Datenschutzanforderungen in AAL-Szenarien

Klaus Pommerening

1. Besonderheiten der Datenverarbeitung in AAL-Szenarien

Medizinische AAL-Projekte finden in einem Behandlungs- und Pflegezusammenhang statt, manchmal auch in einem Forschungszusammenhang. Insoweit bestehen Parallelen zu anderen Szenarien der medizinischen Versorgung und Forschung. Datenschutzkonzepte, die dort schon erstellt wurden, sind auf ihre Übertragbarkeit zu prüfen. Das soll hier für das TMF-Datenschutzkonzept [genDS] skizziert werden; natürlich sind auch die Datenschutz-Überlegungen zur Gesundheitstelematik relevant, soweit sie bisher schon publiziert wurden.

Drei Besonderheiten sind typisch für AAL-Szenarien: Erstens entstehen hochdimensionale Datensätze, die ein hohes Reidentifizierungsrisiko mit sich bringen. Die Daten können eine lückenlose Überwachung des Gesundheitszustands durch Telemonitoring abbilden, sie umfassen umfangreiche Informationen über das Alltagsleben, das Verhalten und den Lebensstil des Betroffenen. Externes Zusatzwissen, das zu einer Reidentifizierung von Datensätzen führen kann, ist leicht zu gewinnen: Persönliche Beobachtungen, Informationen aus sozialen Netzen und Lokalisierungs- oder Ortungsdaten erlauben die Gewinnung von Bewegungs- und Verhaltensprofilen, die für einen Abgleich geeignet sind – Wann hat die Person das Haus verlassen? Wann ist der Sozialdienst gekommen? Wann hat die Person gegessen? Was hat sie im Internet recherchiert? Solche Daten sind leichter zu gewinnen als genetische Fingerabdrücke. Auch sonst ist der Vergleich mit genetischen Daten durchaus angebracht: Während deren Aussagekraft immer mehr angezweifelt wird, können AAL-Daten sehr direkt interpretierbare vertrauliche Informationen enthüllen, z. B. zum Sexualverhalten.

Zweitens treten in AAL-Szenarien Akteure auf, die sonst im Behandlungszusammenhang gar keine oder nur eine periphere Rolle spielen: Bezugs- oder Vertrauenspersonen des Betroffenen, die Sozialstation mit ihren Mitarbeitern, die Notrufleitzentrale, Not- und Rettungsdienste, aber auch andere Sozialdienstleister bis hin zur Essensversorgung. Unter Bezugs- und Vertauenspersonen kann man sich nahe Verwandte, Nachbarn, Freunde, aber durchaus auch Dienstleister vorstellen. Weitere Akteure sind Gerätehersteller und Betreiber eines Sensornetzes, die durchaus oft Zugriffe auf Geräte und Daten benötigen, sowie Heimleitung oder Vermieter, die die Infrastruktur bereitstellen, und schließlich Telekommunikationsdienstleister.

Als Drittes besteht bei automatisierter Auswertung von Sensordaten und bei der Erzeugung geeigneter Reaktionen wie Alarme oder Trigger ein erheblicher Eingriff in die informationelle Selbstbestimmung sowie ein erhebliches Risiko durch Systemfehler; diese Aspekte werden in diesem Abschnitt aber nicht weiter diskutiert. Ebenfalls nicht weiter diskutiert wird hier die Frage, wie weit eine Einwilligung durch mehr oder weniger hilfebedürftige Personen in einem AAL-Szenario als freiwillig und unbeeinflusst gelten kann.

Es gibt große Überschneidungsbereiche von AAL-Szenarien mit anderen Bereichen. Medizinische AAL-Projekte als Ansätze zur individualisierten Versorgung finden zunächst im Behandlungszusammenhang statt, reichen aber über den Pflegezusammenhang auch weit in

nichtmedizinische Bereiche hinein, insbesondere bei der Nutzung „intelligenter“ Wohntechnik. Auch die Überschneidung mit dem Forschungskontext ist erheblich, denn dieser beginnt bereits bei jeder Sekundärnutzung von Daten, von der einfachen Evaluation von Maßnahmen bis hin zu langfristig angelegten Forschungsprojekten, die unverzichtbar zur Sicherung der Behandlungsqualität und grundlegend für den medizinischen Fortschritt sind.

2. Pseudonymisierungsschemata

Wesentliche Methoden für den Datenschutz bei umfangreichen, insbesondere langfristigen, Datensammlungen und -auswertungen sind Anonymisierung und Pseudonymisierung. Das generische Datenschutzkonzept der TMF beschreibt zwei Pseudonymisierungsschemata, die allgemeine Gültigkeit haben:

- Pseudonymisierungsschema A für einen einrichtungsübergreifenden Behandlungszusammenhang; es sieht eine pseudonyme zentrale Datenspeicherung vor, gestattet aber einen personenbezogenen Zugriff für behandelnde Ärzte und gegebenenfalls Pflegepersonal.
- Pseudonymisierungsschema B für einen allgemeinen Forschungskontext; hier sind sowohl die zentrale Speicherung als auch Datenzugriffe pseudonym.

3. Anwendungsfälle

Anhand einiger Anwendungsszenarien sollen die Datenschutzanforderungen an AAL-Projekte und die Anwendbarkeit der Pseudonymisierungsschemata illustriert werden.

Anwendungsfall 1: Direkte Unterstützung von Körperfunktionen

Beispiele hierfür sind Herzschrittmacher, Hörimplantate, Sehchips. Hier besteht zunächst keine unmittelbare Notwendigkeit für eine Datenübertragung oder -speicherung. Dennoch kann zur Funktionsüberprüfung oder zur Fernwartung eine Online-Anbindung erforderlich sein. Das impliziert sofort hohe Anforderungen an die IT-Sicherheit (s. u.). Falls Daten aus den Geräten in einer Patientenakte gespeichert werden sollen, findet Gewinnung und Verarbeitung im direkten Behandlungszusammenhang statt und passt in das Pseudonymisierungsschema A. Eine Nutzbarkeit für spätere Forschungszwecke bleibt dabei gewahrt, sofern eine entsprechende Einwilligung vorliegt.

Anwendungsfall 2: Selbsteingabe von Messdaten

Hier liest der Patient die Werte selbst ab und gibt sie über ein Webformular in eine Datenbank auf einem Server ein, auf die ein Arzt oder Pflegepersonal zugreifen kann. Hier ist die Datenqualität möglicherweise problematisch; die IT-Sicherheit aber durch die üblichen Verfahren der sicheren Kommunikation im Internet zu gewährleisten; die Anforderungen der starken Authentisierung zwischen Client und Server sowie der vertraulichen Übertragung werden durch Mechanismen wie SSL oder VPN gesichert. Die zentrale Datenspeicherung wird durch das Pseudonymisierungsschema A abgedeckt.

Anwendungsfall 3: Ständige Überwachung von Körperparametern

Beispiele hierfür sind Blutdruck, Zuckerwert, Atmung. Die Daten können lokal aufgezeichnet und dabei zu bestimmten Zeitpunkten regelmäßig per Datenträger oder online übertragen werden, oder das Gerät ist ständig online. Die Datenqualität ist gegenüber Fall 2 signifikant erhöht, auch die Bequemlichkeit für den Betroffenen. Sehr problematisch ist aber die Sicherheitslage durch die Online-Anbindung, selbst wenn die Übertragung noch durch ein Gateway kanalisiert wird. Ansonsten kann die zentrale Datenspeicherung wieder nach dem Pseudonymisierungsschema A abgewickelt werden, wobei zur richtigen Zuordnung der pseudonym übertragenen Daten evtl. ein Anwendungsserver zwischengeschaltet werden muss, was im Schema A bisher nicht vorgesehen ist.

Anwendungsfall 4: MPG-Studie oder andere klinische Studie

Hier werden Wirksamkeit und Nutzen des Geräts oder eines Therapieverfahrens, das Daten des Geräts verwendet, überprüft. Ziel kann etwa die Zulassung sein. Die Regularien für klinische Studien nach MPG, AMG und GCP verlangen eine sorgfältige Dokumentation und eine Archivierung der für die Studie verwendeten Daten. Das Pseudonymisierungsschema A (in leicht abgewandelter Form) deckt diesen Anwendungsfall ab; die Abwandlung bezieht sich auf die im AMG geregelte Verwendung von Pseudonymen und wird in der revidierten Version des TMF-Datenschutzkonzepts (in Arbeit) beschrieben.

Anwendungsfall 5: Benchmarking

Benchmarking dient der medizinischen Qualitätssicherung durch einrichtungsübergreifenden Behandlungsvergleich. Hierbei kann evtl. auch eine längerfristige Datensammlung und -auswertung erforderlich sein. Werden Behandlungs- und Messdaten ohne zusätzliche externe Speicherung direkt ausgewertet, kann dies nach Pseudonymisierungsschema A geschehen. Müssen die Daten einrichtungsübergreifend längerfristig, aber ohne direkte Rückwirkung auf den einzelnen Behandlungsfall, gespeichert werden, sollte dies dem Pseudonymisierungsschema B folgen.

Anwendungsfall 6: Epidemiologische Studie

Hier werden typischerweise Daten aus verschiedenen Quellen langfristig zusammengeführt und gespeichert mit dem Ziel, Behandlungserfolge, Spätfolgen, Lebensqualität über größere Zeiträume auszuwerten. Dies ist der typische Anwendungsfall für das Pseudonymisierungsschema B. Zu bedenken ist hierbei, dass Daten in eher reduziertem Umfang, dafür besonders sorgfältig qualitätsgesichert, einer ungezielten Vorratsdatensammlung meist überlegen sind; bei Bedarf werden Daten gezielt nacherhoben.

4. Weitere Datenschutzanforderungen

Aufgrund des hohen Reidentifizierungsrisikos verbietet sich eine Freigabe von Datensammlungen aus AAL-Szenarien zum „Public Use“. Die Freigabe für wissenschaftliche Zwecke („Scientific Use“) sollte nur unter kontrollierten Bedingungen erfolgen, für ordentlich aufgesetzte Projekte, die (etwa) dem TMF-Datenschutzkonzept folgen, in einem verbindlichen organisatorischen Rahmen durchgeführt werden, Audit-Maßnahmen vorsehen und ein Ethik-Votum und ein konsentiertes

Datenschutzkonzept vorweisen können. Eine wichtige Anforderung ist die verbindliche Untersagung von Reidentifizierungsversuchen durch Dienstanweisungen oder Verträge. Zur Senkung des Reidentifizierungsrisikos sollte man in manchen Fällen auch eine getrennte Speicherung von AAL-Daten ins Auge fassen, wie es im TMF-Datenschutzkonzept für Biobanken [BMB] für genetische Analysedaten vorgesehen ist.

Es versteht sich von selbst, dass jede Datenübertragung in einem AAL-Szenario vom Prinzip der Erforderlichkeit geleitet sein muss. Daten, die nur im häuslichen Umfeld oder gar nur im Gerät gebraucht werden, sollten dieses gar nicht erst verlassen.

Auch andere Beteiligte und Akteure in AAL-Szenarien haben Anspruch auf Datenschutz, zum Beispiel Mitarbeiter von Rettungs- und Pflegediensten. Wie weit hier Anonymisierungs- und Pseudonymisierungsverfahren angemessen, sinnhaft und wirksam sind, muss im Einzelfall überlegt werden.

Eine ganz wichtige Datenschutzanforderung in AAL-Szenarien betrifft die IT-Sicherheit. Die Grundforderung lautet: Alle Objekte und Akteure im Netz – Sensoren, Mobilgeräte, Server, Datennutzer – brauchen eine starke wechselseitige Authentisierung sowie Vertraulichkeit und Integrität der Kommunikation. Das ist mit angemessenem Schutzniveau und Aufwand nur auf der Basis einer etablierten Public-Key-Infrastruktur möglich. Passwortschutz und verschlüsselte Datenübertragung sind wichtig, aber alleine unzureichend. Für die Absicherung der erlaubten Datenzugriffe sollten geeignete Token, z. B. Smart-Cards, eingesetzt werden. Zu bedenken dabei ist, dass in den AAL-Szenarien viele IT-Laien mitspielen, für die die eingesetzte Sicherheitstechnik nachvollziehbar und beherrschbar sein muss. Ein besonderes Augenmerk ist auf die technische Absicherung von Fernwartungszugängen zu richten.

5. Fazit

Die Pseudonymisierungsschemata A und B des TMF-Datenschutzkonzepts sind auch für AAL-Projekte angemessen, soweit zentrale Speicherung oder Sekundärnutzung von Daten vorgesehen sind. Sie decken nicht den „Heimbereich“ eines AAL-Szenarios ab, also den Bereich, in dem der Betroffene lebt und die Daten erzeugt werden, und sind hierfür passend zu ergänzen. Künftig werden diese Schemata im „Versorgungs-“ und „Studienmodul“ sowie im „Forschungsmodul“ des revidierten TMF-Datenschutzkonzepts beschrieben.

Für die Sekundärnutzung der AAL-Daten im Forschungszusammenhang sind wegen ihres hohen Reidentifizierungsrisikos zusätzliche organisatorische Maßnahmen und Nutzungsbeschränkungen zu definieren.

Die IT-Sicherheit in AAL-Netzen setzt ein hohes Schutzniveau und insbesondere eine funktionierende PKI voraus.

Literatur

[genDS] Reng CM, Debold P, Specker C, Pommerening K. *Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze der Medizin*. Medizinisch Wissenschaftliche Verlagsgesellschaft, München 2006.

[BMB] Pommerening K, Hummel M, Ihle P, Semler S. *Biomaterialbanken - Datenschutz und ethische Aspekte*. Medizinisch Wissenschaftliche Verlagsgesellschaft, München (im Druck)