mHealth und der TMF-Datenschutzleitfaden

TMF-Workshop „Mobile Medical Devices und Datenschutz“
Berlin, 10. Februar 2015

Univ.-Prof. Dr. Klaus Pommerening

Universitätsmedizin Mainz
+ TMF-AG Datenschutz

Gefördert vom
Bundesministerium
für Bildung
und Forschung

Überblick

A. Mobile medizinische Anwendungen und ihr Datenpotenzial

B. Architekturmodell für mobile medizinische Anwendungen

C. Der TMF-Datenschutzleitfaden

D. Vertrauensmodelle und IT-Sicherheit

Mobile medizinische Anwendungen

Echte Hilfen für „hilflose“ Personen vs. Selbstoptimierungsansätze

- Kontrolle der „Fitness“,
- Motivation zu gesundheitsbewusstem Verhalten,
- Überwachung des Gesundheitszustands(*),
- medizinische (und soziale) Unterstützung und Betreuung,
  z. B. Erinnerung an Tabletteneinnahme,
  Blutzucker-Protokoll.

Zunehmend mit Apps und Mobil-Geräten (Smart Phones, Smart Watches, Aktivitätstracker, Wearables),
→ entwickeln sich zu preisgünstigen de-facto-Standards.

Unerwünschte Nebenwirkungen:

- Eingriff in die informationelle Selbstbestimmung,
- erhebliches Gefährdung durch nicht vertrauenswürdige IT.

* z. B. gestern in SpOn: Der 24-Stunden-Kardiologe (Cardiogo)

Datenpotenzial mobiler medizinischer Anwendungen

Datenspeicherung zunehmend (fast ungefragt) in der „Cloud“:

- Gesundheitszustand, Fitness, Ernährung,
- Bewegungs- und Aktivitätsprofile,
- Sprachsteuerung über Cloud-Funktionen

Datensammlung in der Cloud bei globalem Provider (*personenbezogen*!)

- ermöglicht (vielleicht) Data Mining,
- in Ausnahmefällen evtl. sinnvolle epidemiologische Ergebnisse, **Cave:** Datenqualität, Verzerrungen, *p*-Wert-Schwemme!
- auf jeden Fall aber gezielte („personalisierte“) Werbung (nachts zweimal aufgestanden ⇒ Werbung für Kürbispräparat).
- „Spion am Handgelenk“ (c‘t 2015/3)

Die anfallenden Daten sind *Gesundheitsdaten*.
→ **besonders schutzbedürftig** (z.B. BDSG §3, Abs. 9)

Reidentifizierungsrisiko (RI-Risiko)

Mobile medizinische Anwendungen erzeugen hochdimensionale individuelle Datensätze:

- Gesundheitsdaten,
- sozioökonomische Daten,
- Daten zum Lebensstil und Verhaltensdaten.

„Externes" Wissen nimmt zu und ist immer leichter beschaffbar:

- soziale Netze und andere Internet-Aktivitäten (Bewegungsprofile, freiwillige Angaben über Tagesablauf, Medikamente, Suchanfragen, „intelligente" Stromzähler, …).
- *Schon die Uhrzeit einer einzelnen Arztvisite kann zur Identifizierung ausreichen*.

Anonymisierbarkeit dieser Daten illusorisch.

Verhinderung von Datenlecks illusorisch.

Reidentifizierungsrisiko durch Datenlecks, aber auch durch „erlaubte" Nutzung von Daten zu unerlaubten Zwecken (Insiderproblematik).

Schutz der Daten aus mobilen medizinischen Anwendungen?

Problembewusstsein bisher oft wenig ausgeprägt,
von Hype, Nutzenerwägungen und Machbarkeit
(und anglo-amerikanischem Rechtsverständnis) dominiert.

Hauptproblemkreise:

- Sicherheit der mobilen IT
- informationelle Selbstbestimmung bei der Datenerfassung und -speicherung
  (App-Rechte abklicken ist irreführend.)
- zentrale Datensammlung und -auswertung
  - leicht zugängliches Zusatzwissen mit unkontrollierbarem Umfang
- Freiwilligkeit und Tragweite einer Einwilligung?
  - Der Betroffene ist dem Provider ausgeliefert.
  - Recht auf Nichtwissen? Offenbarungspflicht gegenüber Versicherungen/ Arbeitgeber?

Schreckensszenarien

- Unbefugtes Abhören von Daten,
  - z. B. Ausspähen von Einbruchsmöglichkeiten in Wohnumgebung.
- Systemfehler bei automatisierten Entscheidungen (z. B. Alarm, *Cave*: Fehlalarmfalle).
  - Gerätestörung, Programmierfehler, Netzstörung.

Dazu kommen weniger spektakuläre Angriffsszenarien wie

- unbefugte Reidentifikation durch Insider (VIP-Problematik – Personen von öffentlichem Interesse oder aus dem Bekanntenkreis),
- invasive Werbung,
- Aufkündigung der Solidargemeinschaft durch Individualisierung von Versicherungsprämien.

Besonderheiten der Verarbeitung von mobilen medizinischen Daten

- Wenn das Projekt medizinisch motiviert ist, findet es im Behandlungs- oder im Forschungskontext statt.
  - Insoweit Parallelen zu anderer medizinischer Versorgung und Forschung.
  - Daten unterliegen der ärztlichen Schweigepflicht.
  - Tragweite der vorhandenen DS-Konzepte für Patientenakten und medizinische Forschung ist zu analysieren.

- Zugriffe auch durch „Bezugspersonen", Sozialstation, Notrufleitzentrale, „Sozialdienstleister", **Provider**
  - Trennung medizinischer und nichtmedizinischer Daten und Prozesse nur sehr schwer möglich.
  - Überschneidung mit Forschungskontext; Sekundärnutzung von Daten beginnt schon bei der einfachen Evaluation von Maßnahmen.

Analyse des Handlungsbedarfs zum Datenschutz in AAL-Umgebungen

Workshop der TMF im Juli 2010

Teilnehmer aus Praxis, Technik, MI, Datenschutz, Recht

Arbeitsgruppen Architektur, Prozesse, Organisation

Fazit der AG „Datenschutzgerechte Architektur“ (stark vereinfacht):

- Das TMF-Datenschutzkonzept deckt Datenspeicherung und -verwertung zu großen Teilen ab.
- Die Datenerfassung („Heimbereich“) erfordert zusätzliche Maßnahmen.

Übertragbarkeit von AAL-Szenarien auf mHealth-Szenarien („Gesundheits-Apps“)?

Die drei Bereiche der AAL-Architektur (modifiziert)

1

Heimbereich („zu Hause“) bzw. persönlicher Bereich

Geräte, Sensoren, Sensornetz, Mobil-Geräte, Tracking-Apps

2

Behandlungs- und Dienstleistungsbereich (patientennah)

- a: Behandlung, Patientenakte
- b: Notfalldienste
- c: Geräte-Service
- d: Customer Service

Übergang: **Gateway mit Kontrolle durch Betroffenen**

3

Sekundärnutzungs-bereich (patientenfern)

- a: Auswertung
- b: klinische Forschung
- c: epidemiologische Forschung

Übergang: Anonymisierung oder Identitätsmanagement; Datentreuhänder

Der TMF-Daten-schutzleitfaden

Datenschutzmaßnahmen für medizinische Forschungsverbünde.

Empfehlung durch die Konferenz der Datenschutzbeauftragten

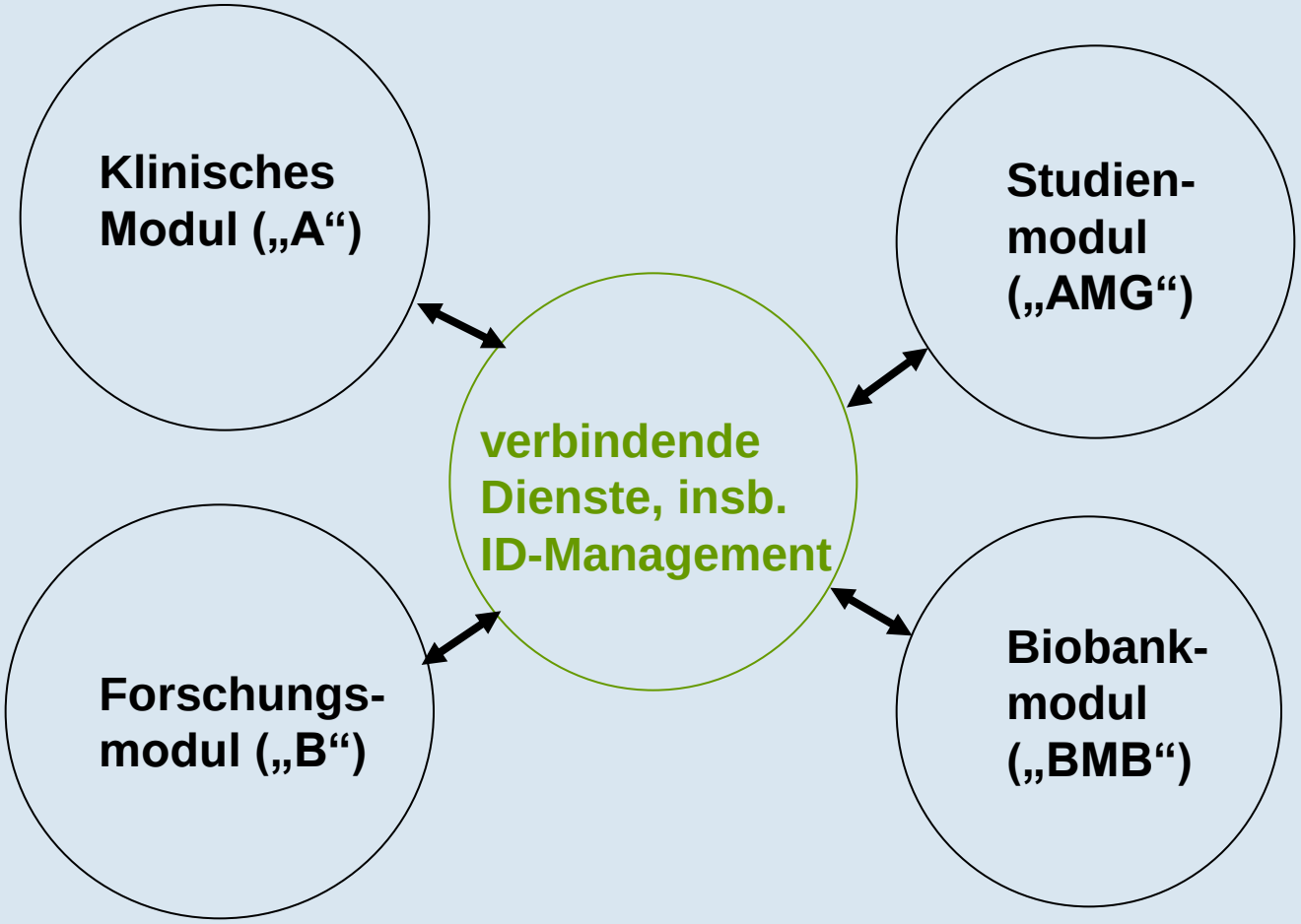
(für medizinische Forschungsprojekte)

In vielen Forschungsnetzen konkretisiert und implementiert.

Auf mHealth-Projekte nur begrenzt direkt anwendbar.

Viele Überlegungen und Prinzipien aber übertragbar.

Grundstruktur des TMF-Datenschutzleitfadens



Durch Modularisierung informationelle Gewaltenteilung

⇒ verschiedene Datenhoheit

⇒ verschiedene Pseudonyme

Stufen: DS-Konzepte für die einzelnen Bereiche („Module“)
DS-Konzept für das Gesamtszenario („Maximalmodell“)

Identitätsmanagement und Datentreuhänderschaft

- Wichtige Werkzeuge des Datenschutzes (nicht nur) im Forschungsbereich.

- Identitätsmanagement bedeutet
  - Verschleierung des Personenbezugs von Daten ohne befugte Nutzung und korrekte Zuordnung zu behindern,
  - insb. Ersetzen identifizierender Daten durch Pseudonyme (unterschiedliche Pseudonyme in unterschiedlichen Modulen oder Teilprojekten).

- Datentreuhänderschaft bedeutet
  - organisatorische Absicherung des Identitätsmanagements, z. B. durch vertrauenswürdige Verwaltung der Zuordnung von Pseudonymen.

Tragweite des TMF-Datenschutzleitfadens für AAL-Szenarien

Deckt den Bereich 2 (Dienstleistung und Behandlung) ab, soweit medizinischer Behandlungskontext gegeben.

Deckt den Bereich 3 (Sekundärnutzung) voll ab.

- ↳ Zusatzüberlegungen nötig zur Pseudonymisierung von Daten, die direkt aus dem Heimbereich kommen (→ Identitätsmanagement im Gateway).

Deckt den Übergang von Bereich 2 in Bereich 3 ab.

Deckt den Bereich 1 (Heimbereich) nicht ab.

Deckt Datenschutzanforderungen für nichtmedizinische Akteure (Rettungsdienst, Pflegedienst, …) nur oberflächlich ab.

Leitfaden der TMF zur Aufklärung und Einwilligung für alle Bereiche nutzbar.

Hinweis: Eine „Datenschutzerklärung" ist in der Regel keine gültige Einwilligungserklärung (Haftungsausschluss statt informierte Einwilligung).

Tragweite des TMF-Datenschutzleitfadens für mHealth-Szenarien

Direkt übertragbar, soweit die Zweckbestimmung „medizinische Forschung“ heißt (auch im weiteren Sinn).

Zweckbestimmung „personalisierte Werbung“ auf keinen Fall abgedeckt.

Übertragbare Prinzipien:

- Gesundheitsdaten: Personenbezug nur im Behandlungskontext
  - außerhalb: Datennutzung nur mit gesetzlicher Regelung oder (wirksam!) anonymisiert/ pseudonymisiert
- informationelle Gewaltenteilung
- tragfähige informierte Einwilligung
- Scientific Use, kein Public Use
  - Keine Freigabe von Datensammlungen (Public Use) wegen des unkontrollierbaren RI-Risikos

Weitere Datenschutz-Anforderungen für Daten mobiler medizinischer Anwendungen

- Scientific Use nur unter kontrollierten Bedingungen („ordentlich aufgesetzte“ Projekte, spezifische Exportfilter)
  - siehe TMF-Datenschutzleitfaden
  - mit verbindlichem organisatorischem Rahmen, insb. Verbot von RI-Versuchen;
  - z. B. Ethikvotum,
  - z. B. konsentiertes Datenschutzkonzept,
  - z. B. Audit-Maßnahmen.
- Datenübertragung nur nach Erforderlichkeit –
  - viele Daten nur „zu Hause“ (lokal) benötigt.
- Datenspeicherung nur nach Erforderlichkeit –
  - viele Daten nur einmal benötigt.
  - Cloud-Speicherung nicht erforderlich.

Vertrauensmodell und IT-Sicherheit

- Globale (anonyme) Dienstleister sind nicht vertrauenswürdig,
  - meist undurchsichtige Einwilligungsregelungen.
  - Seit überall lokaler Speicherplatz im Überfluss vorhanden ist, wird alles in die Cloud gezwungen → keine Erforderlichkeit.
    Die Cloud ist nicht vertrauenswürdig.
- Die globale PKI* ist nicht vertrauenswürdig – dem Endnutzer werden Hunderte unbekannter Root-Zertifikate untergeschoben.
- Mobile Endgeräte sind nicht vertrauenswürdig – sie stehen unter Fremdkontrolle, sind enteignet (s. App-Rechte).
  - IT-Sicherheit typischerweise miserabel.
  - Health-Device-Profile (HDP) verlangt nur Schutz vor versehentlicher Manipulation.
- Sicherheitslücken („Hintertüren“) werden absichtlich eingebaut (ins Netz, in die PKI, in die Endgeräte).

Auf einem unsicheren Gerät oder unsicherer Infrastruktur kann keine sichere App laufen.

* Public Key Infrastructure

Anforderungen an IT-Sicherheit im mHealth-Bereich

Grundforderung: *Alle Objekte* (Sensoren, Mobilgeräte, Server, Datennutzer) im Netz *brauchen starke wechselseitige Authentisierung sowie Vertraulichkeit und Integrität der Kommunikation*
(Sicherheit vor Abhören und Manipulation).

- Das geht mit angemessenem Schutzniveau nur auf Basis einer vertrauenswürdigen PKI und mit vertrauenswürdigen Endgeräten.
- Passwortschutz und verschlüsselte Datenübertragung wichtig, aber allein unzureichend.

Absicherung der erlaubten Datenzugriffe durch starke Authentisierung und Token,

- muss für Angehörige als IT-Laien verständlich sein,
- muss auch Fernwartungszugänge schützen.

Fazit

- mHealth-Daten dürfen nur über ein Gateway mit Kontroll-möglichkeiten durch den Betroffenen nach außen gelangen, und nur in den medizinischen Bereich (Behandlung, Forschung).
- Der TMF-Datenschutzleitfaden ist auch für zentrale Speicherung oder Sekundärnutzung von mHealth-Daten angemessen, soweit diese im Bereich der medizinischen Forschung stattfindet.
- Für Sekundärnutzung (Forschungszusammenhang) sind wegen des hohen RI-Risikos der Nutzdaten zusätzliche organisatorische Maßnahmen und Nutzungsbeschränkungen zu definieren (scientific use).
  (*Projektspezifisch*. *Konzepte existieren: TMF-DS-Leitfaden*.)
- In einer *idealen Welt* mit konsequenter IT-Sicherheit lassen sich sichere Szenarien für mobile medizinische Anwendungen konstruieren.
  (*In der realen Welt bis auf weiteres nicht*. *Missstände müssen abgebaut werden.*)

Fazit (Forts.)

Gesundheitsdaten dürfen nicht gesammelt werden

außer beim Arzt im Behandlungszusammenhang
oder unter der Datenhoheit des Betroffenen
oder im Rahmen von medizinischen Forschungsprojekten/ Studien,
die dem TMF-Datenschutzleitfaden folgen.

Bei Primärnutzung (Behandlungskontext) abwägen zwischen Nutzen und Risiko.

Für Prävention gibt es wirksamere Maßnahmen als die globale personenbezogene Datensammlung.

Diese kann einen Zusatznutzen bringen,

Verhältnismäßigkeit ist problematisch.

Cloud-Techniken sind (nur) mit Einschränkungen zulässig (siehe cloud4health-Projekt).