstützung (*Health*) im Zentrum der Prozesse [1]. Die Konzepte der öffentlichen Gesundheitsförderung (*Public Health*) tragen aktiv zur effektiven Umsetzung dieses Paradigmenwechsels bei (Abbildung 1).

3. Ergebnisse

Der Weg der Miniaturisierung der Geräte bis hin zu biomedizinischer Technik, körpernaher Sensorik, Aktoren, „intelligenter Kleidung“ und Nanotechnologie wird unaufhaltsam beschriftet. Mobile Geräte mit Klein- und Kleinstrechnern (wie Mobiltelefon, Palmtop, PDA), aber auch Notebook, Laptop und Tablet-PC bestreiten heute bereits einen wesentlichen Teil der Kommunikation zwischen allen am Versorgungsprozess im Gesundheits- und Sozialwesen beteiligten Personen und Instanzen [1]. Dies ist aber nur der Teil der Betrachtung mobiler Geräte, der direkt oder indirekt mit der Kommunikation verbunden ist. Der zweite, umfangreichere Teil adressiert Funktionalität, Sicherheit und Anwendung medizinischer und biomedizinischer Geräte, die direkt oder indirekt in den Behandlungsprozess involviert sind (für einige typische Beispiele siehe *Abbildung 2*).

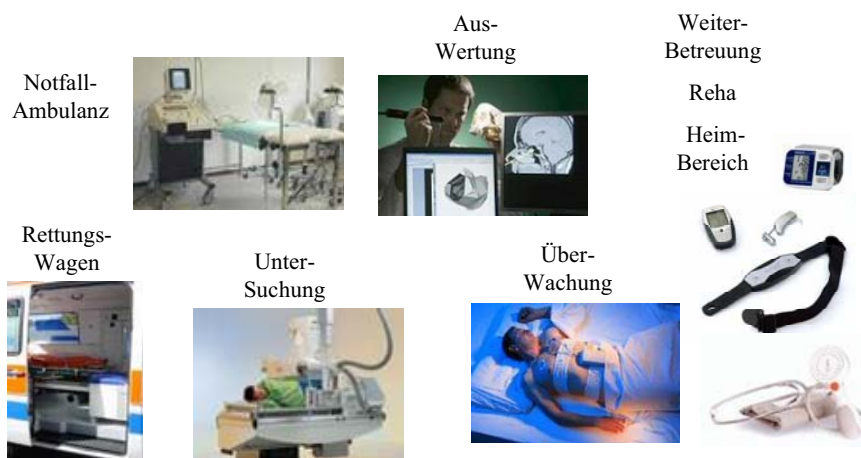


Abbildung 2. Medizinische mobile Geräte halten Einzug in nahezu alle Phasen der Behandlung

3.1. Sichere mobile Geräte und Sensoren

Die Entwicklung von Organisationszentrierten Szenarien zum Personenbezogenen *Secure Mobile Health* bietet Chancen und Risiken. Die Sensibilisierung aller Beteiligten für ein angemessenes Schutzniveau für *Safety* und *Security* ist ein wichtiger Erfolgsfaktor. Diese Aspekte müssen schon bei der Entwicklung mobiler Geräte berücksichtigt werden, ebenso die Akzeptanz der Lösungen beim Einsatz am Patienten. Die bei fast allen Prozessen der langfristigen bzw. hochfrequenten Aufnahme von Daten in unmittelbarer Umgebung des Patienten anfallenden enormen Datenmengen, mit medizinischen Geräten wie EKG, CT und MRI erzeugt, können bei der Betreuung rund um die Uhr nicht mehr unmittelbar und vollständig geprüft werden. Hier setzt die Datenverarbeitung ein, die für Vorverarbeitung, Vorbewertung und sichere Übertragung der Daten an die elektronische Gesundheitsakte (ELGA) sorgt. Komplexe Algorithmen analysieren anfallende Datenmengen, überprüfen Über- oder Unterschreitung von Grenzwerten, werten gespeicherte Aufzeichnungen aus und erkennen Veränderungen an physiologischen Parametern. Oft genügt für eine erste Bewertung die Übermittlung eines Signals (grün, gelb oder rot, analog zur Ampel). Erst das Zusammenspiel einzelner physiologischer Werte ergibt ein für den Arzt auswertbares konkretes Bild über den aktuellen Zustand des Patienten. Hier ergänzen sich medizinisches Wissen und mathematische Algorithmen. Sie bringen die im körpernahen Sensornetzwerk (*Body Area Network, BAN*) gemessenen Vitalparameter zusammen und ergeben ein komplexes Bild über den Vitalstatus der betroffenen Person. Hier gibt es Standards, die Geräte verschiedener Hersteller im BAN unterstützen [1], [6].

3. 2. Das Komplexmessgerät VitaSENS®

Im Rahmen verschiedener Forschungsprojekte wurden in der Abteilung Biomedizintechnik des Fraunhofer-Institutes für Integrierte Schaltungen IIS in Erlangen eine Reihe von Geräten entwickelt, die diese Anforderungen erfüllen (für einige Beispiele siehe *Abbildung 3*). Im Folgenden sollen einige Ergebnisse vorgestellt sowie ihre Funktion kurz beschrieben werden [7], [8].

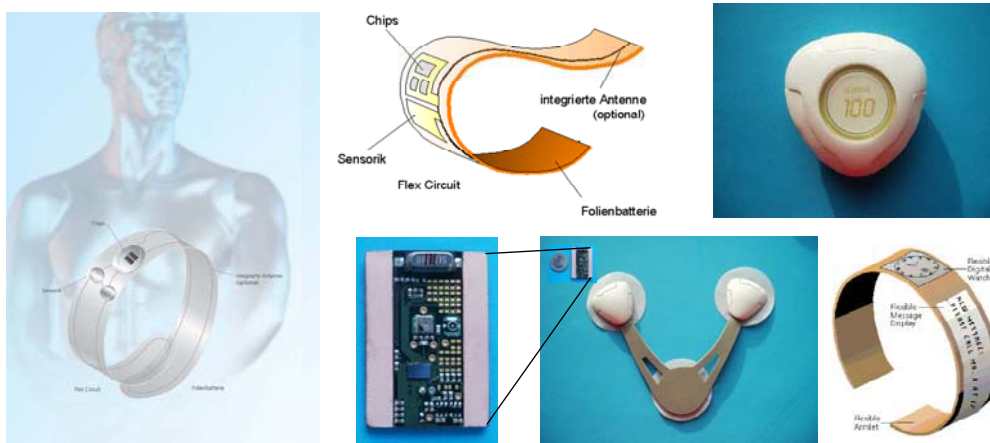


Abbildung 3. Mobile Kleinstgeräte zur Unterstützung von personalisierten Gesundheitsdiensten

Das Messgerät VitaSENS® erfasst verschiedene Vitalparameter am Körper und schickt sie drahtlos weiter. Es besteht aus einem Ohrclip, drei EKG-Elektroden und einer tragbaren Elektronikbox. Der Ohrclip-Sensor ermittelt die Blutsauerstoffsättigung. Die Elektroden erfassen das EKG-Signal [7]. Die Elektronikbox selbst als Verarbeitungs- und Übertragungsstation kann direkt am Körper getragen oder in Kleidungsstücke bzw. Gurtband integriert werden. Sie überträgt die gewonnenen Patientendaten drahtlos an eine zentrale Basisstation in der Nähe des Patienten. Diese analysiert und verarbeitet die eingehenden Messungen, erkennt medizinisch relevante Ereignisse (*Events*) und sendet sie, wenn erforderlich, an die nächste Arztpraxis, Klinik oder festgelegte Betreuungseinrichtung. Dort kann das zuständige Personal je nach Schweregrad des Ereignisses die notwendigen Schritte zur Unterstützung des Patienten einleiten.

Eine zweite Variante von VitaSENS® überträgt die gewonnenen Daten direkt an ein Mobiltelefon, welches sie verarbeitet, anzeigt und weitersendet. Damit ist eine maximale Mobilität gewährleistet, da die empfangende Stelle je nach Standort durchaus wechseln kann. Der Patient kann das Geräteset ganz einfach und bequem am Körper anbringen. Mit geeignetem Gehäuse könnte das Messgerät problemlos auch in der Freizeit, beim Wellness sowie beim Sport eingesetzt werden. Das Gerät eignet sich sehr gut zur Betreuung von Risikopatienten als auch von pflegebedürftigen Senioren zu Hause. Es kann in Kliniken wie auch in Seniorenzentren eingesetzt werden und unterstützt damit das Anliegen von pHealth und mHealth in gleichem Maße [8].

3. 3. Die sichere Funktionsweise

Über vier am Oberkörper des Patienten befestigten Elektroden wird die Herzmuskelaktivität registriert. Hierbei wurden alle relevanten Standards zur *Safety* berücksichtigt. Die Elektrodensignale werden dann einer Box zugeführt, die neben der miniaturisierten EKG-Elektronik ein Funkmodul und eine Batterie beinhaltet. Aus der Werten wird ein 4-Kanal-EKG abgeleitet. Die Messung der Pulswelle und der funktionalen Sauerstoffsättigung im arteriellen Blut erfolgt über einen Fingerclip

an der Hand des Patienten [8]. Die zugehörige Elektronik und das Funkmodul befinden sich in einem kleinen Täschchen, das wie ein Armband getragen werden kann. Alternativ können Pulswelle und Sauerstoffsättigung auch am Ohrläppchen aufgenommen werden. Die Elektronik wird dann nicht am Handgelenk, sondern direkt am Oberarm befestigt getragen. Über eine Nasenbrille und einen speziellen Drucksensor wird ständig die Atmung des Patienten überwacht. Besonders beim Einsatz in der Schlafdiagnostik leistet diese Sensorkomponente einen wichtigen Beitrag bei der Detektion nächtlicher Atemstillstandsphasen. Auf dem Brustkorb des Patienten befindet sich ein Bewegungssensor, der ähnlich einem größeren Pflaster (siehe *Abbildung 3*) getragen wird. Mit dieser Sensorkomponente wird die aktuelle Position des Patienten erfasst. Weiterhin ermöglicht die Auswertung der Messdaten, die unmittelbar im Sensormodul selbst erfolgt, eine Sturzdetektion: Bei ungewöhnlich starken Erschütterungen wird dann ein entsprechendes Alarmsignal ausgelöst und an eine Zentrale gesendet. Zur Messung der Oberflächen- bzw. Umgebungstemperatur kann ein zusätzlicher Temperatursensor eingesetzt werden. Die Ausführung als flexibles Pflaster ermöglicht dabei, diesen Messwertaufnehmer an beliebigen Körperstellen zu applizieren. Zusätzlich zur Überwachung durch die genannten Vitalparametersensoren soll dem Risikopatienten die Möglichkeit gegeben werden, auch manuell einen Alarm auszulösen. Bei Unwohlsein (*Event*) drückt der Patient kurz auf einen Knopf am Notfalltaster, um ein Alarmsignal an die Zentrale zu generieren und zu senden. Dieses Signal wird in der Zentrale dann besonders registriert.

Bei der Entwicklung und beim Einsatz der Sensoren wurde vor allem auf die *Safety* Wert gelegt. Alle Komponenten folgen den aktuellen Standards der elektrischen, elektronischen und mechanischen Sicherheit. Dazu wurde innerhalb des EU-Projektes SENSATION eine Studie zu existierenden Standards erstellt. Die übertragenen Signale werden am Körper verarbeitet, komprimiert und dann verschlüsselt übertragen. Auf die Kontrolle der Identität des Patienten (IDM) wurde besonderer Wert gelegt, um Daten sofort und auch später eindeutig zuordnen zu können. Dazu lief am Erlanger Institut eine entsprechende Diplomarbeit. Durch das geringe Gewicht, die leichte Applizierbarkeit und den unkomplizierten Einsatz waren auch die Testpatienten mit der Gerätepalette sehr zufrieden. Weitere Versuche laufen, klinische Tests sind bereits angedacht [7], [8]. Sowohl die Fragen von Sicherheit (*Safety, Security*) und Verfügbarkeit (Batterielaufzeit) als auch die Akzeptanzaspekte hinsichtlich eines klinischen Einsatzes konnten zufrieden stellend beantwortet werden.

4. Diskussion

Das eingangs genannte Grundprinzip des Vertrauens und der Vertraulichkeit im Arzt-Patienten-Verhältnis basiert heute zunehmend eher auf technischen Mechanismen (z.B. Signaturen) und Algorithmen (z.B. DSA), die ihrerseits Dienste für die Sicherheit (z.B. Integrität, Authentizität) bereit stellen. Dies trifft auf die Kommunikationssicherheit und ihre Dienste wie Identifikation, Authentifikation, Integrität, Nichtabstreitbarkeit von Sender und Empfänger, Verfügbarkeit und Vertraulichkeit genau so zu wie auf spezielle Sicherheitsdienste für Anwendungen wie Anonymisierung und Pseudonymisierung, Autorisierung, Datenschutz und Wahrung der Privatsphäre durch Einsatz einer modernen Zugangs- und Zugriffssteuerung. Weitere, in diesem Zusammenhang zu nennende Dienste sind die Integrität, die Genauigkeit, die Verbindlichkeit sowie die Prüfbarkeit. Das Identitätsmanagement (IDM) ist dabei ein besonders kritischer Basisservice für nahezu alle anderen Sicherheitsdienste. Es schließt alle *Principals* (Personen, Organisationen, Systeme, Anwendungen, Komponenten, Geräte) in die Betrachtung mit ein. Nicht zu vergessen sind Infrastrukturdienste wie das Management von Sicherheitspolicies sowie statische und dynamische Rollen. Die Entwicklung und der Einsatz der Gerätetechnik stehen an vorderster Stelle in einer mobiler werdenden Umgebung. Es gibt inzwischen (siehe *Abbildung 2*) nahezu keinen medizinischen Prozess mehr, der ohne Medizintechnik auskommt. Die Palette der Beispiele reicht vom Rettungsfahrzeug über die Not-

fallbehandlung und die reguläre Versorgung im stationären oder ambulanten Bereich bis hin zu Nachsorge, häuslicher Pflege, Pflege im Heimbereich und Monitoring von Risikopatienten. Dass dabei in sehr vielen Fällen personenbezogene Daten in einer drahtlosen Umgebung sicher und vertrauenswürdig kommuniziert werden müssen, steht ebenfalls außer Frage [1], [2], [6]. Ein weiteres wichtiges Kriterium für die Akzeptanz ist auch die physische und mentale Sicherheit (*Safety*) [4].

5. Schlussfolgerungen

Der Übergang zu personenzentrierten Versorgungsprozessen erfordert offene, sichere, flexible, auf den Versorgenden und den zu Versorgenden zugeschnittene Anwendungen. Mobile Komponenten spielen eine immer größere Rolle. *Mobile Computing* zur Realisierung der Erreichbarkeit (z.B. Telekonsultationen), *Pervasive Computing* zur Realisierung der Ortsunabhängigkeit bei der Diensteanwendung (z.B. Telemedizin) und *Autonomous Computing* zur Realisierung selbst organisierender Systeme sind die Antwort auf einige wesentliche Fragen und Anforderungen, vor denen das heutige Gesundheits- und Sozialwesen steht [4]. Personal Health bzw. pHealth als personenbezogene Form von eHealth wird auf diesem Wege zu Mobile Health bzw. mHealth. Dies erfordert neben technischen auch rechtliche, ethische und soziale Rahmenbedingungen. Grundpfeiler jeder derartigen Entwicklung ist aber die Akzeptanz aller Betroffenen beim Einsatz der genannten Technologien, da jedes Plus an gewünschtem Zugang zu Gesundheitsdiensten auch oft mit einem Minus an Anonymität und Privatsphäre verbunden sein kann. Diese beiden Aspekte in einer sinnvollen Balance zu halten wird Aufgabe der Entwicklung und Standardisierung für die nächsten Jahre sein.

6. Literatur

- [1] BLOBEL, B., NORGALL, T., PHAROW, P., Weiterentwicklung von eHealth im Kontext des Personal Health Paradigmas, in: M. Löffler, A. Winter (Hrsg.), 51. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie GMDS 2006, Jütte-Messedruck Leipzig GmbH, Leipzig 2006.
- [2] PHAROW, P., BRUNNER, M., Zusammenwirken von Ethik, Moral, Schweigepflicht und Datenschutz in Zeiten zunehmender elektronischer Vernetzung, in: P. Schmücker, K.-H. Ellsäcker (Hrsg.), 12. Fachtagung Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS) 2007, Frotscher Druck, Darmstadt 2007.
- [3] PHAROW, P., BLOBEL, B., Von eHealth zu mHealth - Sicherheitsanforderungen in der mobilen Welt, in: H.-E. Wichmann, D. Nowak, A. Zapf (Hrsg.), Wissenschaftlicher Kongress Medizin und Gesellschaft. 52. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie GMDS 2007, Rheinware Verlag, Mönchengladbach, 2007.
- [4] BLOBEL, B., PHAROW, P., Sicheres und nachhaltiges eHealth, in: P. Schmücker, K.-H. Ellsäcker (Hrsg.), 12. Fachtagung Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS) 2007, Frotscher Druck, Darmstadt 2007.
- [5] PHAROW, P., STEINEBACH, M., BLOBEL, B., Dokumentensicherheit in multimedialen klinischen Informationssystemen, in: M. Löffler, A. Winter (Hrsg.), 51. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie GMDS 2006, Jütte-Messedruck Leipzig GmbH, Leipzig 2006.
- [6] PHAROW, P., BLOBEL, B., Probleme und Lösungsansätze der internationalen eHealth-Standardisierung, in: A. Jäckel (Hrsg.), Telemedizinführer Deutschland, 8. Ausgabe 2007, Minerva KG, Darmstadt 2006.
- [7] HOFMANN, C., ASCHENBRENNER, S., WEIGAND, C., Continuous Patient Monitoring and Data Analysis in Real Time with Wireless Sensors, 1. Internationale SENSATION - Konferenz, Basel, 2006.
- [8] ASCHENBRENNER, S., DOUNIAMA, C., Sensor System for Mobile, Continuous and Non-Invasive Blood Pressure Monitoring, 2. Internationale SENSATION - Konferenz, Kreta, 2007, <http://www.sensation-eu.org/>.