Personalisierte Medizin und Informationstechnik – Aspekte des Datenschutzes

K. Pommerening

Johannes Gutenberg-Universität, Universitätsmedizin, Institut für Medizinische Biometrie, Epidemiologie und Informatik, D-55101 Mainz

1. Die Individualisierung der Medizin

Zwei aktuelle Entwicklungen führen zu einer ausgeprägten Individualisierung (oder Personalisierung) der Medizin: die Entwicklungen im Bereich der Arzneimittel und der Telemedizin, insbesondere der Medizingerätetechnik.

- Die immer leichtere Verfügbarkeit genetischer Daten ermöglicht mit den Forschungsergebnissen der Pharmakogenomik und Pharmakogenetik, beruhend auf gendiagnostischer Differenzierung, eine maßgeschneiderte, auf den individuellen Patienten angepasste Therapie durchzuführen.
- Assistierende Technologie ermöglicht eine gezielte individuelle alltägliche, medizinische und pflegerische Hilfestellung, was insbesondere im Hinblick auf die „alternde Gesellschaft" anders gar nicht mehr geleistet werden kann, und ist oft mit einer lückenlosen Überwachung des Gesundheitszustandes oder gar des Alltagslebens eines Patienten verbunden.

Beide Entwicklungen sind äußerst hilfreich:

- für den Patienten, um bestmöglich versorgt zu werden,
- für den Arzt, um seine Therapieerfolge zu verbessern und
- für die Industrie, um in vielversprechende Geschäftsfelder expandieren zu können („Die alternde Gesellschaft verspricht ein Multimilliardengeschäft.").

Wer von Personalisierter Medizin spricht, meint in der Regel den pharmakogenomischen oder -genetischen Aspekt, der assistierende Aspekt ist aber mindestens genau so wichtig, sowohl vom perspektivischen Nutzen als auch von den rechtlichen und ethischen Rahmenbedingungen aus betrachtet. Individualisierung der Behandlung (Diagnose, Therapie, Überwachung und Hilfe) wird in Zukunft immer bedeutsamer und ist – unabhängig vom Ansatz – stets mit der Erzeugung von riesigen individuellen Datensätzen verbunden, darunter neben genetischen Daten und Gesundheitsdaten auch Daten zum Lebensstil, sozioökonomische Daten und Verhaltensdaten in bisher nicht vorstellbarem Ausmaß. „In zehn Jahren gibt es zu jedem Menschen Milliarden von Datenpunkten. Der Knackpunkt ist, wie wir diese zu validen Hypothesen über den jeweiligen Menschen verdichten können." (Leroy Hood nach [1]). Vom Datenschutzgesichtspunkt ebenso wie von der Technikfolgenabschätzung (Health Technology Assessment) aus betrachtet ist es wichtig, die Auswirkungen beider Varianten der Individualisierung zu betrachten, Gemeinsamkeiten herauszuarbeiten und Unterschiede festzustellen. Positiv anzumerken ist jedenfalls, dass die Personalisierte Medizin zumindest im Ansatz den Menschen als Individuum sieht und nicht auf einen statistischen Mittelwert reduziert.

2. Pharmakogenomik und Pharmakogenetik

Pharmakogenomik ist Forschung im Labor. Geklärt werden soll die Interaktion von genetischen Dispositionen, Mutationen oder Polymorphismen mit Medikamenten. Deren Wirkung kann durch die von den Genen gesteuerten Enzyme stark beeinflusst werden bis hin zur Nichtwirksamkeit oder zu unannehmbaren Nebenwirkungen, die sogar zu einer Rücknahme der Zulassung eines Medikaments führen können, obwohl sie bei 90 % der Patienten nicht auftreten. Besonderen Erfolg verspricht man sich in der Krebstherapie, wo der genetische Fingerabdruck eines Tumors direkte Möglichkeiten zur Bekämpfung von Tumorzellen eröffnen soll, ohne gesunde Zellen zu beeinträchtigen [2].
Als Pharmakogenetik wird die klinische Erforschung des gleichen Problembereichs bezeichnet, also die Prüfung am Menschen im Rahmen kontrollierter klinischer Studien: Lässt sich das von der Laborforschung vorhergesagte unterschiedliche Ansprechen von Individuen auf eine Therapie auch in der konkreten Therapiesituation nachweisen? Eine wichtige Rolle bei der unterschiedlichen Wirkung von Therapieversuchen spielen natürlich neben genetischen auch andere persönliche Merkmale wie Alter, Geschlecht, Größe, Gewicht, ebenso Vorerkrankungen oder gleichzeitige andere Erkrankungen sowie persönliche Gewohnheiten wie Ernährung und Suchtmittelkonsum. Alle diese Daten müssen für eine individuelle Therapie erhoben werden.
Die aufgrund genetischer Daten individualisierte Medizin hat viele Vorteile:

- *Für Patienten:* Verbesserung der Diagnose-Genauigkeit, Auswahl einer optimal wirksamen Therapie, Vermeidung unwirksamer Therapien, Reduktion unerwünschter Nebenwirkungen.

- *Für Ärzte:* erhöhte Gewissheit bei Diagnostik und Therapie, Verbesserung des Behandlungserfolgs.
- *Für klinische Forscher:* schärfere Ein- und Ausschlusskriterien für die Aufnahme in eine klinische Studie durch Differenzierung von Subpopulationen, verringerte Anforderungen an Fallzahlen, bessere Nachweisbarkeit von Therapieeffekten.
- *Für Kostenträger:* weniger unnötige oder unwirksame Therapien, weniger Nebenwirkungen, dadurch verbesserte Kosteneffizienz.
- *Für die Pharmaindustrie:* Entwicklung innovativer Produkte und Erschließung neuer Marktsegmente.

Beispielsweise können bei klinischen Studien genetisch ungeeignete Patienten ausgeschlossen werden: Das ist ein Vorteil für die Betroffenen, die keine unnötigen Therapieversuche erleiden müssen, aber auch für die Forscher, die ihre Ressourcen effizienter einsetzen und trennschärfere Ergebnisse erzielen können. Die Problematik des Datenschutzes wird exemplarisch durch vier Anwendungsfälle verdeutlicht.

Anwendungsfall 1: Pharmaforschung mit Probenmaterial
Proben aus einer Biomaterialbank oder einer Klinik werden an eine Pharmafirma für ein pharmakogenomisches Forschungsprojekt abgegeben, zusammen mit dafür relevanten medizinischen Begleitdaten (mindestens Diagnose).

Anwendungsfall 2: Klinische Studie mit individualisierter Medikamentierung
Das Datenmanagement einer solchen Studie unterscheidet sich von einer „herkömmlichen" klinischen Studie nur dadurch, dass auch die nötigen genetischen Daten erfasst werden.

Anwendungsfall 3: Klinische Epidemiologie
Hier ist das Ziel eine systematische Auswertung des Behandlungserfolgs, auch einrichtungsübergreifend. Die nötigen Daten, auch der individualisierten Medizin werden aus dem Behandlungszusammenhang gewonnen, zentral zusammengeführt und – evtl. auch konsekutiv über längere Zeiträume immer wieder – ausgewertet.

Anwendungsfall 4: Individuelles Doping
Dieses ist eine Schattenseite der individualisierten Medizin. Leistungssteigernde Substanzen werden genau auf die genetische Situation des Sportlers angepasst verabreicht und dabei die Nichtnachweisbarkeit optimiert. Zur Bekämpfung dieser unerwünschten Entwicklung ist im Gegenzug eine lückenlose Überwachung aller Spitzensportler erforderlich, die auffällige Änderungen in Körper- und Leistungswerten entdeckt, wenn schon die Substanzen selbst nicht nachweisbar sind.

3. Assistierende Technologie

Assistierende Gesundheitstechnologie (man spricht auch von Ambient Assisted Living oder Wireless Personalized Health Services) umfasst Ansätze, welche für das alltägliche Leben und die Gesundheitsversorgung, vor allem älterer Menschen, Unterstützung und Hilfe gewähren sollen, besonders in Situationen, wo diese sonst auf sich alleine gestellt wären. Hierunter sind vor allem technische Geräte zu verstehen, einerseits direkte Hilfen wie Herzschrittmacher, Hör-Implantate oder Seh-Chips, andererseits aber auch beispielsweise Sensoren und Systeme, die Bewegungen und Gesundheitszustand möglichst unaufdringlich überwachen und in kritischen Situationen entweder direkt eingreifen oder einen Alarm auslösen. Hierbei werden neben den unmittelbar Betroffenen auch Familienmitglieder, Ärzte und Pflegepersonal in die Kommunikation einbezogen. Ziel ist vor allem, den Betroffenen ein längeres selbstständiges Leben im häuslichen Umfeld zu ermöglichen. Die Akzeptanz solcher Systeme soll soweit gefördert werden, dass sie sich nahtlos und wie selbstverständlich in den Alltag der Menschen einfügen lassen.
Vom (tele-)medizinischen Gesichtspunkt steht das Telemonitoring (Überwachung von Körperfunktionen, z. B. des Blutdrucks, und Übertragung der Daten an ein spezialisiertes Behandlungszentrum) im Vordergrund. Visionen reichen bis zum „Body Area Network" (BAN), wo verschiedene Sensoren und Sonden am Körper online geschaltet sind und ihre Daten kontinuierlich an die Zentrale senden; sogar implantierte RFIDs („Radio Frequency Identity"-Chips, auch als Transponder bezeichnet) werden für diesen Zweck diskutiert. Solche Sensoren senden ihre Daten meist zunächst lokal an ein mobiles Gerät (Telefon/Netzrechner), von wo sie über das Internet funk- oder kabelgebunden weitergeleitet werden; der Körper wird Teil des „Internets der Dinge" und unterliegt dem „Pervasive Computing". Tragen die Patienten also künftig ihren Herzrhythmus oder andere kritische Körperfunktionen im Internet spazieren? Besonders kritisch zu beurteilen sind Fernwartungs- oder Administrationszugänge zu solchen Geräten, die den Patienten dem Passwort-Besitzer ausliefern, von Sicherheitslücken und Systemfehlern abhängig machen und den Gefahren des Internets ausliefern. Die Industrie sieht hier ein enormes Wachstumspotenzial im Bereich der Mobiltechnik, der RFID-Chips und der Sensor-Technik. Führende Hardware-Firmen wie Intel, AMD, TI und Qualcomm arbeiten an speziellen Chip-Entwicklungen für drahtlose Monitor-Geräte mit RFID-Technik und Chipkarten [3]. Die Einführung aller solcher Geräte unterliegt in Deutschland allerdings dem Medizinproduktegesetz (MPG); in den USA etwa ist die FDA für die Zulassung zuständig, so dass hier zumindest von der medizinischen und technischen Seite eine gewisse Qualität für die Funktion gesichert wird. Aber komplexe Systeme haben Fehler, die sich auch durch strenge Zulassungsverfahren „hindurchmogeln" können. Und eine Datenschutz- oder Technikfolgen-

abschätzung ist mit dem Zulassungsverfahren nicht in ausreichendem Maße verbunden. Da hier Systemfehler sogar lebensbedrohlich sein können, ist die Integrität der Systeme und Daten im wörtlichen Sinne lebenswichtig. Beispiele für die Gefahren findet man u. a. in den Ausgaben 20.48, 49, 52 des Risks Digest [4]. Die Softwareentwicklung sollte unbedingt den Regeln des „Secure Engineering" [5] folgen.
Auch der Bereich der assistierenden Technologien ist zunächst im Behandlungskontext angesiedelt, allerdings oft im Sinne des „shared care" einrichtungsübergreifend, interdisziplinär und mit Daten, die über das Internet übertragen und auf zentralen Servern zusammengeführt werden. Die vor der Zulassung notwendige klinische Prüfung nach dem MPG definiert allerdings einen Forschungskontext, der aber unmittelbar mit der Behandlung verquickt ist.
Die längerfristige und einrichtungsübergreifende systematische Datensammlung und -auswertung trägt auch hier zur Sicherung der Behandlungsqualität und zum medizinischen Fortschritt bei und ist daher unverzichtbar. Diese definiert einen reinen Forschungskontext. Wichtig dabei ist, Daten direkt vom Gerät verwenden zu können, ohne fehleranfällige Zwischenschritte; das verspricht eine hohe Datenqualität.
Einige weitere Beispiele illustrieren den Nutzen und die Datenschutzproblematik assistierender Technologien.

▶ **Anwendungsfall 5: Direkte Unterstützung**
Zum Beispiel durch Prothetik, ohne direkte Notwendigkeit der Datenspeicherung und -übertragung. Dies ist aus Sicht des Datenschutzes unproblematisch, kann es aber werden, wenn Daten zur Funktionsüberprüfung zumindest kurzzeitig aufgezeichnet oder gar übermittelt werden, und vor allem, wenn diese Geräte zum Zwecke der Fernwartung online erreichbar sind.

▶ **Anwendungsfall 6: Selbsteingabe von Messdaten**
Der Patient liest die Werte selbst ab und überträgt sie mit Hilfe eines (z. B. webbasierten) Eingabeformulars an einen verantwortlichen Arzt. Dabei sind zumindest die Regeln einer sicheren Internet-Kommunikation zu befolgen, wie wechselseitige starke Authentisierung zwischen Server und Client und verschlüsselte Übertragung. Abgesehen davon kann die Datenqualität problematisch sein.

▶ **Anwendungsfall 7: Überwachung von Körperparametern**
Zum Beispiel von Blutdruck, Zuckerwert und Atmung im Schlaf durch Sensoren mit Aufzeichnung und regelmäßiger oder gar ständiger Online-Übermittlung. Hier ist die Datenqualität im Vergleich zu Fall 6 sicher besser, vor allem aber auch die Bequemlichkeit für den Betroffenen. Dafür ist die Gefährdung aber auch wesentlich höher, wenn die Überwachungsgeräte selbst im Netz erreichbar sind.

▶ **Anwendungsfall 8: Sport**
Die laufende Überwachung von Körperwerten von Sportlern während des Trainings und Wettkampfes (Puls, Laktat-Werte, …) ist ein Spezialfall des Falles 7. Problematisch ist hier, dass kein Behandlungszusammenhang besteht und die Daten außerhalb eines besonders geschützten medizinischen Umfeldes entstehen und verarbeitet werden.

▶ **Anwendungsfall 9: MPG-Studie**
Wirksamkeit und Nutzen eines Medizinprodukts werden mit dem Ziel der Zulassung untersucht. Dabei müssen die entstehenden Daten sorgfältig dokumentiert und auch langfristig archiviert werden.

▶ **Anwendungsfall 10: Qualitätssicherung durch Benchmarking**
Hier sind wir in einer Situation ähnlich zu Fall 3; die dortigen Anmerkungen gelten auch hier.

▶ **Anwendungsfall 11: Epidemiologische Studie**
Hierfür werden die gewonnenen Daten, vielleicht in reduziertem Umfang, längerfristig aufbewahrt, zusammengeführt und – möglicherweise immer wieder – ausgewertet.

4. Datenaufkommen der individualisierten Medizin

Die individualisierte Medizin erzeugt Daten in großem Umfang, aber mit unterschiedlicher Datenprozessierung und -verwendung. Bei beiden Ansätzen entsteht ein hohes Reidentifizierungsrisiko:

- Es werden hochdimensionale, für das Individuum charakteristische Datensätze erzeugt.
- Das externe Wissen, über das ein potenzieller Angreifer verfügen kann, nimmt parallel zum technischen Fortschritt zu und ist in Umfang und Detailliertheit schwer einzuschätzen, vor allem für die Zukunft.

Daher muss sorgfältig geplant werden, welche Daten erfasst werden sollen, wohin sie übermittelt und wo sie gespeichert werden, was mit ihnen gemacht wird und wie sie schließlich wieder „aus dem Verkehr gezogen" werden. Werden etwa genetische Daten, z. B. aus Tumorproben, für ein Forschungsprojekt zusammen mit medizinischen Begleitdaten bereitgestellt, so muss ein erhebliches externes Wissen

hinsichtlich genetischer „Fingerabdrücke“ unterstellt werden: Eine teilweise Genom-Analyse, etwa aus einer Speichelprobe, ist inzwischen im dreistelligen Euro-Bereich erhältlich und kann zur Reidentifizierung der medizinischen Begleitdaten führen. Das Gendiagnostikgesetz versucht hier eine Eindämmung. Verstöße sind aber, besonders bei ausländischen Anbietern, kaum kontrollierbar.

Während die Probleme mit den genetischen Daten immerhin schon ausführlich diskutiert wurden, ist das Bewusstsein für die Nebenwirkungen der assistierenden Technologien noch nicht so weit entwickelt, obwohl diese aus der Sicht des Datenschutzes eher noch kritischer zu bewerten sind, und das nicht nur wegen der unzureichend gelösten Sicherheitsfragen der mobilen IT. Da diese Systeme zum Teil automatisiert für den Betroffenen agieren, ist ein Zielkonflikt mit der informationellen Selbstbestimmung offenkundig, sowohl im Hinblick auf Entscheidungen, aber auch im Hinblick auf die entstehenden Datenmengen.

Bei assistierenden Technologien entstehen Verhaltens- und Lebensstil-Daten in großem Umfang. Der Mensch ist möglicherweise ständig online, und zwar nicht mit einem Kommunikationsgerät wie Handy oder Navi, das er auch mal längere Zeit abschalten oder verleihen kann, sondern mit seinem Körper. Die Daten enthalten Details zum Privatleben, die oft mehr über den Menschen enthüllen als seine genetischen Daten, die „nur“ Veranlagungen und Verwandtschaftsbeziehungen wiedergeben und über genetische Fingerabdrücke evtl. mit Diagnosen verknüpft werden können.

Als externes Wissen bei Daten aus assistierenden Technologien muss man Informationen zur Lebensführung unterstellen, die leicht durch persönliche Beobachtung oder durch Suchen in sozialen Netzen auf völlig legale Weise zu gewinnen und zuzuordnen sind: Wann hat der Betroffene Mahlzeiten zu sich genommen, wann hat er das Haus verlassen usw. Dadurch bietet sich die Möglichkeit zur Verfolgung („Tracking“) einer Person, vor allem wenn die Daten mit Alltagsbeobachtungen oder anderen Telekommunikationsdaten verknüpft werden.

Auch der Umgang mit der Patienteneinwilligung zur Nutzung assistierender Technologien muss hinterfragt werden: Wie steht es mit der Freiwilligkeit? Hat der Patient überhaupt die Wahl? Beziehungsweise welche Wahl hat er? Wie weit ist er überhaupt in der Lage, die Folgen seiner Einwilligung zu überblicken?

5. Ansätze zur datenschutzgerechten Gestaltung

Die Datenschutzkonzepte der TMF e. V. [6–8] bilden eine gute Ausgangsbasis, die individualisierte Medizin datenschutzgerecht zu gestalten; sie ersparen jedoch nicht eine gründliche Auseinandersetzung mit den Gefährdungen in einer speziellen Situation und die jeweilige Auswahl geeigneter Maßnahmen nach dem Grundsatz der

Verhältnismäßigkeit. Der Bereich der genetischen Forschung wird durch das TMF-Datenschutzkonzept für Biomaterialbanken zu großen Teilen abgedeckt. Für den Bereich der assistierenden Technologien sind die Ansätze des generischen Datenschutzkonzepts geeignet, aber noch gezielt auszuarbeiten. Diese Aussagen werden im Folgenden, insbesondere für die exemplarischen Anwendungsfälle der Kapitel 2 und 3, genauer ausgeführt. Auch die IT-Sicherheits- und Datenschutzkonzepte der Gesundheitstelematik und telemedizinischer Projekte liefern wichtige Bausteine für die datenschutzgerechte Gestaltung der individualisierten Medizin. Grundsätze, auf denen die Lösungsansätze beruhen, sind:

- Informationelle Selbstbestimmung so weitgehend wie möglich. Da der Patient oft keine wirkliche Wahl hat, wenn er die Vorteile der individualisierten Medizin für sich nutzbar machen will, und die Tragweite einer Einwilligung nicht in allen Details vorhersehen kann, müssen besondere Sicherheitsmaßnahmen getroffen werden und die längerfristige Verwendung der Daten auf das absolut notwendige Minimum reduziert werden. Ansonsten muss die Aufklärung so vollständig wie möglich und dem Patienten angemessen sein [9].
- Informationelle Gewaltenteilung (z. B. durch pseudonymisierte Speicherung und Datentreuhänderdienste) so weitgehend, wie es nach dem Grundsatz der Verhältnismäßigkeit möglich ist. In der individualisierten Medizin ist dies nur in Grenzen möglich; das Problem der hohen Informationsdichte mit daraus folgendem hohem Reidentifizierungspotenzial ist dadurch nicht vollständig behebbar. Wichtig ist daher der absolute Schutz der Datenbanken und die strikte Wahrung des Behandlungszusammenhangs; Forschungsprojekte auf den Daten bedürfen einer gründlichen Vorabprüfung und strikter verbindlicher Regelungen.
- Deutliche Trennung zwischen dem direkten Behandlungszusammenhang und sekundären Datenverwendungen, insbesondere für die medizinische Qualitätssicherung und Forschung. Für die sekundäre Verwertung der Daten ist stets eine Anonymisierung oder Pseudonymisierung vorzusehen.
- Bei langfristiger Aufbewahrung sind die Möglichkeiten zur getrennten, organisatorisch unabhängigen Speicherung verschiedener Datenarten zu nutzen.
- Wegen des hohen, nicht zu kontrollierenden Reidentifizierungspotenzials ist die Bereitstellung von Public-Use-Dateien im Allgemeinen nicht zu vertreten.
- IT-Sicherheit muss nach dem Stand der Technik implementiert werden. Hierfür ist eine gründliche Planung vor Beginn eines Projekts unumgänglich. Das betrifft insbesondere Zugriffsrechteregelungen und die Sicherheit von Servern, Übertragungswegen und Client-Rechnern.
- Auf der organisatorischen Seite sind umfangreiche Überwachungs- und Kontrollmechanismen vorzusehen.

- Die Verantwortung muss klar geregelt sein; insbesondere muss für den Patienten stets ein eindeutig definierter Ansprechpartner erreichbar sein.

Der Schutzbedarf medizinischer Daten ist stets hoch und wird im Behandlungsfall durch die ärztliche Schweigepflicht, im Allgemeinen durch die Datenschutzgesetze besonders betont. Genetische Daten gelten darüber hinaus als besonders sensibel; wegen ihres hohen Reidentifizierungspotenzials muss man dieses gleichermaßen für Daten der assistierenden Technologien annehmen. Daher sind besondere Schutzmaßnahmen zu treffen, die insbesondere unbefugte Zugriffe ausschließen und das Reidentifizierungsrisiko minimieren. „Entscheidend für Akzeptanz und Markterfolg [assistierender Technologien] wird deshalb die verantwortungsvolle Abwägung zwischen technisch möglichen Assistenzfunktionen einerseits und der hierfür nötigen Überwachung und Datenübermittlung andererseits sein." [10].
Die individualisierte Medizin findet zunächst im reinen Behandlungskontext statt, aber in der Regel mit großem Behandlungsteam („shared care"). Dafür sind die Ansätze der Gesundheitstelematik sowie das „Versorgungsmodul" des TMF-Datenschutzkonzepts [7] als Ausgangspunkt geeignet. Der Forschungskontext spielt erst dann eine Rolle, wenn die erhobenen Daten im Rahmen einer klinischen Studie entstehen oder wenn eine Sekundärauswertung, z. B. des Behandlungserfolgs oder von Krankheitsverläufen, geplant wird. Was unbedingt sinnvoll ist und wie weit die Datengranularität vergröbert werden kann, muss im Einzelfall geprüft werden, aber gerade detaillierte langfristige Verlaufsdaten können von besonderer Bedeutung sein. Bei Langzeitspeicherung bieten das „Forschungsmodul" und das „BMB-Modul" des TMF-Datenschutzkonzepts [7, 8] die geeigneten Lösungsansätze, für die klinischen Studien, sei es im Bereich der pharmakogenetischen Forschung – wofür die Regelungen des AMG (Arzneimittelgesetz) greifen oder im Bereich von Medizingeräten, wofür die Regelungen des MPG zu befolgen sind – ist das „Studienmodul" des TMF-Datenschutzkonzepts [7] eine geeignete Basis.
Erwägungen zur IT-Sicherheitstechnik über den Stand der marktverfügbaren Technik hinaus sind bei assistierenden Technologien notwendig. Hier sind die IT-Sicherheitsprobleme durch mobile Kommunikationstechnik verschärft; eine PKI (Public Key Infrastructure)-Implementation ist unumgänglich für die Sicherheit, wird aber wegen Performanz und Speichergröße eingebetteter Chips und RFIDs nur mangelhaft, meistens gar nicht umgesetzt. Eine PKI ist ein flächendeckend verteiltes System, das den netzweiten vertrauenswürdigen Umgang mit Schlüsseln und Zertifikaten für die asymmetrische Kryptographie, einschließlich digitaler Signatur und starker Authentisierung, ermöglicht. Sicherheit bei assistierenden Techniken ist grundsätzlich, wie in jedem vernetzen System, nur möglich, wenn die Anforderungen wechselseitige starke Authentisierung aller kommunizierenden Subsysteme (Sensoren, mobile

Geräte, Server, …), verschlüsselte Datenübertragung sowie die Integritätssicherung durch digitale Signatur gewährleistet sind – mit anderen Worten, wenn eine flächendeckende PKI nach dem Stand der Technik existiert und genutzt wird. Hier besteht auf der technischen Seite noch erheblicher Entwicklungsbedarf; starke kryptographische Verfahren scheitern auf eingebetteten Chips oft an deren mangelnder Rechen- und Speicherkapazität. Kryptographische Verfahren auf der Basis elliptischer Kurven (ECC-Verfahren) bieten Vorteile, sind aber noch nicht genügend weit verbreitet. Dies ist kein Problem der Wissenschaft, die ihre Hausaufgaben hierfür schon längst erledigt hat, sondern des Marktes.
Abschließend werden auf der Basis der oben genannten Grundsätze Empfehlungen für die verschiedenen in den Kapiteln 2 und 3 beschriebenen Anwendungsfälle formuliert. Welche Maßnahmen angemessen sind, ergibt sich im Einzelnen aus den Empfehlungen zur Abschätzung der Verhältnismäßigkeit im TMF-Datenschutzkonzept [7].

Anwendungsfall 1: Pharmaforschung mit Probenmaterial
Hier sind die Überlegungen und Vorschläge aus dem TMF-Datenschutzkonzept für Biomaterialbanken [8] einschlägig; für eine Übersicht siehe [11].

Anwendungsfall 2: Klinische Studie mit individualisierter Medikamentierung
Zu beachten sind die Regelungen des Arzneimittelgesetzes (AMG) und der guten klinischen Praxis (GCP). Die Überlegungen zum Studienmodul aus dem revidierten Datenschutzkonzept der TMF e. V. beschreiben diese Situation.

Anwendungsfall 3: Klinische Epidemiologie
Dies entspricht einer Situation, die vom Modell A des generischen Datenschutzkonzepts der TMF e. V. [6] oder dem Versorgungsmodul des revidierten Datenschutzkonzepts [7] abgedeckt wird. Bei langfristiger einrichtungsübergreifender Datenspeicherung ohne direkte Rückwirkung auf die Behandlung sind die Überlegungen zum Modell B des generischen TMF-Datenschutzkonzepts bzw. zum Forschungsmodul des revidierten TMF-Datenschutzkonzepts zutreffender.

Anwendungsfall 4: Individuelles Doping
Dieser Fall ist in einem ganz anderen Umfeld außerhalb der eigentlichen medizinischen Forschung und Versorgung angesiedelt und erfordert ganz eigene Überlegungen zu Ethik und Datenschutz. Diese werden hier ausgelassen.

Anwendungsfall 5: Direkte Unterstützung
Die Gewinnung und Verarbeitung der Daten findet im direkten Behandlungszusammenhang statt und wird insofern im Modell A des generischen TMF-Datenschutz-

konzepts und in den Überlegungen zum Versorgungsmodul des revidierten TMF-Datenschutzkonzepts beschrieben. Dazu kommen aber noch die oben erwähnten besonderen Anforderungen an die IT-Sicherheit.

▶ **Anwendungsfall 6: Selbsteingabe von Messdaten**
Der erste Satz zum Fall 5 gilt hier ebenfalls; für die IT-Sicherheit der Datenübertragung werden aber nur die wesentlich einfacheren, breit verfügbaren und etablierten Sicherheitsmechanismen im Internet (auf SSL-Basis) benötigt.

▶ **Anwendungsfall 7: Überwachung von Körperparametern**
Hierfür gelten die Bemerkungen zum Fall 5 in analoger Weise.

▶ **Anwendungsfall 8: Sport**
Hier gilt das gleiche wie im Fall 4. Man muss davon ausgehen, dass der Sportler selbst an der Optimierung seiner Körperfunktionen interessiert ist.

▶ **Anwendungsfall 9: MPG-Studie**
Hier sind, insbesondere aus Datenschutzsicht, Regeln der GCP einzuhalten, die auch die Aufklärung der Patienten und Vorgaben für die Einwilligungserklärung umfassen. Die Regeln entsprechen denen für andere klinische Studien. Die Situation wird durch das Studienmodul des revidierten TMF-Datenschutzkonzepts abgebildet, ähnlich wie im Fall 2.

▶ **Anwendungsfall 10: Qualitätssicherung durch Benchmarking**
Hier gelten ähnliche Hinweise wie im Fall 3.

▶ **Anwendungsfall 11: Epidemiologische Studie**
Diese Situation wird im Modell B des generischen TMF-Datenschutzkonzepts und in den Überlegungen zum Forschungsmodul des revidierten TMF-Datenschutzkonzepts beschrieben.

6. Zusammenfassung

Zwei aktuelle Entwicklungen führen zu einer ausgeprägten Individualisierung der Medizin: einerseits die maßgeschneiderte Therapie auf der Basis der Pharmakogenetik und andererseits die assistierende Technologie. Für den Umgang mit den entstehenden umfangreichen individuellen Datensätzen wurden datenschutzgerechte Lösungsansätze vorgestellt.

Schlüsselwörter: Personalisierte Medizin, Pharmakogenomik, Assistierende Technologie, Ambient Assisted Living, Datenschutz, TMF-Datenschutzkonzept

7. Literatur

[1] Singer E: Die Medizin wird vollständig digitalisiert. Technology Review 11.03.10. http://www.heise.de/tr/artikel/Die-Medizin-wird-vollstaendig-digitalisiert-949266.html (12.03.2010).
[2] Briseño C: Meine Gene, mein Krebs, meine Therapie. SPIEGEL online 19. Februar 2010. http://www.spiegel.de/wissenschaft/medizin/0,1518,678943,00.html (12.03.2010).
[3] Fuscaldo D: Chip Makers to Personalize Health Care. The Wall Street Journal May 23, 2007. http://online.wsj.com/article/SB117987928600611499.html (12.03.2010).
[4] Neumann P (ed.): The Risks Digest. http://catless.ncl.ac.uk/Risks/ (12.03.2010).
[5] Anderson R: Security Engineering. Wiley, New York 2001.
[6] Reng CM, Debold P, Specker C, Pommerening K: Generische Lösungen zum Datenschutz für die Forschungsnetze der Medizin. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, München 2006.
[7] Pommerening K, Drepper J, et al. : Das revidierte generische Datenschutzkonzept der TMF (Arbeitstitel). In Vorbereitung.
[8] Pommerening K, Hummel M, Ihle P, Semler S: Biomaterialbanken – Datenschutz und ethische Aspekte. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, München (im Druck).
[9] Berger B, Goebel JW, Harnischmacher U, Ihle P, Scheller J: Checkliste und Leitfaden zur Patienteneinwilligung. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, München 2006.
[10] Wikipedia: Stichwort „Ambient Assisted Living". http://de.wikipedia.org/wiki/Ambient_Assisted_Living (12.03.2010).
[11] Pommerening K: Biomaterialbanken – Rechtliche Aspekte, Datenschutz und Datensicherheit. In: Niederlag W, Dierks C, Rienhoff O, Lemke HU (Hrsg.): Rechtliche Aspekte der Telemedizin. Health Academy 2/2006, Dresden 2006, 178–189.