Datenschutz in Krankenhausinformationssystemen

Klaus Pommerening

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

Zusammenfassung

Medizinische Daten gehören zu den besonders sensitiven Daten einer Person. Sie unterliegen der ärztlichen Schweigepflicht und dem Recht auf informationelle Selbstbestimmung. Durch die Einführung von Informations- und Kommunikationstechnologie soll die Qualität und Effizienz der Gesundheitsversorgung, besonders im Krankenhaus, verbessert werden. Dadurch entstehen aber auch neue Risiken für die Vertraulichkeit der medizinischen Daten. Bestehende Krankenhausinformations-, Abteilungs- und Arbeitsplatzsysteme lassen diese Risiken weitgehend außer Acht. Die existierenden technischen Konzepte für die Verläßlichkeit und Vertrauenswürdigkeit medizinischer Informationssysteme müssen daher so bald wie möglich in die Praxis umgesetzt werden. Die Informatiker sind aufgerufen, sie mit wissenschaftlichen Methoden weiterzuentwikkeln und bei der Modellierung von Krankenhausinformationssystemen endlich zu berücksichtigen.

1 Datenschutz in der Medizin

Von den drei klassischen Grundforderungen an verläßliche informationstechnische Systeme,

- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,

steht die dritte, die Forderung nach der Vertraulichkeit, im Mittelpunkt dieses Vortrags. Selbstverständlich hat der Patient ein mindestens ebenso großes Interesse an der Verfügbarkeit und der Integrität seiner Daten und daran, daß er durch die Automatisierung von diagnostischen und therapeutischen Prozeduren keinen Schaden erleidet. Die Medizin ist daher einer der Bereiche, in denen die Forderung nach verläßlichen und vertrauenswürdigen Informationssystemen am dringendsten ist.

1.1 Die Vertraulichkeit medizinischer Daten

Die Vertraulichkeit medizinischer Daten beruht auf der ärztlichen Schweigepflicht, die im Eid des Hippokrates definiert wird, und auf dem Grundrecht auf informationelle Selbstbestimmung. Das Vertrauen des Patienten in den Arzt ist eine wichtige Grundlage des Gesundheitssystems; ob es angesichts der allgemeinen Undurchschaubarkeit des modernen Medizinbetriebs, aber auch aufgrund menschlicher Unzulänglichkeiten, überhaupt in nennenswertem Maße existiert, ist vielleicht nicht ganz sicher. Jedenfalls darf es durch undurchschaubare Anwendung informationstechnischer Methoden und unkontrollierbare Datenströme nicht noch weiter geschädigt werden. Der Mensch, hier in seiner Eigenschaft als Patient, muß sich darauf verlassen können, daß die Daten zu seiner Person und die Informationen, die er über sich preisgibt, nicht ohne seinen Willen und ohne sein Wissen weiterverwendet werden. Das bedeutet der Ausdruck „informationelles Selbstbestimmungsrecht“, den das Bundesverfassungsgericht geprägt hat. Selbstverständlich sind auch die persönlichen Daten anderer Beteiligter am Gesundheitsprozeß, z. B. Personaldaten im Krankenhaus, wirksam zu schützen.

1.2 Hauptprobleme

Die drei Hauptprobleme für den Datenschutz in der Medizin, speziell in Krankenhausinformationssystemen, sind

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

Die mangelhafte rechtliche Situation ist gekennzeichnet durch eine selbst für Juristen kaum noch überschaubare Fülle einschlägiger Gesetze mit unterschied-

lichem Anwendungsbereich und teilweise widersprüchlichen Regelungen; dabei ist die Subsidiarität der Datenschutzgesetze besonders problematisch: Treten Konflikte zwischen verschiedenen Gesetzen auf, wie sie z. B. beim GSG in Abschnitt 3 beschrieben werden, so tritt der Datenschutz zurück – und dies, obwohl er als Grundrecht definiert ist.

Die organisatorischen Unzulänglichkeiten zeigen sich in fehlenden Regelungen für Verantwortlichkeiten und in der mangelnden Motivation der Beteiligten, wirksame Datenschutzmaßnahmen einzuführen.

Die Informatisierung von Arztpraxen und Krankenhäusern macht rapide Fortschritte. 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. Existierende Sicherheitstechnik, wie kryptographische Protokolle oder PC-Sicherheitssysteme, bleibt dabei weitgehend unbeachtet. Informationstechnische Systeme, speziell in der Medizin, sollten aber so konzipiert und konstruiert werden, daß sie das Recht auf Vertraulichkeit auf allen Ebenen wirksam schützen.

1.3 Initiativen

Neben verschiedenen internationalen und europäischen Initiativen zur Verbesserung von Datenschutz und Datensicherheit in der Medizin 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 Aufgaben dieser Arbeitsgruppe sind:

A) Erstellung eines Datenschutzkonzepts für Krankenhausinformationssysteme.
   - Formulierung der Datenschutzanforderungen.
   - Definition einer modellhaften Zugriffsmatrix.
   - Sicherheitskriterien: Definition von zu beachtenden Gefährdungen und nötigen Sicherheitsstufen aus den Anforderungen des Datenschutzes.
   - Empfehlungen zur technischen Absicherung des Datenschutzes in Krankenhäusern.
   - Definition, eventuell Bereitstellung der kryptographischen Infrastruktur.

B) Umsetzung des Datenschutzkonzepts.

- Durchführung von Modellprojekten, Referenzinstallationen.
- Fachliche Beratung zu Datenschutz-Technologien und organisatorischen Fragen.

Bisher wurde, als Grundlage für ein Muster-Datenschutzkonzept, ein Positionspapier „Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen“ erarbeitet [1]. Ferner wurde für die gruppeninterne Kommunikation das Paket PGP eingeführt, um Erfahrungen mit kryptographischer Technik zu sammeln. Wesentlich für die Arbeitsgruppe ist auch die Mitarbeit in den entsprechenden Working Groups der internationalen Medizin-Informatik-Vereinigungen IMIA und EFMI.

2 Datenschutz im Krankenhaus

Die 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, gelegentlich 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. Dies ist eine schwierige Aufgabe, zumal in verteilten Datenbanksystemen nicht offensichtlich klar ist, wo die Daten überhaupt physisch lokalisiert sind und welcher Systemverwalter verantwortlich für sie ist. 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“. Weitere Vorschläge für Sicherheitsmaßnahmen folgen in Abschnitt 4.3.

2.3 Die elektronische Krankenakte

Die erste und wichtigste Anwendung eines Computersystems in Klinik oder Arztpraxis ist die Verwaltung der Patientendaten. Die elektronische Krankenakte dient mehreren Zwecken:

- Abrechnung mit den Kostenträgern,
- gesetzlich vorgeschriebene Dokumentation von Diagnose und Therapie,
- Qualitätskontrolle,
- wissenschaftliche Auswertung.

Die Daten müssen im Normalfall zehn, teilweise bis zu 30 Jahren aufbewahrt werden (Archivierungspflicht). Technische Maßnahmen müssen die Integrität der Daten gewährleisten und dafür sorgen, daß sie, auch über lange Zeiträume, nur berechtigten Personen zugänglich sind, wobei das „need to know"-Prinzip streng anzuwenden ist. Im Papierzeitalter bot das Chaos und die Unübersichtlichkeit der Patientenakten noch einen gewissen Schutz; im Zeitalter der elektronischen Medien können wir uns keine Nachlässigkeit beim Umgang mit Patientendaten mehr erlauben.

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.

3 Die Struktur des Gesundheitssystems

Das neue 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.

Die Krankenhausinformationssysteme müssen unterschiedliche rechtliche Grundlagen für verschiedenen Typen von Patienten berücksichtigen (z. B. privat versicherte). Streng genommen ist daher eine einheitliche Patientendatenbank rechtlich nicht zulässig.

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. „The need for information must not lead to the protection of the human personality being neglected." [5, 3.1.1]

3.3 Lösungsansätze

Die Datenschutzbeauftragten haben keine Handhabe gegen das GSG, weil es ein vom Parlament beschlossenes Gesetz ist. Wirksam wäre vielleicht eine Verfassungsbeschwerde, die aber nur von einem betroffenen Patienten eingelegt werden kann.

Davon abgesehen gibt es folgende Vorschläge zur Verbesserung der für den Datenschutz bedrohlichen Situation:

- 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]. Musterbeispiele sind:

- die Kontrollnummern, die bei den Pilotprojekten zur Krebsregistrierung in Rheinland-Pfalz und Niedersachsen verwendet werden und die auch Eingang in das Bundeskrebsregistergesetz gefunden haben,
- das anonyme elektronische Rezept [10],
- elektronisches Geld [2, 6.3].

Kontrollnummern nach dem Krebsregistermodell sind für die Abrechnung mit den Krankenkassen nicht so gut geeignet: Sie setzen entweder einen identischen kryptographischen Schlüssel bei allen Krankenhäusern und Ärzten voraus, oder bieten andernfalls den Krankenkassen die Möglichkeit zum Datenabgleich durch Probeverschlüsselung. Voll geeignet sind aber die Modelle „elektronisches Rezept“ und „elektronisches Geld“, wenn man sie sinngemäß anwendet.

Das elektronische Rezept setzt die Ablösung der gegenwärtigen Krankenversicherten-Karten durch echte Smart Cards voraus. Es wird vom Arzt elektronisch signiert, in die Smart Card des Patienten eingetragen, in der Apotheke geprüft und bearbeitet, an die Krankenkasse übermittelt und vollelektronisch abgerechnet. Es wird dadurch pseudonymisiert, daß im Rezeptkopf statt Name, Adresse und Mitgliedsnummer ein Pseudonym des Patienten steht; auch der Arzt kann durch ein Pseudonym repräsentiert werden. Kostenabrechnungen und Auswertungen bleiben möglich, z. B.:

- ob das Rezept für ein Mitglied der betreffenden Krankenkasse erstellt wurde,
- ob das Rezept von einem zugelassenen Kassenarzt ausgestellt wurde, einschließlich Facharzt-Richtung,
- welche Rezepte in einem Zeitraum für eine Person ausgestellt wurden,
- wie oft ein Arzt welche Medikamente verordnet,
- statistische Auswertungen über gewisse nichtidentifizierende Merkmale wie Geschlecht und Geburtsjahr.

Auswertungen können dann natürlich nur statistisch oder, falls einzelfallbezogen, anonym erfolgen. In begründeten Fällen (die gesetzlich geregelt sein müßten) ist im Struifschen Modell eine Aufhebung der Pseudonyme mit Hilfe einer (oder dem Zusammenwirken zweier) spezieller Re-Identifizierungskarten möglich.

Die Übertragung dieses Modells auf die Abrechnung der ärztlichen Behandlung sieht sogar noch einfacher aus. 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, außer dieser selbst; natürlich muß es in einem kryptographisch geschützten Bereich der Karte abgelegt sein. Kein Patient kann ein gefälschtes Pseudonym erzeugen. Es dient also als echter Krankenversicherten-Ausweis.

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 in der Verfügbarkeit asymmetrischer Verschlüsselungssoftware, z. B. PGP, in allen Arztpraxen und bei den Krankenkassen. 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 Sicherheit - wie verwirklichen?

Kehren wir zu den Krankenhausinformationssystemen zurück. Natürlich ist keine vollständige Sicherheit erreichbar. Es läßt sich aber prinzipiell mit dem Stand der Technik ein angemessenes Sicherheitsniveau erreichen. Dabei gibt es mehrere Stufen, auf denen man ansetzen kann:

- die allgemeine Systemsicherheit,
- Sicherheitsanforderungen im medizinischen Bereich allgemein,
- spezielle Gesichtspunkte für Krankenhausinformationssysteme.

Zu beachten sind aber auch psychologische Aspekte bei Benutzern, Entwicklern und Vertreibern von Krankenhausinformationssystemen.

4.1 Die Motivation der Benutzer

Die Verwirklichung des Datenschutzes im medizinischen Bereich ist in einem beklagenswerten Zustand („alarming“ in [5, p. 1]). Ein möglicher Grund ist, daß die Mediziner die Notwendigkeit von Maßnahmen nicht einsehen – es gibt nur wenige bekannt gewordene spektakuläre Fälle von Datenschutzverletzungen im medizinischen 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 fachkundigen 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 „Pro-

fessional 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.

4.2 Die Motivation von Entwicklern und Vertreibern

Hersteller und Entwickler von Krankenhausinformationssystemen und Teilsystemen sehen Datenschutz und -sicherheit 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. In dieser Beziehung haben auch die US-Exportbeschränkungen für kryptographische Produkte eine Menge Unheil angerichtet. Benötigt werden klare Sicherheitsstandards für alle medizinischen Anwendungsbereiche, auf die sich Entwickler stützen können.

4.3 Ansatz zu einem Datenschutzkonzept

Ein allgemeingültiges Datenschutzmodell kann wohl nicht entwickelt werden, denn wegen großer Unterschiede in den Krankenhäusern gibt es nicht einmal

ein allgemeines Modell für Krankenhausinformationssysteme. 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.

Bei den Bedrohungen kann man unterscheiden zwischen naheliegenden Bedrohungen, wie:

- zufällige Besucher an unbeaufsichtigten Geräten,
- nichtmedizinisches Personal (z. B. Putzdienst),
- Wartungsdienst,
- Reparaturdienst (Fall „Vobis-Festplatten“).

und „exotischen“ Bedrohungen, wie:

- Presse,
- Kriminelle,
- Hacker.

Diese sind zwar auch real und müssen bedacht werden; sie werden aber von den Systembetreibern oft heruntergespielt. In jedem konkreten Fall ist eine Schwachstellenanalyse nötig; die Differenzierung der Bedrohungen ist allerdings nicht so wichtig, da die Datenschutzvorschriften sowieso bestmögliche Sicherung nach dem Stand der Technik verlangen. Zu beachten ist, daß 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“).
- Das zu erstellende Modell erfordert also autonome Abteilungsserver, die ihre Zugriffsrechte selbst verwalten.

Die naheliegende Realisierung dieses Modells besteht also aus einem System von Abteilungsservern 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),
- ...

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!
Mögliche Schutzstufen für Daten im Krankenhaus sind (nach dem Katalog der technischen und organisatorischen Maßnahmen zum Datenschutz des staatlichen Koordinierungsausschusses Datenverarbeitung Bayern):

A) Frei zugängliche Daten (z. B. Bibliothekskatalog, Vorlesungsverzeichnis).

B) Daten, deren Mißbrauch keine besondere Beeinträchtigung erwarten läßt (z.B. Adressenverzeichnisse, Verteiler).

C) Daten, deren Mißbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen beeinträchtigen kann („Ansehen“) (z. B. Patientenstammdaten, allgemeine Personaldaten).

D) Daten, deren Mißbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann („Existenz“) (z. B. medizinische Patientendaten, Unterbringung in Anstalten, dienstliche Beurteilungen).

E) Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (z. B. besonders empfindliche Patientendaten, man denke etwa an psychiatrische Behandlungen).

Diese Schutzstufen verdeutlichen die Sensitivität der Daten und helfen bei der Gruppierung von Daten. Für die Anwendung scheinen sie mir von geringerer Bedeutung zu sein, denn grundsätzlich gilt:

1. Im Zweifelsfall ist die höhere Schutzstufe zu unterstellen.
2. Sind Maßnahmen für die höhere Schutzstufe nicht „teurer“, sind sie auch für die niedrigere Schutzstufe anzuwenden.

Daher brauchen sie im Modell eventuell nur sehr eingeschränkt berücksichtigt zu werden, insbesondere, wenn das „need-to-know“-Prinzip konsequent angewendet wird.

Mögliche allgemeingültige Empfehlungen für Sicherheitsmaßnahmen sind

- Verschlüsselte Datenspeicherung,
- 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 (mit PIN-Schutz), auch als „Professional Card“ bezeichnet,
- Firewall- und andere Netzsicherheitstechniken,
- Einsatz von PC-Sicherheitssystemen,
- organisatorisch: Verpflichtung, Schulungen, ...

4.4 Ein Ansatz zur Modellierung

Ein Krankenhausinformationssystem ist kein geschlossenes System. Durch Modularisierung der Kommunikationsströme kann man es aber als ein System mit kontrollierten Ein- und Ausgängen modellieren. Weitere Systeme auf dieser Hierarchiestufe sind der Patient, die niedergelassenen Ärzte und die Krankenkassen und Versicherungsunternehmen, siehe Abbildung 1. (Auch epidemiologische Register, soweit sie existieren, sind auf dieser Stufe anzusiedeln.)

Innerhalb dieser Systeme der oberen Stufe sind jeweils die internen Datenströme und -speicher zu modellieren. Im Krankenhausinformationssystem sind die beteiligten Entitäten: Fachabteilungen, Kliniksverwaltung, Leistungsstellen (wie Labore), siehe Abbildung 2. Diese sind weiter hierarchisch untergliedert nach Funktionen, wie Arzt, Pflegepersonal, technische Angestellte.

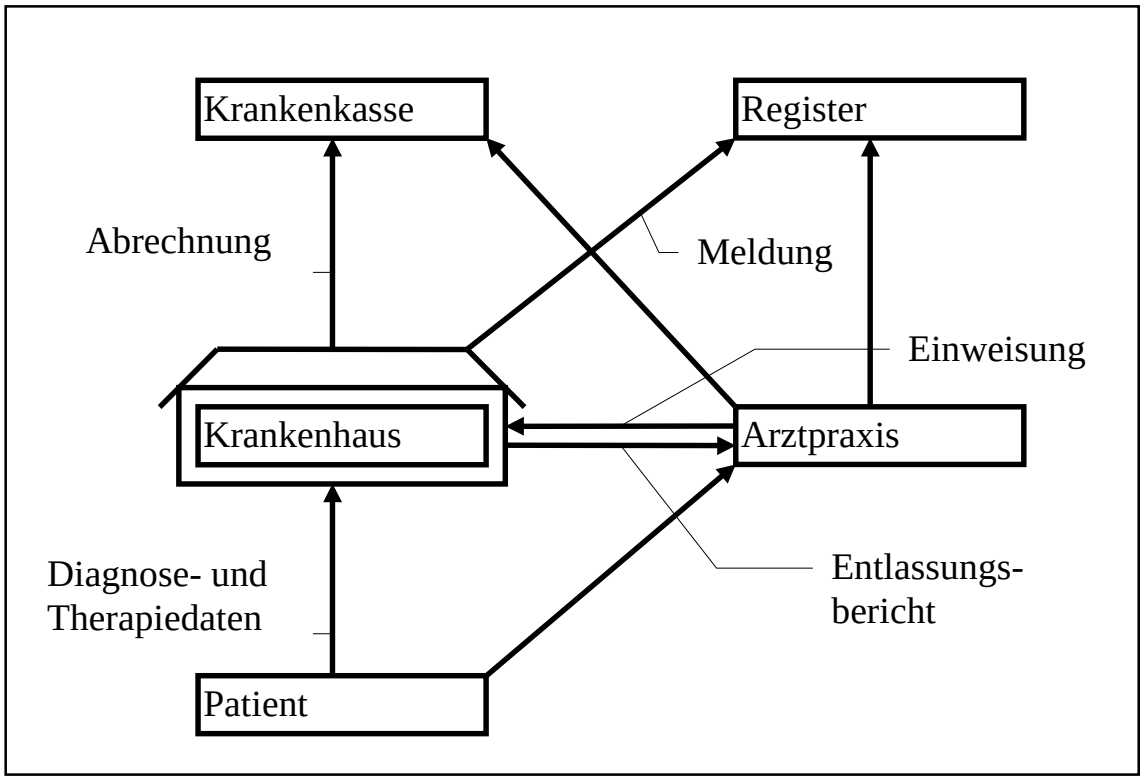

Abb. 1 Datenströme vom und zum Krankenhaus

Die Erfahrung bei der Entwicklung von Informationssystemen läßt erwarten, daß auch bei der Modellierung eines Krankenhausinformationssystems ein sauberes Datenmodell zu einem sauberen Sicherheitskonzept führt. Dieses mündet in eine, durch Gruppierung von Objekten und Subjekten übersichtlich gestaltete, Zugriffsmatrix; ein prototypisches Beispiel dafür ist in [9] angegeben. Verläßlichkeit bedeutet hier, daß die Annahmen, die dem Modell zugrunde liegen, von der Implementation garantiert werden, z. B. Annahmen darüber, wer Zugang zu welchen Informationen hat. Hier dürfen natürlich auch die Möglichkeiten zum Datenzugriff unter Umgehung des Anwendungssystems nicht vergessen werden, z. B. mit Hilfe von direktem Plattenzugriff.

4.5 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.

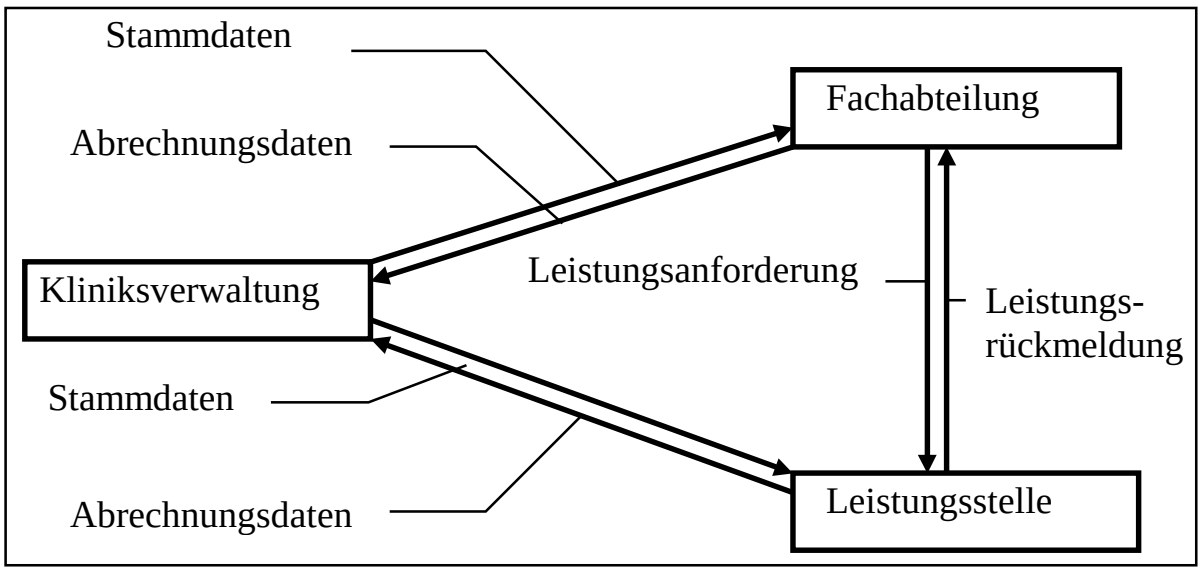

Abb. 2 Datenströme im Krankenhaus

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

Datenschutzinhalte und -ziele sowie Sicherheitsanforderungen sind so zu spezifizieren, daß Hersteller genügend genaue Richtlinien in die Hand bekommen. 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).

5 Zusammenfassung und Ausblick

Die Notwendigkeit, aber auch die Möglichkeit, realisierbare Sicherheitskonzepte zu entwickeln, 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 Krankenhausinformationssystemen berücksichtigt werden. Sie müssen durch eine geeignete sicherheitstechnische Infrastruktur garantiert werden. Nur so kann die rechtliche Zulässigkeit und die gesellschaftliche Akzeptanz des Betriebs von Krankenhausinformationssystemen erreicht werden.

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.