

Patientenversorgungs- und datenschutzgerechte Bildkommunikation

Außer der Umsetzung der RöV gilt es in der Teleradiologie auch, die Vorschriften der ärztlichen Schweigepflicht, die in der Berufsordnung und im Strafgesetzbuch festgelegt sind, sowie die Datenschutzgesetze zu beachten (walz97, walz99f, walz99g). Grundsätzlich muß bei der Verarbeitung von Daten entweder die Erlaubnis durch eine gesetzliche Regelung oder das Einverständnis des Patienten vorliegen (comp96). Dabei muß die teleradiologische Datenübertragung als ein gesonderter, nicht durch die übliche Einwilligung abgedeckter Vorgang betrachtet werden, da beispielsweise institutionenübergreifend gearbeitet, ein möglicherweise dem Patienten unbekannter Arzt herangezogen wird und die Telemedizin noch nicht als ein üblicher, dem Patienten bekannter Vorgang angesehen werden kann (s.a. einb99).

Da einerseits die ärztliche Schweigepflicht über die Datenschutzgesetze hinausgeht und alle anvertrauten - nicht nur die personenbezogenen - Daten umfaßt, und andererseits die Datenschutzbeauftragten eine Verschlüsselung bei Nutzung öffentlicher Leitungen fordern, wird eine einfache Anonymisierung von Bilddaten mit hoher Wahrscheinlichkeit nicht ausreichen (s. a. die Diskussion der aktuellen amerikanischen und deutschen Gesetzgebungsentwürfe in diesem Kapitel). Sie würde auch die Forderung aus der Berufsordnung nach einer sicheren Zuordnung der Patientendaten zum Patienten erschweren. Empfehlenswert ist heute die Verwirklichung der Teleradiologie über eine auf hohem Niveau verschlüsselte und zumindest institutionenbezogene, besser personenbezogene, authentifizierte Datenübertragung. Für die Abbildung eines heute vor Ort üblichen Ablaufs sollte eine möglichst rechtlich haltbare, verbindliche Befunddokumentation und -übermittlung integriert werden. Diese Anforderungen und dazu passende Lösungen werden seit 1998 in einer Arbeitsgemeinschaft zwischen Deutscher Röntgengesellschaft und der medizinischen Elektro- und Informationstechnologie-Industrie (ZVEI) zur Umsetzung einer bundesweiten, sicheren und kostengünstigen, DICOM-basierten Bildkommunikation ausgearbeitet (s. Kapitel 7).

Medizinische Informationstechnik- und Telemedizinanwendungen befinden sich in einem Spannungsfeld zwischen den Anforderungen des Datenschutzes und der Patientenversorgung. Praktikable Lösungen sind kaum und nur in Teilbereichen vorhanden (adam98, bert98, blob95, both99, bran95, foru98, gerl99, isu99, john99, krem99, ries99, ries99b, roge89, wein97). Modelle für wechselnde Rollen des medizinischen Personals, Notfallsituationen und institutionenübergreifende, auch medizinisch - wissenschaftliche Kooperationen sowie für die Umsetzung des Rechts auf informationelle Selbstbestimmung des Patienten müssen entwickelt, umgesetzt und evaluiert werden (blob95, bran95, epst97, euro95, fish96, foru98, hhs99,

jach98, john99, nort93, pomm97, pres97, zent99). Die Aktualität und Bedeutung dieser Fragestellung ist für die Weiterentwicklung der Telemedizin, von Netzen in der Patientenversorgung, für die Informationsverteilung in Kliniken und für wissenschaftliche Projekte als sehr hoch einzuschätzen.

Anforderungen aus ärztlicher Schweigepflicht und Datenschutz

Die Rahmenbedingungen zu Ärztlicher Schweigepflicht und Datenschutz sind durch Gesetzesvorgaben, z. B. den Datenschutz- oder Landeskrankenhausgesetzen, der Definition der Pflichten aus der ärztlichen Schweigepflicht im StGB und in der ärztlichen Berufsordnung, den Dokumentationsforderungen, z. B. in der ärztlichen Berufsordnung, der Röntgenverordnung oder aus Behandlungsverträgen und den Gesetzen zur Telekommunikation sowie dem aus dem Grundgesetz abgeleiteten Recht auf informationelle Selbstbestimmung gegeben (s. Kapitel 4):

❖ **Vertraulichkeit**

- Zugang und Zugriff nur für berechtigte Personen:
 - Trennung nach Gruppen und Rollen (z. B. Ärzte in unterschiedlichen Kliniken und Abteilungen mit verschiedenen, teils wechselnden Funktionen, Wissenschaftler an unterschiedlichen Orten mit unterschiedlichen Aufgaben, Hilfspersonal)
 - Sichere Authentifizierung
 - Nutzung von Zusatzinformationen (z. B. Ort, Zeit, Organisationsabbildungen wie Dienstpläne)
- Minimal – Prinzipien:
 - minimale Rechte
 - minimale Gruppen
 - minimale Informationserfassung und –speicherung
 - minimale Datenweitergabe
- Anonymisierung und Verschlüsselung (Pseudonymanwendung, Kryptographie)
- Unverkettbarkeit und Unbeobachtbarkeit
 - Gefahr durch Informationszusammenführung und Beobachtung von Abläufen

- Gewährleistung der Nichtwiedererkennbarkeit
 - z. B. anhand von rekonstruierten Bilddaten, insbesondere des Gesichtes
- Sicherung der Systeme gegen Angriffe
- Sicherung des Datentransfers
- Organisation und Schulung
- Umsetzung des Rechts auf informationelle Selbstbestimmung
 - Verfügungsbestimmung und Informationskontrolle (über Funktionen wie Zugriffskonfiguration, Sperren, Löschen) durch
 - Patienten
 - Vertrauenspersonen, z. B. Arzt
 - Datenverantwortliche, z. B. Arzt, Betreiber, Administration
- ❖ **Verbindlichkeit**
Dokumentation und Protokollierung (Zurechenbarkeit und Urheberschaft)
- ❖ **Verfügbarkeit**
- ❖ **Integrität**

1.1.1 Anforderungen aus Patientenversorgung und medizinischem Workflow

- ❖ Authentifizierung, Integrität und Verbindlichkeit

Der behandelnde Arzt, z. B. in der Herz- oder Mund-Kiefer-Gesichts-Chirurgie, muß feststellen können, daß die ihm, z. B. für die Operation, zur Verfügung gestellten Daten wirklich von seinem Patienten stammen, auf welchen Untersuchungsdaten sie basieren und welche Manipulationen im Rahmen der Bildverarbeitung durchgeführt wurden. Zusätzliche Informationen, z. B. des Radiologen oder des an der Bildverarbeitung beteiligten Wissenschaftlers, müssen fest verknüpft und zugänglich sein. Eine automatische Zuordnung soll möglichst anhand eindeutiger Identifikationsmerkmale und abgesichert durch Abgleich mit mehreren Kriterien erfolgen. Eine ärztlichen und juristischen Anforderungen genügende Dokumentation durch schnelle, einfache, aber sichere und damit für die Patientenversorgung geeignete Authentifizierungsverfahren, z. B. durch Chipkarten oder Auswertung personenspezifischer Merkmale, wird benötigt. Die Voraussetzungen für eine Anerkennung digitaler Daten als Dokumente müssen auf technischer, organisatorischer und rechtli-

cher Ebene geschaffen werden. Für den Absender soll nicht nur der Versand sondern auch der Empfang nachweisbar sein.

❖ Zentrale Patientendatenverwaltung und Telearchive

Modelle für die Übertragung von Zugriffsberechtigungen, z. B. durch den Patienten, behandelnden Arzt, Kontrollstelle oder fall- oder fragestellungsabhängig innerhalb von organisationsbezogenen Netzen, müssen weiterentwickelt werden. Die beteiligten Ärzte müssen teilweise, z. B. zur Arztbrieferstellung oder bei anschließenden Konsultationen, ohne persönliche Anwesenheit und erneute Autorisierung auf die Daten zugreifen können, z. B. durch zeitlich begrenzte erweiterte Rechtevergabe. Die Sicherstellung der ärztlichen Kontrolle bei externen Datenbanken, z. B. gefährdet durch mit der kontinuierlich stattfindenden, technischen Weiterentwicklung verbesserte Entschlüsselungsverfahren, kann beispielsweise durch regelmäßig notwendige Re-Autorisierungs-, ggf. Re-Verschlüsselungsmaßnahmen, u. U. in Verbindung mit bei fehlender Re-Autorisierung selbstlöschenden Medien, erfolgen.

❖ Standardisierte Übermittlung von Informationen innerhalb des Versorgungssystems

Der Transfer von Diagnostik- oder Behandlungsergebnissen an andere behandelnde Ärzte oder eine Datenbank muß einfach und schnell, möglichst standardisiert, aus den vorhandenen EDV-Systemen heraus und die Integration in die EDV des Empfängers ebenso einfach erfolgen können. Datenschutzmaßnahmen sollen möglichst unbemerkt oder in die üblichen Abläufe (Organisation) gut eingebunden stattfinden, um die Akzeptanz zu gewährleisten. Datenübertragungen zwischen sich in unterschiedlichen Netzwerken befindlichen Systemen, z. B. zwischen Kliniken, muß einfach und gleichzeitig sicher erfolgen können.

❖ Interoperabilität und Systemdurchgriff

Die Zahl der Computer und Informationssysteme nimmt derzeit kontinuierlich zu. Diese Entwicklung muß einerseits durch Zusammenführung, Verknüpfung und Interoperabilität der Systeme wieder umgedreht werden. Gleichzeitig besteht die Anforderung, daß Autorisierte Zugriffe von einem System auf andere, ggf. über weitere zwischengeschaltete System, z. B. Firewalls oder Kommunikationsserver hinweg, erfolgen können. Die Oberflächen müssen möglichst einfach und intuitiv, idealer-

weise Design-Standards folgend, zu bedienen sein. Zugriffe müssen auch von mobilen Systemen und von unterschiedlichen Standorten, z. B. bei einem unüblichen Zugang über einen fremden Computer, ermöglicht werden.

❖ Fernwartung und Systemadministration

Die vielfältigen Informations-, Archivierungs- und Untersuchungssysteme, z. B. auch die radiologischen Geräte wie MRT oder CT, werden wegen der Verkürzung der für die Patientenversorgung relevanten Ausfallzeiten und aus Kostengründen zunehmend per Fernwartung repariert und teilweise auch kontinuierlich oder phasenweise überwacht. Diese Vorteile müssen in Einklang mit der Forderung nach Schutz der auf diesen Systemen vorhandenen Patientendaten sowie bei vorhandener Vernetzung der übrigen Computer gebracht werden. Patientendaten müssen gegenüber Personen, die die technische Betreuung von Systemen durchführen, z. B. auch Systemadministratoren, verborgen bleiben.

❖ Bereitstellung anonymisierter Daten

Aus vorhandenen Datenbanken muß die Extraktion (manuell oder automatisch anhand von Regeln) von anonymisierten Demonstrationsfällen für Lehre, Weiter- und Fortbildung, evtl. auch Patientenaufklärung und –information, statistische Auswertungen sowie Prävention möglich sein. Alternative Verfahren können beispielsweise in beschränkten Views auf die Datenbank bestehen. Modelle wie im Fall des Krebsregisters beziehen eine treuhänderische Stelle ein, die die Pseudonymbildung durchführt und auch die Gefahren der Datenzusammenführung (Verkettbarkeit von Informationen) überwachen sollte.

❖ Bewahrung der ärztlichen Schweigepflicht und des vertrauensvollen Arzt-Patienten-Verhältnisses

Das für eine erfolgreiche Behandlung entscheidende, vertrauensvolle Arzt-Patienten-Verhältnis darf nicht gefährdet werden. Sowie auf der einen Seite keine Einschränkungen der Behandlungsmöglichkeiten des Patienten, z. B. durch zu restriktive Vorgaben oder Maßnahmen, geschehen dürfen, muß andererseits ein Hintereingang zu den patientenbezogenen Daten verhindert werden. Die Verschlüsselung von Patientendaten muß sicher sein.

❖ Qualitätssicherungsmaßnahmen

Andererseits müssen Auswertungen zur Qualitätssicherung, möglicherweise auch personen- oder institutionenübergreifend erfolgen können. Soweit möglich, soll die Ausführung innerhalb der betroffenen Gruppen selbst stattfinden, wie bereits bisher durch die ärztliche Qualitätssicherung, Qualitätszirkel oder Netzorganisationen.

❖ Nutzung von ungesicherter Software oder Hardware

In der Entwicklung oder Evaluation befindliche Systeme müssen in eine für die Patientenversorgung bestimmte Rechnerumgebung eingebunden werden können, d. h. eine vollkommene Abschottung würde die Weiterentwicklung zum Nachteil der Patienten stark behindern. Datenschutzkonzepte müssen die heterogene Struktur in Krankenhäusern berücksichtigen, an der zusätzlich viele Firmen mit ihren Produkten und Servicepersonal, oft auch mit Nutzung von Fernwartung und unter Einbeziehung von wechselndem Personal, teilnehmen. Eine Einteilung in Sicherheitssegmente und -levels ist zu prüfen. Risikoverringende Maßnahmen sollen eine Fehlbedienung oder Nachlässigkeit von Nutzern berücksichtigen und möglichst mehrere Schutzmechanismen (auch als Ausfallschutz) kombinieren sowie die Zugriffsmöglichkeiten möglichst einschränken, ohne allerdings die medizinischen Abläufe zu stören.

❖ Hohe Systemverfügbarkeit und -zuverlässigkeit

Es wird eine hohe Ausfallsicherheit der Systeme und der Kommunikationswege sowie Ausfallkonzepte benötigt, um einerseits in Notfällen schnell die notwendigen Informationen an der Hand zu haben und andererseits im Routinebetrieb mit möglichst geringem Verwaltungsaufwand arbeiten zu können. Der Anwender muß sich darauf verlassen können, daß das System auch das tut, was er erwartet. Mißverständnisse müssen möglichst vermieden werden und, soweit notwendig, Informationen über die möglichen Aktionen sowie Rückmeldungen über ausgeführte Aktionen angeboten werden. Es soll erreicht werden, daß Intention der Handlung eines Nutzers mit der technischen Durchführung übereinstimmt, um beispielsweise zu vermeiden, daß nur der Zeiger innerhalb einer Datenbank gelöscht wird, wenn dagegen das Löschen des Datensatzes selbst gewünscht war.

Datenschutzspezifische Anforderungen an DICOM

Nachfolgend sind die aktuellen Anforderungen aus Datenschutzgesichtspunkten für die Weiterentwicklung des DICOM-Standards, insbesondere aus einer über die Radiologie hinausgehenden Bildkommunikation, aufgeführt, die auch in einem Brief der AGIT an die zuständige Arbeitsgruppe 10 des Strategic Advisory DICOM Committee übermittelt wurden.

❖ Zugangsrechte in DICOM

Aufgrund der Datenschutzgesetzgebung ist es notwendig, konfigurierbare Zugriffsrechte innerhalb von Netzwerken im Gesundheitswesen vorzufinden. Innerhalb einer Umgebung mit Beteiligung vieler unterschiedlicher Firmen wird eine Verwaltung und Übergabe dieser Rechte zwischen den beteiligten Systemen und Geräten benötigt. Deshalb soll DICOM eine Schnittstelle und einen Umgang mit Zugriffsrechten bereitstellen.

❖ Rollenabbildung mit Hilfe der digitalen Signatur

Das Supplement 41 ermöglicht derzeit die Anwendung einer digitalen Signatur bzgl. einer DICOM - Datei durch ein Gerät. Im deutschen Signaturgesetz kann eine Signatur nur durch eine natürliche Person vergeben werden. DICOM sollte deshalb die Abbildung der Rollen von natürlichen Personen (Ärzte, Schwestern, MTA) mit Hilfe der digitalen Signatur vorsehen.

❖ Verschlüsselung von Offline-Medien

Es wird erwartet, daß eine Verschlüsselung von Offline-Medien in nächster Zeit in Europa verlangt wird und deshalb geeignete Strukturen bereitgestellt werden sollen.

❖ Sicherstellung der Integrität bei Übertragung mehrerer Dateien

Nach Supplement 41 können digitale Signaturen in DICOM nur an einzelne DICOM Dateien angehängt werden, um die Integrität dieser Datei zu sichern. Wenn eine Folge von Dateien übertragen wird und dabei eine Datei verloren geht, kann dies anhand der Signatur nicht festgestellt werden. Hierfür sollte eine Lösung bereitgestellt werden.

Darüber hinaus wird empfohlen, folgende Punkte in der weiteren Entwicklung in Betracht zu ziehen:

- Die Datenübertragungsrate sollte durch Verschlüsselungsverfahren möglichst wenig verringert werden.

- Es sollen die gesamte Kommunikation anstatt nur einzelne Daten verschlüsselt werden.
- Standardisierte oder zumindest in der Informationstechnik weit etablierte Sicherheitsverfahren sollen eingesetzt werden und eine Neuentwicklung für medizinische Daten vermieden werden.
- Eine Sicherheitsinfrastruktur soll möglichst alle Informationssysteme einer Institution im Gesundheitswesen einbeziehen. Die intensive Kooperation im Rahmen der IHE (Initiative "Integrating the Healthcare Enterprise") soll ausgebaut werden.
- Die Notfall- und Konsiliarbehandlung soll nicht durch Sicherheitsmechanismen eingeschränkt oder behindert werden.
- Unternehmen im Gesundheitswesen werden zukünftig eine Infrastruktur für ein Zugriffs-, Zugangs- und Schlüsselmanagement bereitstellen müssen.

Amerikanische Initiativen zum Datenschutz im Gesundheitswesen

In den USA haben sich mehrere Institutionen in den letzten Jahren intensiv mit dem Thema Datenschutz in der Informations- und Kommunikationstechnologie in der Medizin beschäftigt (chan99,hhs99,john99,kratz99,reyn98). Man kann dabei zwei Hauptrichtungen unterscheiden: Seit November 1999 existiert ein mehrhundertseitiger Entwurf des Department of Health and Human Services bzgl. der "Standards for Privacy of Individually Identifiable Health Information", der sehr detailliert und mit vielen Erklärungen und die unterschiedlichen Interessen und Gesichtspunkte ausleuchtende Diskussionen angereichert ist, um eine zukunftsfähige Basis für die Umsetzung eines bei der Bevölkerung vertrauensfähigen Datenschutzes in der EDV-unterstützten Medizin aufzubauen. Andererseits gibt es in einer Kombination aus Informatikern, Industrie und medizinischen Berufen Initiativen zur Erstellung gemeinsamer Anforderungen an den Datenschutz in der medizinischen Informations- und Kommunikationstechnik, die beispielsweise allgemeine Empfehlungen von ISO – Standards für den medizinischen Bereich spezifizieren oder einzelne wichtige Themen wie Protection Profiles für eine rollenbasierten Zugangskontrolle ausarbeiten und damit eine Grundlage für eine einheitlichere Handhabung und Umsetzung in den von der Industrie angebotenen Systemen herstellen wollen.

NIAP und Common Criteria Initiativen

Aus dieser zuletztgenannten Gruppe hat sich NIAP (National Information Assurance Partnership) als ein gemeinsames Programm des NIST (National Institute of Technology) und der NSA (National Security Agency) herausgebildet. Auf einem 1999 gehaltenen Vortrag wurde das im Diagramm 6-1 dargestellte Modell präsentiert (john99).

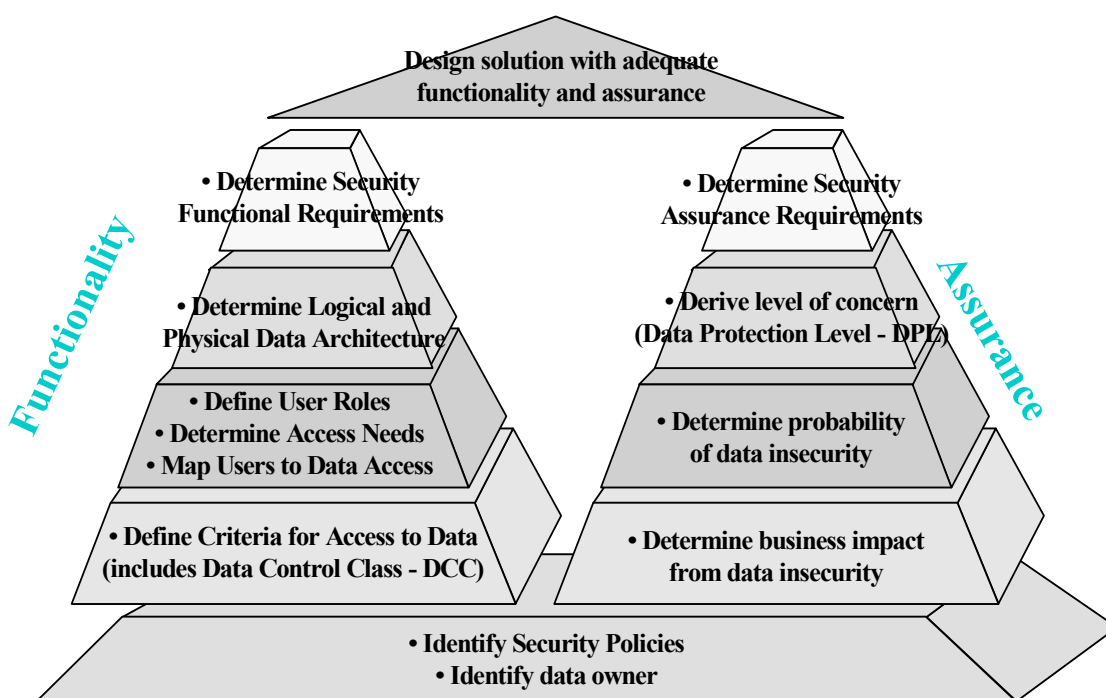


Abbildung 6-1 Defining Security Requirements (aus Vortrag: NIAP Healthcare Project Goals & Structure. Forum on Privacy and Security in Healthcare, 13.9.99, Gaithersburg, MD, USA) (john99)

Die Sicherheitsanforderungen in der Medizin sollen durch zwei Säulen aufgebaut werden: einerseits die Bereitstellung der Funktionalität (s. a. Anforderungen aus unserer Arbeitsgruppe oben), andererseits durch Maßnahmen zur Sicherung und Kontrolle der Funktionsfähigkeit. Das Säulenmodell stellt die notwendigen grundsätzlichen Abläufe dar: zuerst die Definition der Sicherheits-Policy (in einem Krankenhaus, für ein Netz oder andere gemeinschaftlich arbeitende und datenaustauschende Organisationen), anschließend die Festlegung der Kriterien für die Erlaubnis eines Datenzugangs. Danach müssen die Rollen der potentiellen Nutzer erfasst, anhand der Bedürfnisse und des Sicherheitsrisikos bewertet und mit passenden Rechten belegt werden. Die nächsten zwei Schritte betreffen die Umsetzung dieser

Regeln in eine informationstechnische Systemarchitektur sowie die konkreten funktionellen Anforderungen, die dann in die Systeme implementiert werden müssen. Für die Konfiguration eines Testsystems zur WWW-basierten Bild- und Befundverteilung wird derzeit im Klinikum Mannheim das gleiche Schema bzgl. der ersten, an den medizinischen Anforderungen ausgerichteten Schritte eingesetzt. Die Erfahrungen aus der Erprobung am konkreten System sollen anschließend zu einer Anpassung der funktionellen Anforderungen und ihrer Umsetzung führen.

Die zweite Säule basiert auf einer Bedrohungsanalyse, einschließlich der Berücksichtigung von Wahrscheinlichkeiten des Eintretens von spezifischen Ereignissen und einer Ableitung der institutionenbezogenen Liste der wichtigsten Risiken. Daraus kann geschlossen werden, welche Sicherheitsfunktionen kontinuierlich überprüft werden müssen, so daß insgesamt ein System mit angemessener Funktionalität und kontrollierter Sicherheit entsteht. In Diagramm 6-2 ist dargestellt, wie die von den Anwendern erstellten Protection Profiles, d. h. die bewertete Liste der Anforderungen, zusammen mit den entsprechend modular aufgebauten und konfigurierbaren Produkten zu einer geeigneten Systemarchitektur führen sollen (john99). Beide Seiten (Anwender und Industrie) treffen sich bei der Erstellung der systembezogenen Sicherheitsanforderungen, aus denen dann geeignete Produkte entstehen oder bereits vorhandene geeignete Produkte passend zusammengestellt und konfiguriert werden können.

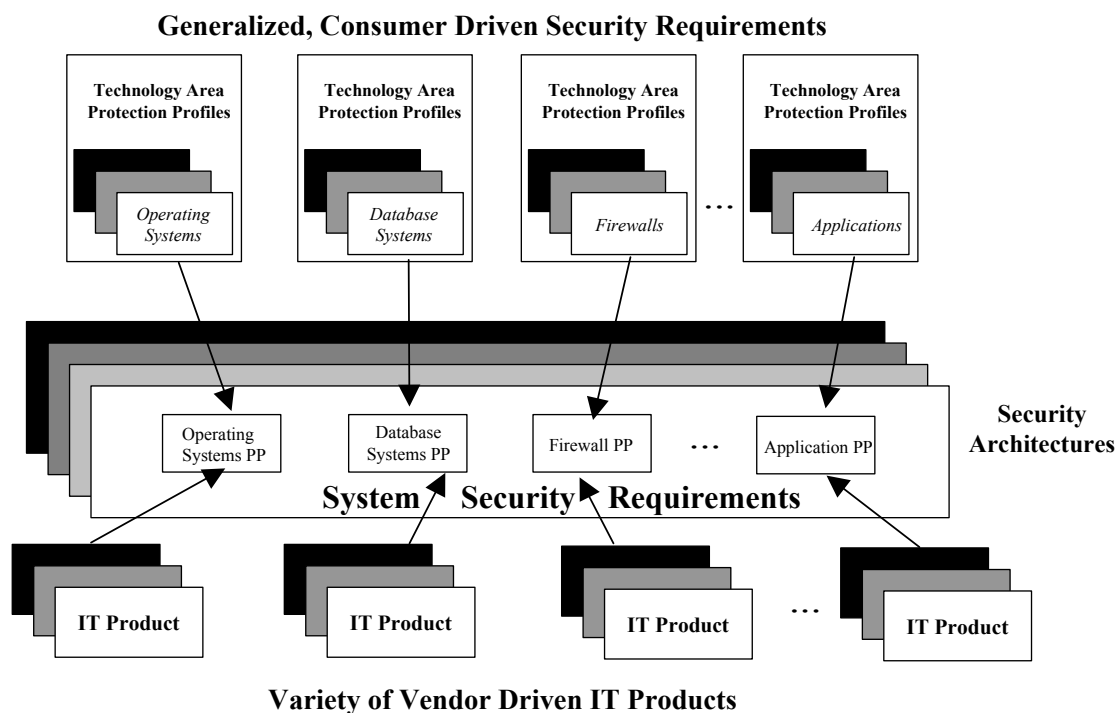


Abbildung 6-2 Role of Protection Profiles (aus Vortrag: NIAP Healthcare Project Goals & Structure. Forum on Privacy and Security in Healthcare, 13.9.99, Gaithersburg, MD, USA) (john99)

Diese Intention findet sich in Deutschland bei den gemeinsamen Arbeitsgruppen von AGIT (DRG) und medizinische Informationstechnikindustrie (überwiegend aus dem ZVEI) zu den Themen "Dicom und Workflow", "Telemedizin und Datenschutz" und "Interoperabilität" wieder. In den USA wurden auf der Ebene der "Common Criteria" – Initiative detaillierte Ausarbeitungen zu den systemspezifischen Anforderungen, auch im medizinischen Bereich, erstellt, allerdings noch vor Veröffentlichung der "Standards for Privacy of Individually Identifiable Health Information" des Department of Health and Human Services, so daß – von einer guten Basis ausgehend – Überarbeitungen wahrscheinlich notwendig sind (chan99,reyn98).

Standards for Privacy of Individually Identifiable Health Information

Mit den „Standards for Privacy of Individually Identifiable Health Information“ des Department of Health and Human Services liegt eine sehr gute Diskussionsgrundlage auch für die Weiterentwicklung und spezifische Ausarbeitung der datenschutzbezogenen Anforderungen im deutschen Gesundheitswesen vor (hhs99). Aufgrund einer bereits länger existierenden, international beispielhaften Datenschutzgesetz-

gebung in Deutschland wurde die Notwendigkeit, spezielle Regeln für den medizinischen Bereich zu entwerfen, als gering angesehen. In der praktischen Umsetzung haben sich jedoch viele Mängel gezeigt, einerseits in der zu geringen Realisierung der Anforderungen und andererseits in den Widersprüchen zu den Anforderungen der Patientenversorgung (adam98, bert98, blob95, both99, bran95, foru98, gerl99, -isu99, john99, krem99, ries99, ries99b, roge89, wein97). Auch auf die in der deutschen Teleradiologie und medizinischen Informationstechnik entstandenen Anforderungsliste sowie die offenen Fragen an die Ärztekammern zur Anwendung der Informations- und Kommunikationstechnologie (s. Kapitel 6.2 und 8.2) finden sich in dem amerikanischen Entwurf einige Antworten.

Die Erstellung der Standards for Privacy wird mit wachsenden öffentlichen Bedenken begründet, daß die elektronische Technologie zu einer substantiellen Erosion der Vertraulichkeit der Patientendaten führt (cali99, hhs99). Der Entwurf betrifft alle elektronischen Patientendaten und daraus entstehende Materialien und unterscheidet sich damit in den Definitionen des deutschen und europäischen Datenschutzrechts. In dem Entwurf wird nicht von dem Begriff persönliche Daten ausgegangen und es werden auch nicht wie in der deutschen ärztlichen Berufsordnung alle einem Arzt anvertrauten Daten eingeschlossen, sondern man spricht von "als persönlich identifizierbaren Informationen". Damit wird die Möglichkeit einer Re-Identifizierung durch Zusammenführung (Verkettung) von anonymisierten Daten und durch Verwendung weiterer Informationen aus anderen Quellen berücksichtigt. Dies stellt eine der mit ansteigenden Datenmengen zukünftig zunehmende Gefahr für die Vertraulichkeit von elektronischen Informationen dar, die in den in unseren Projekten ausgearbeiteten Anforderungen ebenso berücksichtigt ist (s. oben). Im Gegensatz zur ärztlichen Berufsordnung in Deutschland soll die Vertraulichkeit der medizinischen Informationen auf 2 Jahre nach dem Tod des Patienten begrenzt werden; in der deutschen Berufsordnung gilt die ärztliche Schweigepflicht über den Tod hinaus – ohne zeitliche Begrenzung. Hier müssen die beiderseitigen Argumente für eine vielleicht kommende Regelung in Deutschland abgewogen werden.

Grundsätze

Man geht davon aus, daß der Patient dem medizinischen Personal korrekte, detaillierte Informationen über seine Krankheit, seinen Zustand, sein Verhalten und andere Lebensumstände geben muß, damit er eine zuverlässige und passende Diagnose und Therapie erhalten kann. Um dies zukünftig zu gewährleisten und das Arzt-Patienten-Verhältnis vertrauensvoll zu halten, wird der Schutz dieser vertraulichen Daten als dringend notwendig angesehen. Das Prinzip Selbstbestimmung des

Patienten über seine Daten soll, abgesehen von den Zwecken im allgemeinen Interesse, im Vordergrund stehen; grundsätzliche Begrenzungen der Weitergabe oder Verwendung von Daten sollen nicht aufgestellt werden. Gleichzeitig wird die Aufbewahrung und der Austausch von Patientendaten als ein integraler Bestandteil der Patientenversorgung betrachtet und es werden der Anwendung von elektronischer Informationsverarbeitung klare Vorteile für den Patienten und das Gesundheitssystem als Ganzes bescheinigt. Ebenso wie in Europa existieren bisher in den USA unterschiedliche Regelungen und Gesetze in den einzelnen Staaten, während viele Organisationen und Firmen staatenübergreifend arbeiten. Auf diesen grundsätzlichen Voraussetzungen basiert der Entwurf.

Es werden folgende Ziele gesetzt:

- ❖ Reibungsloser Austausch von Patientendaten für Behandlung, Abrechnung und spezifische Zwecke in öffentlichem Interesse
- ❖ Verhinderung der Weitergabe von identifizierbaren Daten für irgendwelche andere Zwecke, soweit nicht durch spezifische und freiwillige Autorisierung durch den Patienten erlaubt
- ❖ Bereitstellung von ausgewogenen Anleitungen, durch die Personen erfahren können, wer ihre Daten nutzt und wozu.
- ❖ Bereitstellung von ausgewogenen Anleitungen, durch die Personen Zugang zu ihren Daten und eine Korrektur falscher Informationen erhalten können.
- ❖ Bereitstellung von Personen, die für die Sicherung der Patientendaten verantwortlich sind
- ❖ Definition von Verantwortlichkeiten und von Sanktionen

Bis auf den ersten spezifischen Punkt, der auf die administrativen Anforderungen im Gesundheitswesen eingeht, werden auch in der deutschen Datenschutzgesetzgebung diese Ziele verfolgt. In dem vorliegenden Entwurf werden aber die spezifischen Ausführungen auf die medizinische Situation angepaßt; es soll der Gebrauch und der Austausch von geschützter Information für die Patientenversorgung so leicht wie möglich und für andere Zwecke erschwert werden. In Deutschland fehlt bisher hierzu ein vergleichbares Werk, was zumindest in Form einer Anleitung oder Klarstellung, mit ebenso flexiblen Passagen wie der Entwurf, hilfreich wäre. In den USA sollen auch keine fixierten Ausführungsvorschriften erstellt werden, sondern jede Institution kann ihr eigenen Bedürfnisse abschätzen und geeignete Maßnahmen erstellen; für Institutionen, die diesen Aufwand nicht leisten können oder wol-

len, werden aber für viele Bereich Standardvorgaben gemacht, an die man sich dann halten muß.

Einwilligung

Grundsätzlich wird in Anwendungen unterschieden, die einer individuellen Autorisierung bedürfen oder nicht. Zur letzteren werden, wie auch in Deutschland anhand des Referentenentwurfs zur Gesundheitsgesetzreform 2000 diskutiert, Auswertungen im öffentlichen Interesse (Public Health, Wissenschaft, Gesundheitsberichte, Durchsetzung von Gesetzen) gerechnet. Bei einer individuellen Autorisierung sollen allgemeine oder pro forma – Einwilligungen nicht mehr gültig sein. Ein zentraler Aspekt soll durch das Prinzip der minimal notwendigen Datenweitergabe vertreten werden; in Deutschland geht man bereits von einer minimalen Datenerfassung aus. Daraus kann das Prinzip der minimalen Weitergabe abgeleitet werden. Im amerikanischen Entwurf werden auch explizit die Prinzipien der minimal notwendigen zugriffsberechtigten Gruppen und der minimalen Rechte genannt.

Außer für Notfälle soll zwischen Patient und Institution oder Arzt vor der Behandlung eine Vereinbarung über Verwendung oder Weitergabe seiner Daten getroffen werden. Die Nutzung der Daten für die Patientenversorgung und Abrechnung ist primär ohne Einwilligung erlaubt. Die Institution kann die vom Patienten vorgeschlagene Regelung auch ablehnen; sie muß als gegenseitiges Einverständnis über die Handhabung vorliegen. Dies soll für die Institution die Einhaltung von Verträgen mit Dritten sichern. Die Autorisierung kann vom Patienten widerrufen werden. Als Beispiele für Begründungen bzgl. von Patienten gewünschter Einschränkungen werden genannt, daß nicht jeder Arzt auf einen Zugriff auf die Patientendaten erhalten soll, weil persönliche Bekannte unter den Ärzten sind, oder daß eine Zweitmeinung ohne Wissen des behandelnden Arztes eingeholt werden soll.

Unter die ohne Einwilligung des Patienten mögliche Verwendung der Daten im Rahmen der Patientenversorgung fallen auch:

- ❖ Qualitätssicherung, auch im weiteren Sinne mit Qualitätskontrollen oder Auswertungen von Tätigkeiten medizinischen Personals, Zertifizierungs- oder Anerkennungsverfahren u.a.
- ❖ Aus- und Bewertungen durch Versicherungen, falls der Patient aufgrund eines Vertrages dieser Versicherung versorgt wird
- ❖ “Auditing Services”, z. B. Betrugs- oder Mißbrauchsaufdeckung

❖ Informationen für straf- oder zivilrechtliche Prozesse

Hier wird der Begriff "Health Care Operations" wesentlich weiter gefaßt als der deutsche Begriff "Patientenversorgung". Unter deutscher Auffassung von Datenschutz sind die Verwendungsmöglichkeiten ohne Einwilligung des Patienten enger gefaßt; dies ist schon daran zu erkennen, daß die strafrechtlich abgesicherte Ärztliche Schweigepflicht die Herausgabe von ärztlich anvertrauten Daten für eine strafrechtliche Verfolgung des Patienten, erst recht nicht für zivilrechtliche Prozesse, verbietet. Nur in einer Abwägung zu anderen sehr hochstehenden Rechtsgütern, z. B. bei Gefährdung anderer Personen, darf, aber muß nicht, ein Arzt die ärztliche Schweigepflicht durchbrechen. Ein anderer interessanter, wahrscheinlich unter amerikanischer Interessensvertretung einzustufender Punkt ist der Ausschluß von bestimmten Personen, z. B. ausländischem diplomatischen Personal, von den Schutzbestimmungen des Entwurfs.

Identifizierbare Gesundheitsinformationen

Die Definition des geprägten Begriffs "als persönlich identifizierbare Gesundheitsinformationen" (individually identifiable health information) wird als zentraler Punkt des geplanten Gesetzes ausführlich erläutert. Selbst nach Entfernung der sichtbaren Identifikationsmerkmale besteht das Risiko, daß re-identifizierende zusätzliche Informationen genutzt werden können; in einer MIT-Studie von 1997 wurde gezeigt, daß anhand der Wählerliste von Cambridge, Massachusetts, die nur die Postleitzahl und das Geburtsdatum enthielt, 97 % der Personen identifiziert werden konnten (gold97). In einer Stadt wie Manhattan kann es Hunderte von Personen geben, auf die bestimmte Merkmale wie Alter, Rasse, Geschlecht und Diagnose zutreffen können, während in einem Dorf möglicherweise diese Kriterien nur auf eine Person zutreffen und diese damit identifiziert ist.

Offensichtliche Identifikationsmerkmale können entfernt oder durch Zufallsnummern ersetzt oder verschlüsselt werden. Letztere Methode, soweit sichere Verfahren eingesetzt werden, ermöglichen eine vertrauliche Behandlung der Daten und eine Re-Identifizierungsmöglichkeit, wo notwendig, durch den Halter des Schlüssels. Als Beispiel wird ein wissenschaftliches Programm genannt, bei dessen Auswertungen eine Fehldiagnose oder -behandlung festgestellt wird und zum Nutzen des Patienten bei der ursprünglich behandelnden Institution die Re-Identifizierung erfolgt. Der Begriff "als persönlich identifizierbare Gesundheitsinformationen" wird weiter erläutert: Es sind Gesundheitsinformationen gemeint, die das Individuum erkennen lassen oder von denen man aufgrund einer vernünftigen Basis ("reasonable basis") glauben muß, daß sie zur Identifizierung des Individuums genutzt

werden können. Im Rahmen eines anderen Gesetzgebungsprozesses wurde vom amerikanischen Kongreß die Definition "identifiable" ohne den Zusatz "reasonable basis" abgelehnt, da eine absolute Sicherheit in vielen Fällen oder mit vertretbarem Aufwand im Vergleich zum Risiko nicht erreichbar ist.

Weil manche Institutionen nicht die statistischen Kenntnisse besitzen, um mit hoher Sicherheit feststellen zu können, ob alle möglicherweise identifizierenden Informationen vor Weitergabe der Daten entfernt wurden, sollen nach Ansicht der Entwurfsersteller konkrete Anleitungen gegeben werden, wann Daten in Bezug auf diese Vorschrift als identifizierbar oder nicht betrachtet werden. Generell wird empfohlen, fragliche Informationen – woimmer möglich – zu entfernen oder zu verschlüsseln (Pseudonymisierung). Erfahrene Anwender können selbst entscheiden, welche Informationen zu entfernen oder zu verschlüsseln sind. In den Anleitungen soll vorgeschlagen werden, die folgenden Informationen nicht weiterzugeben:

- ❖ Name, Geburtsdatum, die gesamte Adresse einschließlich Bundesstaat, Telefon- oder Faxnummer, E-Mail-, IP- oder WWW-Adresse, Sozialnummer, Patientenkodierungsnummern (einschließlich der krankenhausinternen), Kontonummer, Ausweis-, Führerscheinnummer und ähnliches, Fahrzeugkennzeichen,
- ❖ Fingerabdrücke, Stimmufzeichnungen, photographische Bilder
- ❖ Namen von Angehörigen und Arbeitgeber
- ❖ Generell keine Merkmale oder Kodierungen, die entweder öffentlich oder intern verfügbar sind

Weitere, nicht aufgeführte Informationen, von denen man im Einzelfall ausgehen kann, daß sie zur Identifizierung, auch in Kombination mit anderen Informationen, führen können, müssen ebenfalls entfernt werden. Als Beispiel wird der Beruf genannt, falls es sich um eine sehr ausgefallene Beschäftigung handelt. Die amerikanische Behörde stellt – auch nach ihren Ansichten – sehr hohe Ansprüche, weil diese Regelung nur für Institutionen des Gesundheitswesens gelten wird und deshalb verhindert werden muß, daß identifizierbare Daten außerhalb ihres Geltungsbereiches gelangen können. Dort gelten diese hohen oder ähnlich formulierte Datenschutzanforderungen bisher in den USA nicht. Es sollen auch Anleitungen herausgegeben werden, wie mit Testmethoden, z. B. aus der Statistik, die ausreichende Anonymisierung oder Pseudonymisierung überprüft werden kann.

Kostenschätzung

Das Department of Health and Human Services hat eine umfangreiche Kosten-Nutzen-Schätzung für die Implementierung der Standards for privacy durchgeführt. Viele einzelne Kostenfaktoren sind nur sehr ungenau oder gar nicht vorausszusehen. Der Nutzen ist in diesem Fall schwer zu messen, da die Vertraulichkeit in erster Linie als ein Recht und erst in zweiter Linie als ein Vorteil oder Nutzen zu verstehen ist. Als wesentliche Nutzenaspekte für Einzelpersonen und Gesellschaft werden die Verringerung der Bedenken bei psychischen Krankheiten, Drogenabhängigkeit, Krebsvorsorge, genetischen Tests, sexuellem Mißbrauch oder Infektionserkrankungen, z. B. AIDS, sowie generell eine erhöhte Vertraulichkeit gesehen.

Unter Einbeziehung der meisten Anforderungen werden die Kosten auf 8 Milliarden DM, über fünf Jahre angesetzt, belaufen. Die Spannbreite bewegt sich zwischen 3,5 Milliarden DM und 13 Milliarden DM über fünf Jahre. Im ersten Jahr würde dies einen Anteil von 0,09 % der angesetzten Ausgaben für das Gesundheitswesen in den USA und 1,0 % des Anstiegs der Kosten im Gesundheitswesen über fünf Jahre hinweg ausmachen.

Über die Hälfte der Kosten würde durch die Patienteninformation, -nachfragen und Korrekturen von Patientenakten entstehen. Die – in diesem Zeitrahmen – einmaligen Kosten für die Entwicklung von Policies und Verfahrensweisen würde die Gesundheitsdienstleister knapp 10 % des Gesamtumfangs, ca. 650 Millionen DM, kosten. Die Verwaltung von schriftlichen Zustimmungserklärungen würde ungefähr 550 Millionen DM über fünf Jahre begründen. Nicht eingerechnet wurden beispielsweise Kosten für die Anonymisierung bzw. Pseudonymisierung, die Überwachung von Datenaustauschpartnern oder zusätzliche Aufwendungen für Datennutzung im wissenschaftlichen Bereich.

Als Nutzen wurden die erhöhte Wahrscheinlichkeit eines Arztbesuches aufgrund des größeren Vertrauens angesetzt, was sich in einer verbesserten Versorgung für den Einzelnen, in reduzierten Kosten für die Allgemeinheit bei unverzüglicher Behandlung und verbesserter öffentlicher Gesundheit bei übertragbaren Krankheiten niederschlagen würde. Als ein Rahmen für die Diskussion der Kosten wird vorgeschlagen, an der Überlegung anzusetzen, daß die Kosten der Einführung der Vertraulichkeitsstandards pro Behandlung knapp 1 DM oder pro Versicherten 7 DM pro Jahr betragen würden, und ob die Patienten bereit wären, diesen Betrag zu übernehmen. Bei Betrachtung der einzelnen, besonders von Ansprüchen an Vertraulichkeit betroffenen medizinischen Gebiete wird allein für die psychischen Erkrankungen ein potentieller ökonomischer Nutzen (oder alternativ bei Nichtverwirklichung der Vertraulichkeitsstandards entsprechende Kosten) zwischen 400 Millionen DM und 3 Milliarden DM pro Jahr errechnet.

Stellungnahme der Zentralen Ethikkommission zur Verwendung von patientenbezogenen Informationen für die Forschung in der Medizin und im Gesundheitswesen

Ende 1999 wurde von der Zentralen Kommission zur Wahrung ethischer Grundsätze in der Medizin und ihren Grenzgebieten (Zentrale Ethikkommission) eine Stellungnahme zur Verwendung von patientenbezogenen Informationen für die Forschung in der Medizin und im Gesundheitswesen abgegeben (zent99). Grundlageninformationen, Überlegungen und Anforderungen aus diesem für Deutschland wegweisenden Papier sollen aufgrund der Bedeutung für Telemedizin und Teleradiologie vorgestellt und diskutiert werden (Kommentare in Kursivschrift).

Grundlagen

Da Gesundheitsdaten personenbezogene Daten sind, steht ihre Erhebung und Verwendung unter dem Vorbehalt der Zustimmung der betroffenen Person. Die vom Patienten mitgeteilten oder bei ihm erhobenen Informationen sind zudem durch das Arztgeheimnis geschützt; ihre Weitergabe zu Abrechnungszwecken steht unter dem Sozialgeheimnis. Jenseits dieser ethisch und rechtlich geschützten Verhältnisse bedarf eine Verwendung personenbezogener Gesundheitsdaten einer ausdrücklichen Rechtfertigung (zent99).

- 1) Personenbezogene Daten im Gesundheitswesen werden in einem großen Umfang kontinuierlich und nahezu für die gesamte Bevölkerung verarbeitet.
- 2) Sie werden in einem auch rechtlich besonders geschützten Vertrauensverhältnis offenbart.
- 3) Sie sind für die Beratung und Therapie der betroffenen Person sowie für die Bereitstellung von Geldleistungen unentbehrlich.
- 4) Sie müssen sorgfältig dokumentiert, sachkundig aufbereitet, mit anderen Informationen verglichen, beurteilt und für zukünftige Verwendungen aufbewahrt werden. Ihre Weitergabe an Dritte zur Konsultation oder Mitbehandlung sowie zur finanziellen Abgeltung der Leistungen und deren Kontrolle kann dem Rat- und Hilfesuchenden nur im Vertrauen auf einen ordnungsgemäßen Umgang mit den Informationen zugemutet werden.
- 5) Sie sind eine gesellschaftliche Ressource für die ständige Verbesserung der gesundheitlichen Versorgung. Ihre systematische Sammlung und methodische

Auswertung dient gesellschaftlich anerkannten und von den Personen, deren Informationen verwendet werden, erwünschten Zwecken. Es sind dies unter anderem

- a) das rechtzeitige Erkennen von Risiken und ihre Vorbeugung
 - b) die Kontrolle der Zuverlässigkeit diagnostischer Befunde
 - c) die Beurteilung der Wirksamkeit therapeutischer Maßnahmen
 - d) die Sicherung und Verbesserung der Qualität ärztlicher und nichtärztlicher Leistungen
 - e) die Transparenz der Kosten, nicht zuletzt auch in bezug auf ihren Nutzen, und die Unterstützung eines effektiven Managements in der Organisation und Erbringung gesundheitlicher Leistungen
 - f) die Durchsetzung des Wirtschaftlichkeitsprinzips im Umgang mit knappen Ressourcen
 - g) die Versachlichung des öffentlichen Diskurses über eine gerechte und sozial verträgliche Verteilung der Mittel.
- 6) Sie enthalten aber über die Gefahr einer Verletzung der Intimsphäre im Verhältnis zu Personen des privaten Lebenskreises und gesellschaftlichen Verkehrsbeziehungen hinaus ein Gefährdungspotential für gesellschaftliche Ausgrenzung und Diskriminierung. Im Falle des Zusammenbrechens einer freiheitlich-demokratischen Gesellschaftsordnung bieten sie Handhabe für Verfolgung und physische Vernichtung.
- 7) Ihre Zweitverwendung bietet Handhabe für wirtschaftliche und politische Fremdkontrolle.

Gegenüber dem Recht auf informationelle Selbstbestimmung und der Ärztlichen Schweigepflicht als Grundlage eines vertrauensvollen Arzt-Patienten-Verhältnisses ist das Prinzip „Wirtschaftlichkeit“ – der Begriff ist stark an ökonomische Gesichtspunkten orientiert und kann die Ängste der Patienten noch vergrößern - kritisch zu diskutieren und abzuwägen (s. Punkt 5f).

Problemstellung

Aus der Sicht des Bürgers, des Sozialversicherten oder des Patienten betrachtet, müssen zwei Interessen auch im Einzelfall gegeneinander abgewogen werden. Auf der einen Seite steht das Interesse, daß Gesundheitsdaten genutzt werden, um zum Beispiel die Qualität der Versorgung zu sichern und zu verbessern, um neue

Erkenntnisse über Gesundheitsrisiken oder über therapeutische Ergebnisse zu gewinnen oder um Informationen zur Wirtschaftlichkeit und Qualität der Versorgungsstrukturen zu erhalten. Auf der anderen Seite steht das verfassungsrechtlich geschützte Recht, daß jede Verwendung von persönlichen Daten unter dem Vorbehalt der ausdrücklichen Zustimmung der betroffenen Personen steht.

- 1) Aus sachlichen Gründen und aus Verantwortung gegenüber dem Patienten kann es bedenklich sein, die Zustimmung der betroffenen Person in schriftlicher Form einzuholen.

Es kann auch in Einzelfällen bedenklich sein, die Zustimmung der betroffenen Person in irgendeiner Form einzuholen.

- 2) Bei der Verarbeitung von Daten einer sehr großen Personenzahl kann es praktisch undurchführbar oder mit einem unverhältnismäßig hohen Aufwand verbunden sein, die Zustimmung einzuholen. Beispiele hierfür sind:
 - a) Die Verarbeitung soll über den Zweck hinausgehen, dem die betroffene Person bei der Datenverarbeitung zugestimmt hat; es ist aber nicht möglich, von allen Personen nachträglich eine Zustimmung einzuholen (zum Beispiel von Verstorbenen).
 - b) Informationen sollen aus verschiedenen Datenquellen zusammengeführt werden (data linkage).
 - c) Informationen über eine Person sollen fortlaufend erhoben werden, zum Beispiel für die Anlage einer pharmakoepidemiologischen Datenbank zur Erkennung von Arzneimittelrisiken nach der Marktzulassung oder für eine Versichertenstichprobe zur Unterstützung von Vorhaben der Qualitätssicherung. Beide Vorhaben erfordern sehr hohe Stichprobenumfänge und erwarten eine zuverlässige Zuordnung der Datensätze zu ein und derselben Person.
 - d) Die Daten sollen über eine sehr lange Frist gespeichert werden.

Für bereits existierende Daten gilt die obige Argumentationslinie. Wie auch in der amerikanischen Gesetzgebung vorgesehen, kann aber für die Zukunft ein flexibles, zumindest die meisten Fälle abdeckendes Rahmenwerk geschaffen werden, das auf einer vorherigen Vereinbarung zwischen dem Patienten und der behandelnden Institution oder Person über die Verarbeitung und Verwendung seiner Daten beruht (hhs99). Man sollte auch diskutieren, ob – wie in den USA geplant - eine zeitliche Begrenzung der Geheimhaltungspflicht von Daten Verstorbener eine in der Gesamtabwägung bessere Lösung darstellen kann.

Gerade die Zusammenführung von Informationen aus verschiedenen Datenquellen stellt durch die Reidentifizierungsmöglichkeiten und die Erstellung eines umfassenden Personenprofils die wesentliche Bedrohung für die Zukunft dar und sollte nicht als Begründung für eine Verarbeitung ohne Zustimmung angenommen werden (s. Punkt 2b); für die Anforderung der personenbezogenen Zusammenführung, z. B. auch für fortlaufende Erhebungen, müssen die heutigen und zukünftigen Möglichkeiten der Verschlüsselung (Pseudonymisierung) und zusätzlicher, z. B. organisatorischer Maßnahmen ausgeschöpft werden. Man kann verschiedene Prinzipien miteinander kombinieren, z. B.:

- ❖ *Das in USA geplante vor der Behandlung auszuübende, gegenseitige Vereinbarungsprinzip über die Verwendung der Daten (Notfälle sind von dieser Anforderung ausgeschlossen) (hhs99)*
- ❖ *Einsatz von Pseudonymisierungsverfahren zur Erhöhung der Sicherheit und dem Schutz vor zufälliger Erkennung*
- ❖ *Minimalprinzip (bzgl. Weitergabe der Daten, Zugriffsrechte nach Gruppen, Rollen und Daten)*
- ❖ *Verbot der soweit nicht durch Gesetze erlaubten Zusammenführung von Daten mit medizinischen personenbezogenen Inhalten zur Reidentifizierung von Personen; damit kann für den Fall, daß Daten außerhalb von Einrichtungen des Gesundheitswesens gelangen, eine Abschreckung durch Androhung von Sanktionen auch für außerhalb des Gesundheitswesens stehende Institutionen und Personen errichtet werden.*
- ❖ *Man kann eine Verpflichtung aufstellen, daß personenbezogene Daten (auch nach Anonymisierung; wegen der Gefahr der Re-Identifizierung durch Datenverkettung) nur an vertrauenswürdige Institutionen, die sich zur Einhaltung von Qualitätsvorgaben zum Datenschutz verpflichtet haben und die dementsprechend haftbar gemacht werden können, weitergegeben werden dürfen.*
- ❖ *Ausbau des Prinzips „Selbstbestimmung des Bürgers“, indem vertrauenswürdige Institutionen geschaffen werden, bei denen der Bürger seine medizinischen Informationen strukturiert und kontrolliert ablegen und verwalten und auch durch eigenbestimmte Definitionen und nach eigenen Vorstellungen für bestimmte Auswertungen freigeben kann. In solchen Datenbanken können auch nicht personenbezogene oder auch, falls die Zustimmung hierzu gegeben wurde, intern personenbezogene Auswertungen durchgeführt werden, aber nach außen nur nicht personenbezogene, sondern z. B. nach Gruppen eingeteilte Ergebnisse bereitgestellt werden. Diesem Ablauf wird ein Patient wahrscheinlich eher zu-*

stimmen als einer Weitergabe seiner Daten nach außen. Dahinter steht immer die Befürchtung, daß diese potentiell reidentifizierbaren Daten auch an andere, unerwünschte Institutionen oder Personen gelangen.

- ❖ *Man könnte unterschiedliche Anforderungen und Handhabungen diskutieren, je nachdem ob es sich um personenbezogene identifizierbare Daten, personenbezogene pseudonymisierte oder anonymisierte, mit sehr hoher Wahrscheinlichkeit (oder andere Definition) nicht reidentifizierbare Daten oder um nicht personenbezogene medizinische Daten (sondern beispielsweise bereits in Gruppen zusammengefaßte Daten, in denen keine reidentifizierbaren Informationen enthalten sind) handelt. Für pseudonymisierte Daten könnte eine weitere Unterteilung erfolgen, je nachdem, ob die Daten nur durch die ausgebende Institution reidentifizierbar sind, durch eine besonders geschützte vertrauenswürdige Institution (ähnlich Trustcenter) oder durch eine Gruppe zusammenarbeitender Institutionen (wie beispielsweise bei pharmakologischen Studien, die eine personenbezogene Zusammenführung der Daten sicherstellen wollen).*
- ❖ *Es sind auch Konzepte vorstellbar, in denen zwar die Pseudonymisierung in der behandelnden Institution anhand eines von der vertrauenswürdigen Institution übergebenen studienspezifischen Schlüssels erfolgt, das Pseudonym aber nicht in dieser Institution gespeichert wird und dort auch keine Möglichkeiten zur eigenständigen programmtechnischen Reidentifizierung vorliegen, sondern eine Reidentifizierung nur durch Abgabe eines – am besten auch nur einmalig gültigen – Codes durch die vertrauenswürdige Institution möglich wird. Dadurch haben die an einer Multi-Center-Studie teilnehmenden Institutionen selbst keine Möglichkeit einer Reidentifizierung, z. B. der aus einer anderen, auch an der Studie beteiligten und gleichartig verschlüsselnden Institution stammenden Daten. Sie können aber über die vertrauenswürdige Institution eine Reidentifizierung erreichen, ohne daß bei diesem Ablauf die Patientendaten über die vertrauenswürdige Institution laufen müssen, was die Sicherheit wieder reduzieren würde.*
- ❖ *Man sollte auch die Diskussion zur Einführung einer deutschland- oder europa-weiten medizinischen oder allgemeinen Identifikationsnummer für Personen wieder aufnehmen, wenn die datenschutzrechtlichen Rahmenbedingungen geschaffen werden. Gerade für die Zuordnung von Personen für übergeordnete Auswertungen wäre dies äußerst hilfreich; der Einsatz der Pseudonymisierung für solche Zwecke, der zumindest eine sofortige Erkennung, z. B. eines Bekannten, verhindert, wäre erleichtert. Derzeit sind – bei ungenügender Datenschutzumsetzung und auch bei ungenügender Anpassung der Datenschutzbestimmungen bzw. praktikabler Anleitungen im Gesundheitswesen – das Chaos*

der vielen Identifizierungscodes und der unterschiedlich geschriebenen und verwalteten Namen sowie anderer Merkmale und die sehr eingeschränkten technischen Auswertemöglichkeiten der Datensammelinstitutionen das beste Mittel zum Datenschutz. Dies sollte erst bei zukunftsgerechter Sicherstellung des Datenschutzes aufgegeben werden.

Worin das Problem der langfristigen Speicherung besteht, wird nicht ausgeführt; hier ist eine Spezifizierung erforderlich, um für dann zu formulierende Anforderungen Lösungskonzepte entwickeln zu können. In diesem Abschnitt werden nicht alle, auch praktisch umsetzbaren Möglichkeiten für einen zukünftig verbesserten Schutz der Patientendaten in Betracht gezogen.

Kritische Situationen, in denen der Persönlichkeitsschutz gegen Verwendungszwecke der Datenverarbeitung gegeneinander abgewogen werden muß, seien anhand aktueller Beispiele genannt:

- 1) Die Freiheit der Arztwahl, verbunden mit einer zunehmend beanspruchten Sachkompetenz der Patienten, führt dazu, daß gerade bei chronischen Erkrankungen die Patienten Leistungen verschiedener Ärzte und therapeutischer Einrichtungen in Anspruch nehmen. Die in dieser Situation geforderte Zusammenarbeit legt einen Austausch von Informationen auch in der ambulanten Versorgung nahe, wie er sich in den Krankenhäusern bereits eingespielt hat. Den im Entstehen begriffenen, von interessierter Seite geförderten "Netzwerken" in der ambulanten Versorgung fehlen für den Informationsaustausch eine ethische Begründung und rechtliche Garantien. Aus diesem Blickwinkel stellt sich die Frage, wie die ärztliche Schweigepflicht gesichert und der Datenschutz gewährleistet werden kann.

Gesundheitsnetzen können sehr wohl ethische Begründungen zugrunde liegen, z. B. die Verbesserung der Patientenversorgung und der medizinischen Kommunikation; allein für die medizinische Begründung der Teleradiologie, nur einem Teilbereich der Telemedizin, liegt eine umfangreiche Literatur vor (bolt98,cawt91,dall99,-fery96,fran97a,frey99,gohk97,gray97,heau99,lee98,-lloy97,mald98,muel99,repo98,stoe96,tec97,wils96). Rechtliche Garantien können immer durch Zustimmung des Patienten erreicht werden. Hierzu braucht man allerdings vernünftige, verwirklichbare Konzepte.

- 2) Die Erforschung der gesellschaftlichen Bedingungen für Entstehung und Verlauf insbesondere chronischer Krankheiten, die Beurteilung der Wirksamkeit der angewendeten Therapien und ihrer Risiken, die Abschätzung der ökonomischen Folgen gesundheitlicher und medizinischer Maßnahmen sowie

Folgen gesundheitlicher und medizinischer Maßnahmen sowie ihres therapeutischen Nutzens sind auf Informationen über große Bevölkerungskollektive angewiesen. Gleich ob diese Informationen primär durch Befragung oder Untersuchung von Personen oder sekundär durch Abschöpfen der Routinedaten der Versorgung gewonnen werden, bedeutet die Datengewinnung einen Eingriff in die Persönlichkeitssphäre der Betroffenen, dessen Verhältnismäßigkeit ebenso zu prüfen ist wie der Persönlichkeitsschutz im Umgang mit diesen Daten.

- 3) Die schrittweise Verbesserung der gesundheitlichen Versorgung hinsichtlich ihrer Ergebnisse, zum Beispiel im Erreichen von Versorgungszielen und unter Bezug auf die Wirtschaftlichkeit in der Erbringung der Leistungen, zwingt zu einer Ordnung des Leistungsgeschehens unter Systemaspekten. Bezogen auf Gesundheitsziele, werden geeignete Maßnahmen einander folgerichtig zugeordnet und implementiert. Diese Strategie zur Verbesserung der Leistungsfähigkeit des Gesundheitswesens, derzeit unter den Begriffen "Health Maintenance Organization", "Disease Management" oder "Case Management", aber auch auf kommunalen Gesundheitskonferenzen diskutiert und angewendet, kann jedoch nur dann zu den angestrebten Erfolgen führen, wenn die eingeleiteten Maßnahmen evaluiert werden können. Eine Evaluation ist ohne den Zugriff auf die Routinedaten der Versorgung, ohne eine den Evaluationszielen entsprechende Gestaltung dieser Daten und eine hohe Zuverlässigkeit des Personenbezuges unmöglich. Vorliegende Planungen zum Einsatz der genannten Strategien zu mehr Qualität und mehr Wirtschaftlichkeit im Gesundheitswesen entbehren weithin, wenn man von allerdings bemerkenswerten Ausnahmen absieht (zum Beispiel Lowrance Report*), einer ethischen Begründung und einer Erwägung interner und externer Kontrollen zur Einhaltung des Persönlichkeitsschutzes.

Schlußfolgerungen und Vorschläge

Ein striktes Verbot der Verarbeitung von personenbezogenen Daten über die Gesundheit unterbindet die Erfüllung wesentlicher Funktionen der Gesundheitssicherung, auf die der Bürger vertrauen muß, insbesondere wenn er zur Finanzierung des Gesundheitssystems gesetzlich verpflichtet wird. Die Aufhebung oder Lockerung des Verbots der Verarbeitung läuft dagegen Gefahr, den Schutz der Persönlichkeit wieder preiszugeben, der gerade durch das Verbot gewährleistet werden soll. Dieses Spannungsverhältnis läßt sich nur auflösen, wenn Optimierungen konkret und eindeutig benannt werden. Die Optimierungen müssen den Schutz der

Persönlichkeit auf der einen Seite und die Erfüllung der für den Bürger wesentlichen Funktionen des Gesundheitswesens, die nur durch die Verarbeitung personenbezogener Daten erfüllt werden können, auf der anderen Seite auszuwogen in Einklang bringen. Optimierungen sind weithin Einzelfallentscheidungen unabhängiger und hierfür kompetenter Gremien.

Bei Zustimmung zu den Grundaussagen muß aber darauf hingewiesen werden, daß, anders als bei wissenschaftlichen Patientenstudien, die Zahl der Einzelfallentscheidungen sehr hoch wäre und dies ein insgesamt zu aufwendiges und wahrscheinlich zu langwieriges Verfahren darstellen würde. Das amerikanische Konzept oder ein ähnliches, ggf. auch feiner aufgegliedertes Stufenkonzept, bei dem es für die üblichen Fälle und für Institutionen ohne entsprechende Gremien und ohne Erfahrung im Umgang mit sensiblen Daten Standardvorgaben, z. B. für die De-Identifizierung, gibt, aber kompetente Institutionen in eigener Verantwortung und, wie bisher, unter zumindest stichprobenartig stattfindenden Kontrollen oder z. B. nach Prüfung und Genehmigung durch eine Beurteilungsinstanz von den Standardvorgaben abweichen dürfen, würde den Aufwand deutlich reduzieren.

Gegen den ethischen und rechtlichen Grundsatz, die Selbstbestimmung der Persönlichkeit über ihre Informationen zu achten, sind die Verwendungszwecke in ihrer Bedeutsamkeit abzuwägen. Dabei ist zunächst die Erforderlichkeit zu prüfen, das heißt, ob der Verwendungszweck nicht auch auf anderem Wege zu erreichen ist oder der Persönlichkeitsschutz durch Anonymisierung (sogenannte Einwegverschlüsselung) gewährleistet werden kann (zent99). Dabei gilt es zu beachten:

- 1) Vermeiden der Exposition für gesellschaftliche Ausgrenzung.
- 2) Garantien für das ärztliche Berufsgeheimnis bei der "sekundären" Verwendung von Patientendaten.
- 3) Verhältnismäßigkeit von Nutzen und Risiko für die Personen, deren Informationen verwendet werden.
- 4) Unterscheidung zwischen Informationen, die Kernbereiche der Persönlichkeit betreffen, und solchen, die zwar auf die Person beziehbar, aber eher peripherer Natur sind.
- 5) Ausschöpfen der gegebenen technischen und organisatorischen Möglichkeiten, die ausdrückliche Zustimmung der betroffenen Person für die Verarbeitung ihrer Informationen zu erhalten.
- 6) Anonymisierung der personen- und institutionenbezogenen Kennungen in allen Fällen, in denen der Verwendungszweck es zuläßt, und unter Ausschöpfung aller zu diesem Zeitpunkt bekannten technischen (kryptographische Verfahren

oder Umsetzungstabellen) und organisatorischen Möglichkeiten (zum Beispiel Vertrauensstelle) des Datenschutzes und der Datensicherheit.

- 7) Verbot der Zusammenführung von Patienten- oder Versichertendaten zu dem Zweck, eine wirtschaftliche oder gesundheitliche Kontrolle über einzelne Personen auszuüben.
- 8) Ausschluß der Möglichkeit, durch die Verfügung über Patienten- und Versichertendaten Wettbewerbsvorteile zu erlangen oder (gesundheits)politische Kontrolle auszuüben.

Wie hier aufgeführt, sollten moderne Konzepte und Verfahren sowie deren Kombinationsmöglichkeiten in möglichst großem Umfang und unter Zurückstellung des kurzfristigen finanziellen Aufwands in die Betrachtung einbezogen werden, weil daraus der Gegensatz zwischen Vertraulichkeit und anderen, z. B. öffentlichen Interessen leichter ausgeglichen werden kann. Zur Abschätzung der Kosten und des Kosten-Nutzen-Verhältnisses einer umfassenden Datenschutzzumsetzung im Gesundheitswesen soll auf die Ausarbeitung des Department of Health and Human Services hingewiesen werden (hhs99). Eine Handhabung nach dem Entweder – Oder - Prinzip sollte, wie auch dort genannt, möglichst vermieden werden (hhs99).

Über das amerikanische Konzept hinausgehend und die Sicherheit erhöhend wäre eine Verwirklichung des vorgeschlagenen Verbots der Zusammenführung von Patienten- oder Versichertendaten. Diese Anforderung sollte nicht nur für die Verwendung der Daten innerhalb der Institutionen des Gesundheitswesens (wie derzeit in den USA wegen der Kompetenzbeschränkungen nur möglich) gelten sondern für alle Rechtspersonen in Deutschland oder besser bei entsprechender Harmonisierung in Europa, idealerweise irgendwann weltweit. Es ist zu diskutieren, ob die Einschränkung des Verwendungszwecks und die damit zu erzielende Erhöhung der Sicherheit - bei Abwägung der anderen im Artikel aufgeführten Anforderungen - besser durch expliziten Ausschluß eines Zwecks oder umgekehrt durch Benennung eines erlaubten Zwecks erreicht werden kann.

Die Unterscheidung nach mehr oder weniger sensiblen Daten ist kritisch zu betrachten. Bereits die äußerst geringe Information, daß jemand einen Arzt aufgesucht hat, ist als sensibel einzustufen und diese Information ist bei einer Identifizierung fast immer enthalten. Man muß nur an einen Kandidaten für ein hohes politisches Amt denken, der sich für einen Arztbesuch, der sofort Spekulationen aufwirft, rechtfertigen muß. Aus wenigen Spuren können bei den zu erwartenden zukünftigen Möglichkeiten der Datensammlung und –verarbeitung Profile einer Person erstellt werden; zu diesem Aspekt der vielen minimalen Informationen sollten das

Bewußtsein in der Bevölkerung eher erhöht und die potentiellen Gefahren berücksichtigt werden.

Unter Berücksichtigung rechtlicher Vorgaben sollen differenzierte Erwägungen, die sich an geltenden und anerkannten Werten orientieren, erfolgen:

- ❖ auf das individuelle Risiko unter Erwägung von Kern- und Randbereichen der Persönlichkeit (nicht alle Gesundheitsdaten sind im engeren Sinne sensibel und bedürfen in gleichem Maße des Schutzes)
- ❖ auf das Vertrauensverhältnis, in dem die Informationen gegeben werden (Arzt- und Patientengeheimnis)
- ❖ auf Persönlichkeitswerte wie den Schutz der Gesundheit und die Qualität der Gesundheitsversorgung, die mit der "informationellen Selbstbestimmung" insoweit konkurrieren, als sie eine Auswertung von Patientendaten erfordern
- ❖ auf die Zumutbarkeit im Rahmen solidarischer Bindungen der betroffenen Personen (zum Beispiel der Mitwirkungspflicht der Versicherten nach SGB V § 1 Abs. 2)

Die Kritik an einer Unterscheidung anhand der Sensibilität von medizinischen Daten erfolgte bereits oben; hinzu kommt noch die Frage, wer darüber entscheiden soll. Eine Entscheidung über die Sensibilität einer Informationen müßte personenbezogen gefällt werden, da dies von den jeweiligen Lebensumständen abhängt (s. obiges Beispiel). Dies wäre aber praktisch unmöglich und würde darüber hinaus den Datenschutz sogar primär reduzieren, da für eine Entscheidung gerade diese zu schützenden Informationen notwendig wären.

Man könnte sich überlegen, ob wie vorgeschlagen, der situative Kontext, in dem die Information gegeben wird, berücksichtigt werden soll; als Beispiel wird das Vertrauensverhältnis genannt. Man könnte beispielsweise unterscheiden, ob die Informationen im Rahmen eines Formblattes der Krankenhausverwaltung oder bei Schilderung der Beschwerden und Umstände gegenüber dem Arzt oder der medizinischen Hilfsperson bereitgestellt wurden. Falls wirklich in einem zukünftigen Gesetz eine Unterscheidung, insbesondere mit der Folge einer Verringerung des Datenschutzes für bestimmte Informationen, getroffen werden sollte, müßten die Patienten bei Bereitstellung dieser Information explizit auf diese Einschränkung des sonst üblichen Datenschutzes aufmerksam gemacht werden. Der amerikanische Vorschlag bietet hierzu das auch für diese Fälle hilfreiche Konzept einer gegenseitigen Vereinbarung zwischen Patienten und den medizinischen Leistungserbringern (Ärzten oder

Institutionen) an. Hierdurch kann eine Weitergabe von beispielsweise administrativen Daten, z. B. für weitere interne oder externe Auswertungen, erleichtert werden. Die Patienten werden für solche Zwecke - bei entsprechender Erklärung und Zusicherung der Datenschutzgewährleistung im Rahmen des Verarbeitungsprozesses - , zumindest wenn man von der heutigen Verhaltensweise ausgeht, ihre Zustimmung überwiegend erteilen. Nach amerikanischem Muster kann eine Institution die Behandlung eines Patienten auch ablehnen, wenn keine einvernehmliche Entscheidung gefunden werden kann; Notfälle sind anders geregelt.

Die Einhaltung der Grundsätze, wie sie von der Europäischen Richtlinie und wissenschaftlichen Fachgesellschaften vorgeschlagen werden, ist ohne rechtliche Garantien und angemessene organisatorische Vorkehrungen nicht zu erwarten. Es bedarf eines gesetzlichen Rahmens für Entscheidungen, die unter Bezug auf konkrete Zwecke verbindlich getroffen werden können. Zu diesem Zweck ist die Einrichtung von unabhängigen und kompetenten Beurteilungsinstanzen, die die für eine Entscheidung erforderlichen Abwägungen sachkundig vornehmen, zu fordern.

Für die Einrichtung von Beurteilungsinstanzen im Gesundheitswesen ("institutionalized review boards"), denen die erforderliche Rechtsgüterabwägung zur Gewährleistung des Persönlichkeitsschutzes bei der Verwendung von Gesundheitsdaten verantwortlich übertragen werden sollten, können die Ethikkommissionen der Ärztekammern und der Medizinischen Fakultäten wegweisend sein. Diese sind interdisziplinär zusammengesetzt, ihr gehören Vertreter der gesellschaftlich relevanten Gruppen an, sie sind unabhängig, sie können problembezogenen Expertisen anfordern. Es gibt einen ständigen Erfahrungsaustausch; bei einander widersprechenden Entscheidungen gibt es Gremien der Konsensfindung wie die Arbeitsgemeinschaft der Ethikkommissionen oder die Zentrale Ethikkommission bei der Bundesärztekammer.

Die Aufgaben und Befugnisse solcher internen, unabhängigen und kompetenten Instanzen sollten allerdings nach drei Richtungen hin präzisiert werden.

- 1) Hinsichtlich ihres sachlichen Inhalts sollten die von ihnen getroffenen Entscheidungen bei den Datenschutzbeauftragten des Bundes beziehungsweise der Bundesländer sowie bei den Aufsichtsbehörden der Sozialversicherung grundsätzlich Anerkennung finden.
- 2) Die Patientendaten der von ihnen geprüften und befürworteten Vorhaben müssten strafrechtlich den gleichen Schutz genießen wie unter dem ärztlichen Berufsgeheimnis.

- 3) Sie müßten sich vorausschauend mit den ethischen und rechtlichen Fragen der Nutzung von personenbezogenen Informationen über die Gesundheit für die Forschung und für das Management im Gesundheitswesen mit der Zielsetzung beschäftigen, die Risiken eines möglichen Mißbrauchs zu minimieren.

Die Erweiterung um wesentliche Aufgaben und Befugnisse erfordert jedoch eine Transparenz und Begründungspflicht der Entscheidungen, verbunden mit der Pflicht öffentlicher Berichterstattung.

Bei der Umsetzung der Datenschutzrichtlinie der EU sind die hierfür derzeit fehlenden rechtlichen Rahmenbedingungen (Bundesdatenschutzgesetz, Sozialgesetzbuch, Strafprozeßordnung, Strafgesetzbuch) zu schaffen.

Übergeordnete Beurteilungsinstanzen mit den obengenannte Aufgaben und Befugnissen sind bei der Verwirklichung eines verbesserten Datenschutzes und gleichzeitig verbessertem Datenfluß für die Aufgaben des Gesundheitswesens hilfreich. Diese Instanzen sollten auf Anfrage für eine Beurteilung und Absicherung eines von einer betroffenen Institution entworfenen Konzeptes, möglicherweise auch für eine Kontrolle von Institutionen im Gesundheitswesen zur Verfügung stehen. Ein Genehmigungsprinzip wäre, wie oben begründet, nur für Konzepte, aber nicht regelmäßig für Einzelentscheidungen praktikabel. Ebenfalls wie oben aufgeführt, würde eine Stufenkonzept die Realisierung und die Handhabung erleichtern: Wenig erfahrene Institutionen könnten durch Standardvorgaben zur Verfahrensweise eine praktische Hilfestellung und grundsätzlich einzuhaltende Anleitung erhalten, während erfahrene Institutionen, ggf. mit Absicherung durch die vorgeschlagenen Beurteilungsinstanzen, auch eigenständige Konzepte zum Umgang mit medizinischen Daten und Patienteninformationen entwickeln können.