Workshop
Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

Einleitung

Jens Schwanke & Alexander Stahmann
jens.schwanke@med.uni-goettingen.de

www.mi.med.uni-goettingen.de

Inhalt

- Intention des Workshops
- Einführung
- Herausforderung
- Lösungsansätze

Intention

Workshop: Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

GMDS-Arbeitsgruppe: „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Leitung: Dr. Bernd Schütze (Telekom Healthcare) und Jens Schwanke (Universitätsmedizin GÖ)

Mit Beschluss der Beiratssitzung wurde die Arbeitsgruppe am 07.09.2014 von

„Datenschutz in Gesundheitsinformationssystemen“

in

„Datenschutz und IT-Sicherheit im Gesundheitswesen“

umbenannt.

Aufgabenbereiche(1/2)

- Einbringung und Kommentierung von Datenschutzfragen in Gesundheitspolitik und Recht

- Systematische Darstellung der Herausforderungen der Umsetzung von Datenschutzfragen sowie die Unterbreitung von Lösungsvorschlägen

Aufgabenbereiche(2/2)

- Fragen zu technischen Umsetzung bzgl. Datenschutzanforderungen

- Hilfestellungen bei
  - Organisation,
  - Strukturierung
  - und Integration

  von Datenschutz und Datensicherheit

Tätigkeitsbereich

Erarbeitung von Stellungnahmen

- Orientierungshilfe Krankenhausinformationssysteme (OH-KIS)
- §203 StGB - Problematik

Erarbeitung einer Empfehlung zur Auftrags-datenverarbeitung gemeinsam mit bvitg, GDD, BVD

Nächstes AG-Treffen

Das nächste Treffen der Arbeitsgruppe findet gemeinsam mit der AG Datenschutz der TMF am

Termin: **Mittwoch, 19. November 2014**

Ort: in der TMF Geschäftsstelle (Berlin)

statt.

Zielsetzung des Workshops(1/2)

Im Workshop sollen

- Herausforderungen
- und Lösungsansätze

zum Thema

- Datenschutz
- und Mobile Computing

im Gesundheitswesen vorgestellt und diskutiert werden.

Zielsetzung des Workshops(2/2)

Durch den Einsatz von Mobile Computing ergeben sich neue Anforderungen an den Datenschutz:

- Bring Your Own Device (BYOD)
- Mobile Device Management Software
- Automatische Datenspeicherung in der Cloud
  - icloud von Apple für iPhone
  - Google Drive für Android

Ergebnis des Workshops(1/2)

Erfassung neuer Anforderungen, Herausforderungen und Lösungsansätze an den Datenschutz aus Sicht verschiedener Personengruppen

- Datenschutzbeauftragte
- IT-Verantwortliche
- Mitarbeiter/Angestellt
- Personalrat/Betriebsrat

Ergebnis des Workshops(2/2)

- Gemeinsame Diskussion der Anforderungen, Herausforderungen und der möglichen Lösungsansätze.
- Abstimmung ob durch die Arbeitsgruppe eine Handlungsempfehlung für den Einsatz mobiler Geräte im Gesundheitswesen arbeitet werden soll.

Agenda des Workshops

1. Einleitungsvortrag zum Thema „Datenschutz und Mobile Computing im Gesundheitswesen“ / J. Schwanke
   Pause 5 Minuten
2. Mobile Security im Zusammenhang mit dem BSI Grundschutzkatalog / A. Stahmann
   Pause 5 Minuten
3. Organisatorische Anforderungen an Mobile Computing im Gesundheitswesen / B. Schütze
   Pause 5 Minuten
4. Abschlussdiskussion

Einführung

Workshop: Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

Mobile Computing – Was ist das?(1/2)

- Eine Google-Suchanfrage zu diesem Thema ergab 9.500.000 Ergebnisse

- Der Beitrag zu Mobile Computing auf der englischen Wikipedia wird diskutiert:

Mobile computing

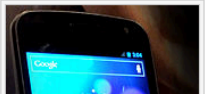
From Wikipedia, the free encyclopedia

It has been suggested that *Mobile Internet device* be merged into this article. (Discuss) *Proposed since June 2012.*

It has been suggested that *Mobile device* be merged into this article. (Discuss) *Proposed since June 2012.*

This article **needs attention from an expert in Technology or Computing**. Please add a *reason* or a *talk* parameter to this template to explain the issue with the article. WikiProject Technology or WikiProject Computing (or their Portals) may be able to help recruit an expert. *(May 2009)*

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.



Quelle: http://en.wikipedia.org/wiki/Mobile_computing

Mobile Computing – Was ist das?(2/2)

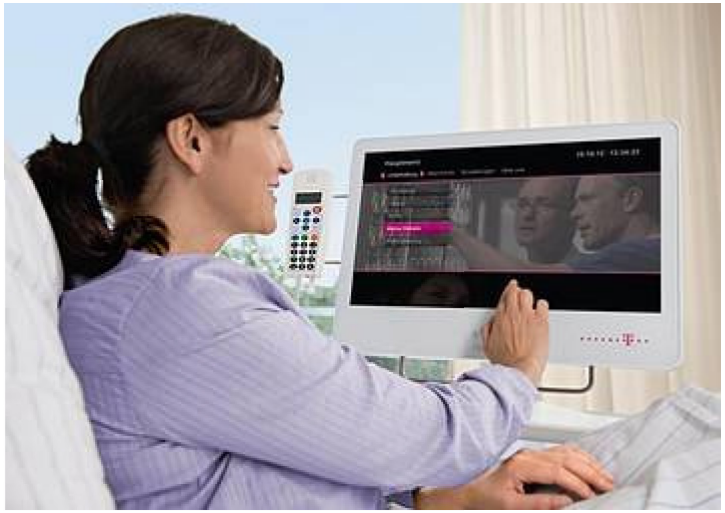
- Der Begriff fast die Nutzung der vielfältigen Geräte zusammen, die Menschen einsetzen um standort(un)abhängig Daten zu verarbeiten.
- Dabei wird oftmals eine (dauerhafte oder Adhoc) Datenverbindung benutzt um Daten mit Servern, anderen Mobilgeräten und/oder Sensoren auszutauschen.
- Die Geräte dienen in den meisten Fällen primär der Darstellung und sekundär der Eingabe von Daten.

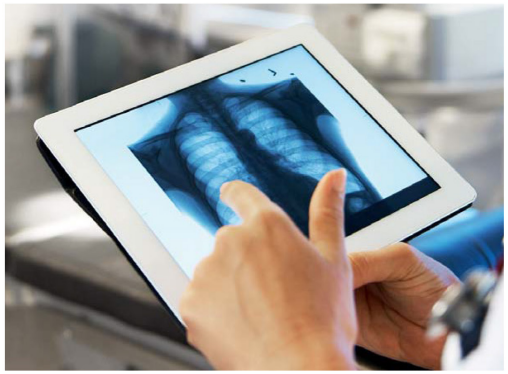
Entwicklung des Mobile Computing

- "PalmTX" by Stefano Palazzo - Own work. Licensed under Creative Commons Attribution-Share Alike 3.0 via Wikimedia Commons – http://commons.wikimedia.org/wiki/File:PalmTX.jpg#mediaviewer/File:PalmTX.jpg
- „IFA 2010 Internationale Funkausstellung Berlin 18“ von Bin im Garten - Eigenes Werk. Lizenziert unter Creative Commons Attribution-Share Alike 3.0 über Wikimedia Commons - http://commons.wikimedia.org/wiki/File:IFA_2010_Internationale_Funkausstellung_Berlin_18.JPG#mediaviewer/Datei:IFA_2010_Internationale_Funkausstellung_Berlin_18.JPG

Anwendungsgebiete mobiler Geräte im Gesundheitswesen(1/2)

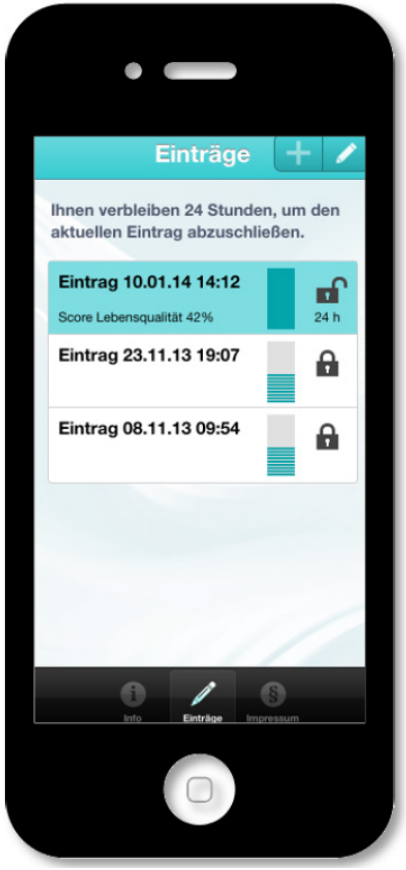
- Patientenentertainment
- Patientenbefragungen
- Befunddarstellung
- Dokumentation von Behandlungen
- Recherche
- Steuerung von Assistenz-systemen (AAL)





http://www.mcs-ag.com/MCSLABAPP/MCS_Lab_App.pdf
http://www.healthtechwire.de/deutsche-telekom-ag-t-systems/t-systems-zeigt-auf-der-conhit-it-loesungen-fuer-eine-schnellere-vernetzung-3307/

Anwendungsgebiete mobiler Geräte im Gesundheitswesen(2/2)



https://epic.hpi.uni-potsdam.de/Home/HanaOncolyzer

Herausforderung

Workshop: Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

Motivation – Apps im Gesundheitswesen (1/2)

Analysten gehen für den Gesundheitsbereich davon aus, dass sich der Weltmarkt für mobile Gesundheits-App-Services in der nahen Zukunft stark positiv entwickeln wird:

- Der größte Umsatz wird dabei weniger durch die App-Downloads erwartet,
- vielmehr sind die angebundenen Services und Geräte Treiber des Umsatzes.

Quellen:
[1] Compact: Durch die Decke. E-HEALTH-COM Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin. 2013;(2/2013):10.
[2] http://us.123rf.com/400wm/400/400/Krisdog/Krisdog1111/Krisdog111100051/11383880-a-mobile-phone-with-stethoscope-wrapped-round-it-problem-diagnosis-concept.jpg

Motivation – Apps im Gesundheitswesen (2/2)

- Der Einsatz von Smartphones und Tablets im privaten und beruflichen Umfeld hat in den letzten Jahren stark zugenommen.
- Im Gesundheitswesen wird diese Entwicklung durch mehrere Faktoren gebremst:

Hygiene	Abgrenzung zu med. Produkten
Schnittstellen	Datensicherheit

Datensicherheit(1/4)
Diebstahl

- Wie können mobile Endgeräte vor Diebstahl geschützt werden?
- Was passiert wenn ein Endgerät gestohlen wird:
  - Wie können die Daten vor Missbrauch geschützt werden?
  - Wie kann der Nutzungsbereich eingeschränkt werden?
  - Wie können die Endgeräte über Remotezugriff gelöscht bzw. zurückgesetzt werden?

Datensicherheit(2/4)
Zugriff

- Wie kann der Zugriff auf das Unternehmensnetzwerk geregelt und gesichert werden?
- Wie kann sichergestellt werden, dass ausgewählte Daten das Unternehmen nicht verlassen?
- Wie müssen Richtlinien gestaltet werden, dass alle Datenschutzrelevanten Aspekte berücksichtigt werden ohne den Mitarbeiter zusätzlich zu belasten?

Datensicherheit(3/4)
Kontrolle über Endgeräte

Wie kann das Endgerät kontrolliert werden, sodass Daten beispielsweise nicht mit der Cloud synchronisiert werden:

- Synchronisierung von Mails mit iCloud
- Speicherung von Dokumenten mittels Dropbox oder Google Drive
- Erkennung von Jailbreak
- Beschränkung der Zugriffsrechte von installierten Apps

Datensicherheit(4/4)
Trennung von geschäftlich und privat

- Durch den Einsatz von mobilen Endgeräten vermischt sich die Nutzung des Gerätes für
  - private und
  - berufliche

  Zwecke.
- Diese Herausforderung ist besser bekannt unter:
  - Bring Your Own Device
  - Corporate Owned, Personally Enabled

BYOD – Bring Your Own Device(1/2)

- BYOD bezeichnet die Nutzung von privaten Endgeräten (vor allem im mobilen Bereich) im geschäftliche Umfeld.
- Beispiele:
  - Abruf und Speicherung von dienstlichen Emails auf dem privaten Handy-
  - Entwicklung von Software auf privaten Laptops.
  - Zugang zum Intranet des Unternehmens vom privaten Tablet.
- BYOD-Richtlinien regeln meist die Nutzung von privaten Engeräten.

BYOD – Bring Your Own Device(2/3)
Vorteile

- Mehr Wahlfreiheit für die Mitarbeiter des Unternehmens
- Erreichbarkeit des Mitarbeiters auch außerhalb der Arbeitszeit
- Weniger Endgeräte für den Mitarbeiter
  und das Unternehmen muss den Mitarbeitern kein Endgerät zur Verfügung stellen

BYOD – Bring Your Own Device(2/3) *Nachteile*

- Unternehmen kann nur bedingt Einfluss auf das Endgerät nehmen
- Wirkt der Vereinheitlichung der Infrastruktur entgegen -> höhere Kosten für den Arbeitsgeber
- Ungelöste Probleme:
  - Haftungsfall
  - Sicherstellung des Datenschutzes (Verarbeitung von personenbezogenen Daten

COPE – Corporate Owned, Personally Enabled

- COPE, bedeutet die Bereitstellung eines (mobilen) Endgerätes durch das Unternehmen mit der Erlaubnis zur privaten Nutzung.
- Das Unternehmen kann hierdurch Richtlinien für die Geräte verbindlich festlegen.
- Nutzung von Mobile Device Management zur Umsetzung der Richtlinien verwenden.

Lösungsmöglichkeiten

Workshop: Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

Welche Lösungsmöglichkeiten existieren?

- Erstellung von Richtlinien oder Betriebsvereinbarungen zum Einsatz von mobilen Endgeräten
- Nutzung von Mobile Device Management zur technischen Umsetzung der Richtlinien
- Verbot zur Nutzung von mobilen Endgeräten

Richtlinien / Betriebsvereinbarungen

- Durch den Einsatz von Richtlinien können organisatorische Maßnahmen zum Einsatz von mobilen Endgeräten im Unternehmen getroffen werden.
- Diese umfassen u. a.
  - Einsatzzweck und die zu verarbeitenden Daten
  - Vereinbarungen zu BYOD
  - Verhaltensweise im Umgang mit dem mobilen Endgerät
  - Maßnahmen zur Sicherstellung der Datensicherheit

Mobile Device Management

- Software zur Umsetzung von Richtlinien und Betriebsvereinbarungen
- Ermöglicht Administratoren mobile Endgeräte zu verwalten:
  - Inventarisierung der Hardware
  - Softwareverteilung
  - Backup
  - Richtlinien über Eingabe von PIN und Password
  - Festlegung eines eignen/gesicherten App-Stores

Kontakt

Jens Schwanke

Universitätsmedizin Göttingen
Institut für Medizinische Informatik
Robert-Koch-Str. 40
37075 Göttingen

Tel.: +49 551 39-14240
Fax: +49 551 39-22493

Web: www.mi.med.uni-goettingen.de
E-Mail: jens.schwanke@med.uni-goettingen.de