Anforderungen des Datenschutzes an die Medizinische Informatik

Klaus Pommerening

Institut für Medizinische Statistik und Dokumentation
Johannes-Gutenberg-Universität, D-55101 Mainz
Email: pom@anke.imsd.uni-mainz.de

Bei der Modellierung, Konzeption und Implementation von Informationssystemen in der Medizin müssen die Anforderungen des Datenschutzes mit besonderer Dringlichkeit berücksichtigt werden. Bestehende Krankenhausinformations-, Abteilungs- und Arbeitsplatzsysteme lassen die Risiken für die in ihnen gespeicherten und übermittelten Daten weitgehend außer Acht. Die existierenden technischen Konzepte für den Datenschutz müssen daher so bald wie möglich in die Praxis umgesetzt werden. Die Medizin-Informatiker sind aufgerufen, diese Konzepte beim Aufbau von medizinischen Informationssystemen endlich zu berücksichtigen und wo nötig weiterzuentwickeln.

1 Probleme und Initiativen

Die Medizinische Informatik beschäftigt sich mit der systematischen Informationsverarbeitung in der Medizin, insbesondere mit der Modellierung von Informationsfluß und -speicherung zwischen und innerhalb von Institutionen des Gesundheitswesens. Da die Medizin mit besonders sensitiven personenbezogenen Daten umgeht, sind die Anforderungen des Datenschutzes in diesem Bereich besonders hoch und müssen bei der Modellierung, Konzeption und Implementation von Informationssystemen mit besonderer Dringlichkeit berücksichtigt werden.

Die Informatisierung von Arztpraxen und Krankenhäusern macht rapide Fortschritte. Durch die Einführung von Informations- und Kommunikationstechik soll die Qualität und Effizienz der Gesundheitsversorgung verbessert werden. Personalcomputer, Server und Netze werden installiert und betrieben, obwohl sie ohne besondere Maßnahmen keinen wirksamen Schutz gegen Ausspähung und Verfälschung der gespeicherten oder übermittelten Daten bieten. Das Eindringen offener Informations- und Kommunikationssysteme in das Gesundheitssystem läßt die Gefährdung der empfindlichsten persönlichen Daten immer weiter wachsen. Informationstechnische Systeme, speziell in der Medizin, sollten aber so konzipiert und konstruiert werden, daß sie das Recht auf Vertraulichkeit auf allen Ebenen wirksam schützen.

Die Grundprobleme für den Datenschutz in der Medizin sind

1. die mangelhafte rechtliche Situation,
2. organisatorische Unzulänglichkeiten,
3. fehlende Umsetzung der existierenden Technik.

Die mangelhafte rechtliche Situation ist durch widersprüchliche und inkonsistente Vorschriften und durch die Subsidiarität der Datenschutzgesetze gekennzeichnet. Die organisatorischen Unzulänglichkeiten zeigen sich in fehlenden Regelungen für Verantwortlichkeiten und in der

mangelnden Motivation der Beteiligten, wirksame Datenschutzmaßnahmen einzuführen. Existierende Sicherheitstechnik, wie kryptographische Protokolle oder PC-Sicherheitssysteme, bleibt in der Praxis weitgehend unbeachtet.

Es gibt verschiedene internationale und europäische Initiativen zur Verbesserung von Datenschutz und Datensicherheit in der Medizin. Daneben hat auch die in Deutschland zuständige Fachgesellschaft GMDS (Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie) eine Arbeitsgruppe „Datenschutz in Krankenhausinformationssystemen“ gegründet, aus deren Arbeit wesentliche Teile dieses Vortrags entstanden sind [1]. Die Aufgabe dieser Arbeitsgruppe ist vor allem die Erstellung eines modellhaften Datenschutzkonzepts für Krankenhausinformationssysteme. Bisher wurde als Grundlage dafür ein Positionspapier „Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen“ erarbeitet [1]. Ein weiterer Schwerpunkt war die Diskussion der Datenschutzprobleme, die das GSG mit sich bringt, und das Suchen nach Lösungsvorschlägen. Wesentlich für die Arbeitsgruppe ist auch die künftige Mitarbeit in den entsprechenden Working Groups der internationalen Medizin-Informatik-Vereinigungen IMIA und EFMI.

2 Datenschutz im Krankenhaus

Die allgemeinen Datenschutzanforderungen für medizinische Daten müssen in der speziellen Situation eines Krankenhauses weiter präzisiert werden.

2.1 Die Organisation des Krankenhauses

Das Krankenhaus ist arbeitsteilig organisiert. Während eines Krankenhausaufenthalts wandert der Patient durch mehrere Fachabteilungen zu verschiedenen Untersuchungen; Blut- und andere Proben werden an verschiedene Laboratorien übergeben. Patienten-Stammdaten werden von der Klinksverwaltung bearbeitet, ebenso die Abrechnung mit den Kostenträgern. An allen diesen Stellen fallen Daten an, die gespeichert und übermittelt werden müssen. Dennoch kann der Krankenhausbetrieb nicht als informationelle Einheit angesehen werden, in der uneingeschränkt Patientendaten ausgetauscht und verwendet werden dürfen. Vielmehr dürfen diese Daten nur im Rahmen der Zweckbestimmung des Behandlungsvertrags verarbeitet werden; sie sind unter Verantwortung der erhebenden Stelle oder der Stelle ihrer überwiegenden Verwendung zu speichern und dürfen nur bei Bedarf nach einem überprüfbaren Verfahren anderen Leistungsstellen offenbart werden. Sie unterliegen also der Datenhoheit der Fachabteilung.

Der Patient willigt mit dem Abschluß des Behandlungsvertrags zwar darin ein, daß Daten über ihn erhoben und gespeichert werden; er hat aber das Recht darauf, daß nur die jeweils erforderlichen Teilinformationen aus der Krankenakte anderen an der Behandlung beteiligten Personen oder Stellen offenbart werden. Auch die Krankenhausverwaltung darf nur zu den Daten Zugang haben, die für ihre Zwecke erforderlich sind.

Für eine vertiefte Darstellung der Situation und die Herleitung im Begründungszusammenhang sei auf [9] verwiesen.

2.2 Krankenhausinformationssysteme

Ein Krankenhausinformationssystem (KIS) ist ein kompliziertes Geflecht von verschiedenen, oft verschiedenartigen Subsystemen. Es gibt, besonders in kleineren Krankenhäusern, gele-

gentlich zentrale Systeme; der Normalfall ist heute aber ein dezentrales System mit Arbeitsplatzsystemen, Abteilungssystemen, einigen zentralen Datenbanken und einem globalen Informations- und Kommunikationssystem. Die Daten müssen zur rechten Zeit am rechten Ort zugänglich sein. Die Krankenakten werden in verschiedenen Teilen an verschiedenen Stellen geschrieben und müssen eine Vielfalt verschiedener Sichten bieten. Hersteller und Betreiber solcher Systeme sind froh, wenn die Kommunikation zwischen den Subsystemen irgendwie klappt und schrecken davor zurück, zusätzliche Komplexität in Form von Datenschutzmaßnahmen einzuführen.

Für das gesamte Krankenhaus sollte ein einheitliches Konzept existieren, das Verantwortlichkeiten, Prozeduren und Zugriffsrechte definiert. Dieses Gesamtkonzept muß in jedem Teil des Systems implementiert und nach dem Stand der Technik abgesichert werden. Jedes Krankenhaus, vielleicht sogar jede Abteilung, sollte einen Sicherheitsbeauftragten haben. Krankenhausnetze müssen von Fernverkehrsnetzen abgekoppelt werden, sei es physisch oder logisch (durch kryptographische Techniken), zumindest durch einen Firewall.

Die Patientendaten sind nach dem Stand der Technik zu schützen, wobei aber das Prinzip der Verhältnismäßigkeit zu beachten ist. Insbesondere für medizinische Daten ist wegen ihrer Sensitivität ein hoher Sicherungsaufwand geboten. Durch technische und organisatorische Maßnahmen muß gewährleistet sein, daß nur der zuständige Arzt und, soweit für die Behandlung nötig, mitbehandelnde Ärzte und Pflegepersonal die Patientendaten lesen oder im zulässigen Rahmen weitergeben können.

Wie soll dies in Krankenhausinformationssystemen verwirklicht werden? Natürlich ist keine vollständige Sicherheit erreichbar. Es läßt sich aber prinzipiell mit dem Stand der Technik ein angemessenes Sicherheitsniveau erreichen. Zu beachten sind dabei auch psychologische Aspekte bei Benutzern, Entwicklern und Vertreibern von Krankenhausinformationssystemen.

2.3 Die Motivation von Benutzern, Entwicklern und Vertreibern

Ein möglicher Grund für die mangelhafte Datenschutzpraxis im medizinischen Bereich ist, daß die Mediziner die Notwendigkeit von Maßnahmen nicht einsehen – es gibt nur wenige bekannt gewordene spektakuläre Fälle von Datenschutzverletzungen in diesem Bereich. Außerdem fürchten sie zusätzlichen Streß und Hindernisse im Arbeitsablauf. Sie fürchten, daß Datenschutzmaßnahmen eine Menge Geld und Zeit kosten und sich nicht lohnen. Die Medizin-Informatiker sollten hier ganz klar machen, daß moderne Sicherheitstechniken für Anwender und Systembetreiber nicht besonders kompliziert sind. Voraussetzung dafür ist, daß diese Techniken bereits beim Systemdesign berücksichtigt und als integrierte Systemleistung konzipiert werden. Eine ideale Sicherheitsmaßnahme scheint die Verwendung von Chipkarten (als Professional Cards) zu sein, die mit kryptographischen Funktionen ausgestattet sind. Sie machen Systemzugang (als Paßwortersatz) und Datenzugriff (über kryptographische Funktionen) einfach und trotzdem sicher und veranlassen den Besitzer, besonders wenn sie mit der elektronischen Unterschrift gekoppelt sind, die Sicherheit ernst zu nehmen. Alle anderen Sicherheitsmaßnahmen sollten vor dem Benutzer verborgen bleiben, solange er sich legal verhält. Ein Detailbeispiel für ein benutzerfreundliches Design: Eine Login-Logout-Sequenz ist für einen Wechsel der Zugriffsrechte in einer zeitkritischen Situation völlig ungeeignet; statt dessen sollte der Wechsel fliegend durch Wechsel der Chipkarte möglich sein, ohne daß man die laufende Anwendung verlassen muß.

Die Sicherheitsmaßnahmen sollen die Aufmerksamkeit des Arztes nicht vom Patienten ablenken. Zwar sind Datenschutzmaßnahmen ohne Mitwirkung der Beteiligten nicht zu verwirklichen, aber die Belastung des medizinischen Personals durch organisatorische und technische Verfahren ist zu minimieren. Der sachgerechte Umgang mit den Patientendaten darf durch Schutzmaßnahmen nicht beeinträchtigt werden. Die Verfügbarkeit der Daten, besonders in kritischen Situationen, ist im Interesse des Patienten zu gewährleisten. Technische Datenschutzmaßnahmen sollen den freien Austausch nichtgeschützter Informationen möglichst wenig behindern, z. B. den Zugriff auf externe Informationsdienste wie DIMDI und elektronische Post. Auch die Verwendung der Daten für Forschungszwecke soll, soweit die Datenschutzanforderungen für wissenschaftliche Forschungsvorhaben erfüllt sind, gewährleistet sein.

Hersteller und Entwickler von medizinischen Informationssystemen sehen Datenschutz und Datensicherheit anscheinend nicht als positive Systemeigenschaft an, mit der man attraktive Werbung machen kann; negative Konzepte wirken nicht verkaufsfördernd. Es gibt einen großen Markt für billige Hardware und spektakuläre Software wie grafische Benutzungsoberflächen. Der Markt für sichere Systeme ist dagegen sehr klein; diese sind daher auch unverhältnismäßig teuer. Benötigt werden klare Sicherheitsstandards für alle medizinischen Anwendungsbereiche, auf die sich Entwickler stützen können. Solche Standards vorzuschlagen, ist ebenfalls Aufgabe der Medizin-Informatik.

2.4 Ansatz zu einem Datenschutzkonzept

Wegen großer Unterschiede in den Krankenhäusern gibt es kein allgemeines Modell für Krankenhausinformationssysteme; erst recht kann kein einheitliches Datenschutzmodell entwickelt werden. Daher muß man sich bei Empfehlungen auf möglichst allgemeingültige Ansätze und systemunabhängige oder anpaßbare Vorschläge beschränken, z. B. bei der Schwachstellen- und Bedrohungsanalyse, der Identifikation relevanter Subjekte und Objekte, der grundsätzlichen Definition von Zugriffsrechten und bei Empfehlungen für Sicherheitsmaßnahmen organisatorischer oder technischer Art. Die Differenzierung der Bedrohungen ist nicht so wichtig, da die Datenschutzvorschriften sowieso bestmögliche Sicherung nach dem Stand der Technik verlangen. Zu beachten ist allerdings, daß die Wartung komplizierter Datenbanksysteme oft nur mit realen Daten sinnvoll ist, im Gegensatz zur oft erhobenen Forderung nach Wartung mit Testdaten. Einziger Ausweg: Überwachung und Aufzeichnung der Aktionen des Wartungspersonals.

Aus der Grundsatzerklärung der Arbeitsgruppe folgen einige Vorgaben für ein Sicherheitskonzept in Krankenhausinformationssystemen:

- Daten werden in der Verantwortung der erhebenden Abteilung gespeichert und sind vor anderen Abteilungen zu schützen.
- Die erhebende Abteilung verwaltet auch die Zugriffsrechte zu den Daten (Prinzip der logischen Überweisung).

Die naheliegende Realisierung dieses Modells besteht also aus einem System von Abteilungsservern, die ihre Zugriffsrechte selbst verwalten, und Abteilungsnetzen, wobei die Kommunikation zwischen den Abteilungen über ein Backbone-Netz stattfindet. Insbesondere ist die Netztopologie nicht nach Gebäuden, sondern nach Abteilungen zu gliedern. Die Abteilungssubnetze werden durch Router, eventuell sogar durch Firewallsysteme getrennt. Auf lange Sicht sollte man die Subnetze aber besser logisch durch kryptographische Protokolle trennen.

Bei den Zugriffsrechten ist zu unterscheiden zwischen statischen Zugriffsrechten, die an die Person gebunden sind, und dynamischen Zugriffsrechte, die an die Rolle gebunden sind. Die Zugriffsrechte sind nach den Hierarchieebenen innerhalb einer Abteilung zu gliedern: Chefarzt, Oberarzt, Stationsarzt (sieht nur seine Patienten), usw. Analog ist die Hierarchie beim Pflegepersonal (etwa Oberschwester) zu berücksichtigen. Weitere relevante Rollen sind: Forscher, Medizinstudent, Krankenhausverwaltung, Patient (der Rechte an seinen eigenen Daten hat), Arztsekretariat. Nicht vergessen werden dürfen die Notfallzugriffsrechte!

Die Differenzierung von Schutzstufen für die Daten im Krankenhaus erscheint mir von geringerer Bedeutung, denn grundsätzlich ist im Zweifelsfall ist die höhere Schutzstufe zu unterstellen; sind Maßnahmen für die höhere Schutzstufe nicht teurer, sind sie auch für die niedrigere Schutzstufe anzuwenden. Besser ist es, im Modell konsequent das 'need-to-know'-Prinzip anzuwenden.

Mögliche allgemeingültige Empfehlungen für Sicherheitsmaßnahmen sind

- grundsätzlich verschlüsselte Datenspeicherung,
- grundsätzlich verschlüsselte Kommunikation (Datenübermittlung),
- überprüfbare Zugriffskontrolle (mandatory) aufgrund einer systemweit definierten Zugriffsmatrix,
- elektronische Unterschrift von Verordnungen, Leistungsanforderungen, Kommunikation, Dokumentation,
- zentrales Schlüsselverzeichnis (mit zentraler Zertifikationsinstanz),
- Chipkarten als persönlicher Ausweis und Schlüsselablage (Professional Card),
- Firewall- und andere Netzsicherheitstechniken,
- Einsatz von PC-Sicherheitssystemen,
- organisatorisch: Verpflichtung, Schulungen, …

Die technischen Schutzmaßnahmen sollen als Systemleistung konzipiert werden, die vom Benutzer kontrollierbar, aber nicht ohne weiteres abschaltbar ist. Als technische Absicherung müssen Patientendaten (wie auch andere möglicherweise vertrauliche Daten) per Systemvoreinstellung gegen Einsichtnahme und Übermittlung geschützt sein; die jeweilige Freigabe muß ein bewußter Akt sein und richtet sich nach der im Datenmodell definierten Zugriffsmatrix (Sicherheitsprinzip des geschlossenen Systems).

2.5 Sicherheitsinfrastruktur für Krankenhausinformationssysteme

Die technischen und organisatorischen Datenschutzmaßnahmen in einer Klinik sind nicht nebenbei zu erledigen. Sie erfordern die Schaffung einer entsprechenden Infrastruktur und eine klare Festlegung der Verantwortlichkeiten sowie die Einplanung eines angemessenen finanziellen und personellen Aufwands, insbesondere für einen Sicherheitsverantwortlichen.

Für medizinische Anwendungssysteme aller Arten sind geeignete technische Standards in Anlehnung an die IT-Sicherheitskriterien [11] wünschenswert, die man den Herstellern gegenüber durchsetzen kann und die die Planung und Beurteilung von Systemen erleichtern. Insbesondere ist eine geeignete kryptographische Infrastruktur zu definieren und soweit wie möglich zu schaffen. Kryptographie ist die einzige Möglichkeit, in offenen Systemen die Offenbarung und Manipulation von Informationen zu kontrollieren, und somit die Voraussetzung, das beim logischen Systemdesign erstellte Zugriffsmodell technisch abzusichern. Zu dieser kryptogra-

phischen Infrastruktur gehört ein Satz von standardisierten Verschlüsselungsverfahren ebenso wie eine Zertifizierungsorganisation für öffentliche Schlüssel.

3 Die Struktur des Gesundheitssystems

Das Gesundheitsstrukturgesetz (GSG) hat zum Ziel, die Aufwärtsspirale der Kosten für das Gesundheitssystem zu brechen. Wirtschaftlichkeit und Qualitätssicherung der Krankenversorgung sollen verbessert werden; Hauptziel ist aber die Kostendämpfung im Gesundheitswesen.

3.1 Inhalte des GSG

Um seine Ziele zu erreichen, führt das GSG die leistungsorientierte Vergütung nach Leistungskatalogen, Fallpauschalen und Sonderentgelten anstelle der bisherigen pauschalen Pflegesätze ein. Außerdem verlangt es eine ziemlich genaue Dokumentation der erbrachten diagnostischen und therapeutischen Leistungen und deren Übermittlung an die Kostenträger (Krankenkassen oder Versicherungen). Die Daten müssen in standardisierter, maschinenlesbarer Form und patientenbezogen übermittelt werden. Dazu heißt es im GSG [3, § 302]:

> „Die ... Krankenhäuser sind verpflichtet, den Krankenkassen bei Krankenhausbehandlung folgende Angaben maschinenlesbar zu übermitteln:
> ...
>
> 3. den Tag, die Uhrzeit und den Grund der Aufnahme sowie die Einweisungsdiagnose, die Aufnahmediagnose, bei einer Änderung der Aufnahmediagnose die nachfolgenden Diagnosen, die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung.
> ...
>
> 6. Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen,
>
> 7. den Tag, die Uhrzeit und den Grund der Entlassung oder der externen Verlegung sowie die Entlassungs- oder Verlegungsdiagnose; ...
>
> 8. Angaben über die im jeweiligen Krankenhaus durchgeführten Rehabilitationsmaßnahmen sowie Vorschläge für die Art der weiteren Behandlung mit Angabe geeigneter Einrichtungen,
> ...“

3.2 Datenschutzprobleme des GSG

Das GSG hat mit den bisherigen Vorstellungen von Datenschutz nicht viel gemeinsam. Insbesondere werden Daten nach außen übermittelt, die nach bisherigem Rechtsverständnis nicht einmal zwischen verschiedenen Abteilungen eines Krankenhauses ausgetauscht werden dürften. Die Unterscheidung zwischen administrativen und medizinischen Daten verblaßt. Patientendaten werden zwischen den Instanzen des Gesundheitssystems ohne Mitbestimmungsrecht des Patienten umhergeschoben. Das informationelle Selbstbestimmungsrecht der Patienten wird verletzt. Der Datenschutz verschwindet im Bermuda-Dreieck zwischen Patient, Arzt und Krankenkasse. Es entstehen riesige Datensammlungen über alle Versicherten. Der gläserne Patient und der gläserne Arzt werden geschaffen.

Sehr zu beanstanden ist auch die fehlende Transportsicherung: Das bevorzugte Medium für die maschinenlesbare Datenübermittlung ist der Postversand einer Diskette in einem Brief. Da die Krankenkassen den Aufwand minimieren wollen, sind Einschreiben dabei ausdrücklich ausgeschlossen. Erst recht lassen die Durchführungsbestimmungen keine kryptographische Verschlüsselung der Daten zu.

Da die optimale Versorgung immer teurer wird, ist für die Kosteneffizienz sicherlich eine größere Transparenz der medizinischen Prozesse nötig. Die Optimierung der Gesundheitsversorgung sollte aber auch möglich sein, ohne solch große Mengen personenbezogener Daten zu offenbaren.

3.3 Lösungsansätze

Folgende Vorschläge zur Verbesserung der für den Datenschutz bedrohlichen Situation wurden in der Arbeitsgruppe bisher gemacht:

- Verschlüsselung der Datenübermittlung,
- Verwendung von Pseudonymen,
- Verlagerung der Qualitätskontrolle auf krankenhausinterne Instanzen.

Der erste Vorschlag wäre relativ leicht zu verwirklichen, da es geeignete Verschlüsselungsprogramme gibt, etwa PGP. Die zu schaffende Infrastruktur bestünde im wesentlichen aus der Installation von PGP bei jedem Arzt und in jedem Krankenhaus, der einmaligen Schlüsselerzeugung und dem Führen eines Verzeichnisses aller öffentlichen Schlüssel bei der Krankenkasse.

Pseudonyme sind kryptographische Protokolle, die Anonymität bei elektronischen Transaktionen sichern [4]. Mustermodelle sind das anonyme elektronische Rezept [10] und das elektronische Geld [2, 6.3]. Diese Modelle vereinfachen sich sogar, wenn man sie sinngemäß auf die Abrechnung der ärztlichen Behandlung überträgt. Der Patient wählt ein Pseudonym und läßt es sich in „camouflierter“ Form von der Krankenkasse durch elektronische Unterschrift bestätigen – ganz analog zum Prägen einer elektronischen Münze wie in [2] beschrieben. Jeder, auch die Krankenkasse selbst, kann die Echtheit des Pseudonyms mit dem öffentlichen Schlüssel der Krankenkasse prüfen. Niemand kann das Pseudonym seinem Besitzer zuordnen, nur dieser selbst; natürlich muß es in einem kryptographisch geschützten Bereich der Patientenkarte abgelegt sein. Kein Patient kann ein gefälschtes Pseudonym erzeugen. Es dient also einerseits als echter Krankenversicherten-Ausweis und ermöglicht andererseits den Krankenkassen die von ihnen erwünschte personenbezogene Auswertung in *anonymer* Form. Die Pseudonymisierung des Arztes wäre zwar analog machbar, würde aber auch die Führung von pseudonymen Bankkonten zur Überweisung der Honorare nötig machen.

Die nötige Infrastruktur für die Einführung von Pseudonymen besteht aus asymmetrischer Verschlüsselungssoftware, z. B. PGP, die in allen Arztpraxen und bei den Krankenkassen zu installieren wäre. Erzeugt werden können die Pseudonyme auf dem Arztcomputer oder auf dem Computer des Patienten. Als zusätzlicher organisatorischer Aufwand kommt das Übermitteln des (camouflierten) Pseudonyms an die Krankenkasse hinzu, die es in unterschriebener Form zurückreicht. Datenträger dafür könnte die Smart Card des Patienten sein.

4 Zusammenfassung und Ausblick

Die Notwendigkeit, aber auch die Möglichkeit, realisierbare Sicherheitskonzepte zu entwikkeln, ist gegeben. Die Zeit ist reif, daraus funktionsfähige Systeme zusammenzubauen, anstatt weiterhin auf unwirksame oder schwache vermeintliche Sicherheitsmaßnahmen zu vertrauen. Datenschutz und Datensicherheit müssen bereits beim Design von medizinischen Informationssystemen berücksichtigt werden. Sie müssen durch eine geeignete sicherheitstechnische Infrastruktur garantiert werden. Nur so kann die rechtliche Zulässigkeit und die gesellschaftliche Akzeptanz des Betriebs solcher Systeme erreicht werden. Auch für die Kommunikation zwischen den Institutionen des Gesundheitswesens gibt es praktisch fertig entwickelte Techniken, die den Datenschutz in sinnvoller Weise gewähren könnten, wenn sie nur eingesetzt würden.

Literatur

[1] Arbeitsgruppe Datenschutz in Krankenhausinformationssystemen. Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen. Positionspapier, GMDS, 1994.

[2] Albrecht Beutelspacher. *Kryptologie*. Vieweg, Braunschweig, Wiesbaden, 1993.

[3] Bundesgesetzblatt, Jahrgang 1992, Teil I.

[4] David Chaum. Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM 28 (1985), 1030–1044.

[5] The Commission of the European Communities DG XIII/F AIM. *Data Protection and Confidentiality in Health Informatics.* AIM Working Conference, Brussels, 19–21 March 1990. IOS Press, Amsterdam, Washington DC, Tokio, 1991.

[6] Datenschutzkommission Rheinland-Pfalz. *Datenschutz im Krankenhaus.* Mainz, 1989.

[7] Michael Hortmann. Interim technical recommendations for data protection in CC computer systems: Guidelines for the use of security functions. Deliverable 3, AIM project TANIT, Workpackage PROTEC, 1992.

[8] Klaus Pommerening. *Datenschutz und Datensicherheit*. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991.

[9] Hans-Jürgen Seelos. *Informationssysteme und Datenschutz im Krankenhaus*. DuD-Fachbeiträge Band 14, Vieweg, Braunschweig, Wiesbaden, 1991.

[10] Bruno Struif: Datenschutz bei elektronischen Rezepten und elektronischem Notfallausweis. Forum Vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung, Bonn, 15./16. September 1994.

[11] Zentralstelle für Sicherheit in der Informationstechnik. *IT-Sicherheitskriterien Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT*). Bundesanzeiger, Köln, 1990.