Datenschutz von Daten aus Ambient Assisted Living (AAL) Umgebungen

Thilo Weichert, Leiter des ULD

TMF-Workshop

Technologie- und Medienplattform für die vernetzte medizinische Forschung e.V.

Berlin, 26.07.2010

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Hilfsbedarfe, Datenflüsse und Rollen
- Verfassungsrechtliche Grundlagen
- Gesetzliche Grundlagen
- Einwilligung
- Betroffenenrechte und Verantwortlichkeiten
- Medizinische Besonderheiten
- Technisch-organisatorische Maßnahmen
- Forderungen und Schlussfolgerungen

Hilfsbedarfe

- Alter
- Demenz, geistige Behinderung
- Körperliche Behinderung
- Sonstige Pflegebedürftigkeit, z.B. Krankheit, Rehabilitation
- Unterstützung im Alltag

- Tägliche Verrichtungen, Komfort
- Kommunikationserleichterung
- Verbesserung der Informationslage f. Betroffene u. Helfer
- Notfallhilfe (vor Ort, automatisches Fernwirken)

Datenflüsse

(von innen nach außen)

- Datenerhebung in Wohnung, am Körper
- Verfügung durch Betroffenen
- Verfügung durch Freund/Eltern/Familie
- Externe individuelle Dienstleistung
- Offenes Notfallmanagement und tägliche Begleitung
- Einbeziehung von Pflegeeinrichtungen/Krankenkassen u.Ä.
- Sonstige Bedarfsträger: Statistik, Kostenträger (Krankenkassen, Versicherungen), Sicherheitsbehörden, Forschung, IT-Anbieter

Rollen beim AAL

- Betroffener als Patient, Klient, Kunde, Nutzer, Mensch
- Privater Dritter (Nachbar, Vermieter, Familienangehöriger)
- IT-Infrastruktur-Anbieter (Acces, Content, Service)
- Medizinische und sonstige Hilfsanbieter (Arzt, Krankenhaus, Pflegedienst...)
- Mitarbeitende von IT- und Hilfsanbieter
- Öffentliche Verwaltung (110, 112, Soziales, Medizin, Datenschutz)
- Forschende
- Interessengruppen
- Öffentlichkeit

Verfassungsrechtliche Grundlagen I

- Art. 2 II 1 GG: Jeder hat das Recht auf Leben und körperliche Unversehrtheit
- Art. 3 III 2 GG: Niemand darf wegen seiner Behinderung benachteiligt werden
- Art. 5 GG: Informations-, Meinungs- und Pressefreiheit
- Art. 6 GG: Schutz von Ehe und Familie
- Art. 10 GG: Telekommunikationsgeheimnis
- Art. 12 GG: Berufsfreiheit (Vertraulichkeit bei Berufsausübung, Patienten- und Sozialgeheimnis)
- Art. 13 GG: Unverletzlichkeit der Wohnung

Verfassungsrechtliche Grundlagen II

Allgemeines Persönlichkeitsrecht nach Art. 2 I iVm 1 I GG (Menschenwürde, Autonomie)

- Grundrecht auf informationelle Selbstbestimmung
- Schutz der Privatsphäre, insbes. Kernbereich persönlicher Lebensgestaltung, right to be let alone
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme
- Verbot von Persönlichkeitsprofil, Vorratsdatenverarbeitung, Rundumüberwachung
- Datensparsamkeit, Transparenz, Wahlfreiheit

Analog: Europäische Grundrechtecharta (insbes. Art. 8)

Gesetzliche Grundlagen

- Ärztliche Berufsordnung, § 203 StGB, MedizinprodukteG
  EU-Datenschutzrichtlinie, ePrivacy-Directive
  Bundesdatenschutzgesetz (BDSG), LDSG, SGB, SpezialR
  Telemediengesetz (TMG), TelekommunikationsG (TKG)
- Einwilligung § 4a BDSG (incl. informed consent) od.
- gesetzliche Grundlage (§§ 28 I Nr. 1, 3 IX, 28 VI-IX BDSG):
  Schutz lebenswichtiger Interessen, Gesundheitsvorsorge, medizinische Diagnostik, Gesundheitsversorgung, Behandlung, Verwaltung von Gesundheitsdiensten
- Verbot automatisierter Entscheidungen § 6a BDSG

7 goldene Regeln des Datenschutzes (nach Bizer)

1. **Einwilligung**
   Eine Einwilligung ist nur dann wirksam, wenn der Betroffene ausreichend informiert worden ist und seine Einwilligung freiwillig erteilt hat.
2. **Zweckbindungsprinzip**
   Personen bezogene Daten dürfen nur für den explizierten Zweck verwendet werden.
3. **Rechtmäßigkeit**
   Jede Datenverarbeitung mit Personenbezug bedarf einer rechtlichen Grundlage, entweder als Gesetz, Vertrag oder als betriebliche Regelung.
4. **Erforderlichkeit und Datensparsamkeit**
   Die Datenverarbeitung ist auf den für den Erhebungszweck notwendigen Umfang zu begrenzen, insbesondere im Hinblick auf Menge und Art der verarbeiteten Daten. Sie umfasst auch Löschung von Teildaten, sobald diese nicht mehr benötigt werden.
5. **Transparenz und Betroffenenrechte**
   Erhebung und Verarbeitung personenbezogener Daten muss gegenüber Betroffenen transparent sein. Dies schließt Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte ein.
6. **Datensicherheit**
   Datenschutz ist nur dann gewährleistet, wenn personenbezogene Daten sicher verarbeitet werden.
7. **Kontrolle**
   Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen.

Einwilligung I

Jede Einwilligung muss **freiwillig**, **bestimmt** und **informiert** erfolgen

- Freiwillig = frei von (innerem und äußerem) Zwang:
  - z.B. fraglich im Bereich der öffentlichen Leistungserbringung, im Krankenversicherungsrecht und in Abhängigkeitsverhältnissen, da bei Nichteinwilligung ggf. die Leistung nicht bewilligt wird oder die Befürchtung besteht, nicht die optimale Leistung zu erhalten (Behandlungsverhältnis, Pflegeverhältnis)
  - Folgen der Nichtteilnahme? (Koppelungsverbot)
  - Technikzwang?
  - Widerruflichkeit

Einwilligung II

- Bestimmt = erkennbar, was mit den personenbezogenen Daten geschieht
  - Problem bei komplexen, schnell variablen und außerhalb des Herrschaftsbereichs liegenden Systemen
  - Unbewusste, unbemerkte Erhebung der Daten?
  - Einflussmöglichkeiten (z.B. bei Besuch)?
  - Einsichtnahme in das System?
- Informiert = Information über die Daten, Stellen und Zwecke und Folgen einer Verweigerung der Einwilligung
  - Nutzergruppe + Verständlichkeit
  - Technikzwang?
  - Komplexität der Anwendung
  - „laufende“ Informiertheit

= Kein Alleinlassen mit der Technik: Datenflüsse und ihre Steuerbarkeit müssen den Nutzern transparent gemacht werden (Bringschuld!)

= Keine „Bevormundung“ oder „Entmündigung“ der Nutzer

= Höchstmaß an Selbstbestimmung und Wahlmöglichkeit der Betroffenen nötig

= Durch die Einwilligung muss tatsächlich Einfluss auf den Umgang mit den eigenen Daten ausgeübt werden können

Einwilligung III

Lösungsansätze

- Abgestufte Einwilligungen
  - Ausschlussmöglichkeit hinsichtlich verschiedener Datenverarbeitungszwecke (Modulare Angebote z.B. bzgl. Sicherheit, Gesundheit, Soziales)
  - Ausschlussmöglichkeit von Empfängern
  - Ausschlussmöglichkeit hins. Umfang und Art der Datenerhebung
  - Möglichkeit des zeitliches Aussetzens der Anwendung
  - Delegation/Patenschaft/Treuhänderschaft?
- Kein Alleinlassen mit der Technik: Datenflüsse und ihre Steuerbarkeit müssen den Nutzern aktiv transparent und verständlich gemacht werden
- Laufende Information über Veränderungen
- Keine Nachteile in der Betreuung, wenn auf AAL-Technik verzichtet werden möchte

Betroffenenrechte

- § 4 III Information über Stelle, Zweck und Empfänger
- § 34 BDSG Auskunft, Einsicht
- § 33 BDSG Benachrichtigung
- § 42a BDSG Informationspflicht bei Zwischenfällen
- § 35 I BDSG Berichtigung
- § 35 II BDSG Löschung (u.a. bei Nichtnutzung, auf Wunsch, bei Tod)
- § 35 III BDSG Sperrung
- § 7 BDSG, §§ 823 ff. BGB Schadensersatzanspruch
- § 6 BDSG Unabdingbarkeit
- § 38 BDSG Anrufung Datenschutzkontrolle
- Anrufung Ärztekammer, allgemeiner Rechtsschutz

Verantwortlichkeiten

- Datenschutzrechtliche Verantwortlichkeiten müssen festgelegt werden
- § 3 VII BDSG: Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt
- Tatsächliche Einflussmöglichkeiten notwendig
  - Nutzer?
  - Hersteller der AAL-Anwendung?
  - Betreiber der AAL-Anwendung?
  - Sog. Paten (Freund/Arzt/Krankenhaus) auf gesetzlicher, vertraglicher od. gewillkürter Grundlage?

Berufliche Schweigepflicht (Patientengeheimnis)

Rechtliche Grundlage: Standesrecht, § 203 StGB

Gilt für Ärzte, Kliniken, Berufspsychologen und andere Heilberufe sowie Mitarbeiter

> Keine Aufzeichnung von Verbindungsdaten

- bei jeder Art von elektronischer Kommunikation: Keine Rückschlüsse auf die Identität der Kontaktpersonen (Patienten).
- Grund: Nur die Berufsgeheimnisträger selbst sind berechtigt, solche Daten zu speichern. Es darf also keine automatische Speicherung von E-Mail-Adressen der Patienten in Systemen geben, auf die von anderen als den Ärzten und sonstigen Schweigepflichtigen zugegriffen werden kann.
- Wo sich eine solche Speicherung nicht vermeiden lässt, gilt: Es muss eine ausdrücklich Einwilligung bzw. Entbindung von der Schweigepflicht stattfinden.

> Grds. keine Einschaltung externer Dritter (Dienstleister) ohne Einwilligung der Betroffenen einschalten, soweit personenbezogene Kenntnisnahme nicht ausgeschlossen (z.B. durch Verschlüsselung der Daten)

Medizinische Dokumentationspflichten

- Im Rahmen des Behandlungszusammenhangs in Ausübung des Berufs gemachten Feststellungen und getroffenen Maßnahmen
- Vertragliche Nebenpflicht aus Behandlungsvertrag
- Einblickrecht des Patienten
- Evtl. Beweislastumkehr zugunsten des Patienten
- Bei digitalen Dokumenten Sicherung von Unverfälschtheit und Authentizität notwendig

Fernbehandlungsverbot

- Nach § 7 Abs. 3 der Berufsmusterordnung der Ärzte (BMO-Ä) ist es Ärzten verboten, „individuelle ärztliche Behandlung, insbesondere auch Beratung, weder ausschließlich brieflich noch in Zeitungen oder Zeitschriften noch ausschließlich über Kommunikationsmedien oder Computerkommunikationsnetze“ durchzuführen
- Entscheidend ist, dass die Behandlung nicht ausschließlich durch die o. g. (unpersönlichen) Kommunikationswege erfolgt
- Es muss gewährleistet sein, dass dem Patienten ausreichende Möglichkeiten einer persönlichen Arzt-Patient-Beziehung verbleiben

Technisch-organisatorische Maßnahmen

§ 9 BDSG mit Anhang

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Datenoder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“

Schutzziele

- Verfügbarkeit Maßnahme: Redundanz
- Integrität Maßnahme: Hash-Wert-Vergleiche
- Vertraulichkeit M.: Verschlüsselung, Abschottung, Rollentrennung
- Transparenz M.: Dokumentation, Protokollierung, Unterrichtung, Auskunft
- Revisionsfähigkeit M.: Dokumentation, Protokollierung
- Nichtverkettbarkeit M.: Rollen- und Strukturkonzept
- Intervenierbarkeit M.: Einrichtung eines Single-Point-of Contact, Interventionsmanagement, Wahloptionen, Treuhänderverfahren

AAL-Problemkonstellationen (nach Rost)

- *Verfügbarkeit / Vertraulichkeit / Integrität*: Wem gehören die Daten sowie die technische Infrastruktur? Wer bekommt in welcher Form wie lange auf welche Systeme, Applikationen, Daten Zugriff? Wie lange werden welche Daten (roh, aggregiert, anonymisiert?) wo zu welchem Zweck (Generierung von Referenzwerten für eine „normale Lebensführung“) wie lange unter welchen Bedingungen gespeichert? Wie wird die Qualität der Daten gesichert?
- *Transparenz*: Mit welchen Instrumenten können Betreiber und Betroffene die laufenden Daten, Komponenten, Systeme überprüfen?
- *Intervenierbarkeit*: Mit welchen Instrumenten können Betroffene und Betreiber in die laufenden Systeme eingreifen, Trigger konfigurieren, Daten korrigieren, löschen, Prozesse bzw. Systeme stoppen?
- *Verkettbarkeit*: Mit welchen Prozessen lässt sich seitens der Betreiber, der Betroffenen und der Aufsichtsinstanzen prüfen, dass die AAL-DV jeweils Zweck-konform stattfindet?
- Wie lässt sich phasenweise Unbeobachtbarkeit durch den Betroffenen herstellen (Sexualität)?
- Interaktion mit unbeteiligten Dritten (diese haben keine Mögl. zur Einwilligung)
- Gestaltung des gesundheitlichen Graubereichs des gesellschaftlich akzeptierten Drogenkonsums (ungesundes Essen, Bewegungsarmut, riskante Freizeitgest.)?
- Abfluss von Daten an Versicherung, Forschungsinstitute, Sicherheitsbehörden.

Forderungen

2003: Gemeinsames Forschungszentrum der EU-Kommission

- Keine Bevormundung und Entmündigung
- Datenvermeidung u. Datensparsamkeit
- Datenschutzfreundliche Einstellungen (Privacy by Design)
- Assistenz für Betroffene bei AAL
- Verfügbarkeit analoger Alternativhilfsangebote

- Beherrschbarkeit durch Betroffene
- Zertifizierung

  2001: § 9a BDSG Auditplatzhalterregelung

  seit 2000: §§ 4 II, 43 II LDSG SH: Zertifizierung von Produkten, Dienstleistungen und Verfahren m. Gütesiegel u. Audit

  Koalition 2009: Stiftung Datenschutz

Datenschutzhindernisse

- Bisher unzureichende Integration des Datenschutzes in IT-Produkte und -Strukturen
- Technikkritische Einstellung v. Anwender, v.a. in der Ärzteschaft
- Mängel bei Medienkompetenz der Betroffenen
- Gutmenschselbstverständnis bei Hilfedienstleistern
- Ökonomische Zweitverwertungsinteressen an den Daten

Schlussfolgerungen

- AAL kann Informationsbasis erhöhen, Selbständigkeit wahren, Kommunikation verbessern, technisch unterstützen, schnelle Hilfe erleichtern, Kosten einsparen
- Standardisierungen sind nötig (Schutzprofile)
- Zertifizierung von Produkten und Dienstleistungen ist förderlich
- Einführung von AAL modular und sukzessiv
- Einbindung aller Interessengruppen (Betroffene, Hilfeleister, IT, Datenschutz, Kostenträger)
- Technikhilfe kann menschliche Zuwendung nicht ersetzen

Datenschutz von Daten aus Ambient Assisted Living (AAL) Umgebungen

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de