Dr. Ross J. Anderson & British Medical Association

SICHERHEIT IN KLINISCHEN INFORMATIONSSYSTEMEN

In Auftrag gegeben vom Komitee für Informationstechnologie der
British Medical Association für den Rat der British Medical Association

London, Januar 1996

Autorisierte deutsche Übersetzung von
Dr. med. Andreas von Heydwolff

Inhaltsverzeichnis

Über dieses Dokument

Abkürzungen

Vorwort von Dr. Macara (Vors. der BMA)

1 Einführung
- 1.1 Geltungsbereich der Sicherheitspolitik
- 1.2 Definitionen
- 1.3 Worauf verzichtet wird [Disclaimers]

2 Bedrohungen und Verletzlichkeiten
- 2.1 Die ethische Basis von klinischer Vertraulichkeit
- 2.2 Andere Sicherheitserfordernisse für klinische Informationen
- 2.3 Bedrohungen der klinischen Vertraulichkeit
- 2.4 Andere Bedrohungen der Sicherheit von klinischen Informationen
- 2.5 Schutzprioritäten
- 2.6 Beispiele für Aggregationen in NHS-Systemen

3 Die Sicherheitspolitik
Eine Bemerkung zu Struktur von Patientenakten
- 3.1 Zugangskontrolle
- 3.2 Einrichten einer Akte
- 3.3 Kontrolle
- 3.4 Einwilligung und Mitteilung
- 3.5 Fortbestand
- 3.6 Zuschreibung
- 3.7 Informationsfluß
- 3.8 Aggregationskontrolle
- 3.9 Die Trusted Computing Base (Vertrauenswürdige Einrichtung zur Datenverarbeitung)
- 3.10 Klinische Akten oder Patientenakten?

4 Optionen für eine Sicherheitsarchitektur
- 4.1 Compusec
- 4.2 Comsec
- 4.3 Evaluation und Akkreditierung
- 4.4 Europäische und globale Standardisierung

5 Schlußfolgerungen

Danksagungen

6 Literatur

Über dieses Dokument

Veröffentlicht im Internet am 4. Februar 1998.

Zitierweise: Anderson RJ, British Medical Association (1998) Sicherheit in klinischen Informationssystemen. Deutsche Übers. von: Dies. (1996) Security in Clinical Information Systems. London, British Medical Association. Elektronisch publiziert unter Internet-Adresse
"http://ourworld.compuserve.com/homepages/gesundheitsdatenschutz/bma-s-d.htm"

Anmerkungen zum besseren Verständnis im deutschen Sprachraum
sind von Dr. Anderson ("rja") und vom Übersetzer ("avh").

Technische Ausdrücke wurden manchmal ausführlicher erläutert beziehungsweise übersetzt, da das Dokument insbesondere im Gesundheitswesen beschäftigte Personen und sonstiges interessiertes Publikum erreichen will. Damit wird bewußt von Gepflogenheiten in der deutschsprachigen Fachliteratur zur Computersicherheit abgewichen; diese verwendet viele englische Ausdrücke unübersetzt.

Englisches Original

Zitierweise: Anderson RJ, British Medical Association (1996) Security in Clinical Information Systems. London: British Medical Association, Januar 1996. ISBN 0 7279 1048 5

Gedruckt zu beziehen von Lina Coelho, BMA Library, BMA House, Tavistock Square, London WC1H 9JP, England; e-mail: "lina.coelho@bma.org.uk", Tel. +44 171 383 6452.

URLs der elektronischen Form

"http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html" (HTML-Version) auf der Site
"http://www.cl.cam.ac.uk/users/rja14/#Med" (dort auch in den Formaten Postscript und ASCII)

Anschriften

Dr. Ross Anderson: Computer Laboratory, University of Cambridge,
Pembroke Street, Cambridge CB2 3QG, England; e-mail: "Ross.Anderson@cl.cam.ac.uk"

British Medical Association: BMA House, Tavistock Square, London WC1H 9JP, England
e-mail: "bma-library@bma.org.uk"; Tel. +44 171 387 4499, Fax +44 171 383 6400

Übersetzer: Dr. Andreas von Heydwolff
Dreifaltigkeitsgasse 3, A-5020 Salzburg; e-mail: "106624.446@compuserve.com"

Abkürzungen

BMA: British Medical Association (Britische Ärztevereinigung)

GMC: General Medical Council

NHS: der National Health Service in Großbritannien. Im Kürzel
NHSE steht "E" für "Executive", die Zentralverwaltung von mehreren tausend Personen, von der ein großer Teil die IMG ist

IMG: Information Management Group [versucht unter anderem, alle Computersysteme im NHS unter ihrer Kontrolle zu behalten - rja]

VORWORT

Neue Technologien können dramatische Vorteile für die Patientenversorgung bringen. In jedem Einzelfall hat die Ärzteschaft die Pflicht, sowohl die Risiken als auch die Vorteile der betreffenden Technologie zu untersuchen, wozu sie sich der Forschungsergebnisse und der dokumentierten Zeugnisse klinischer Erfahrungen bedient. Die unbezweifelbaren Vorteile, welche die Informationstechnologie bieten kann, dürfen die Ärzte nicht blind für ihre Pflicht machen, dieselben rigorosen ethischen Standards auch auf deren Gebrauch anzuwenden.

Ausgedehnte Diskussionen über den Plan der NHSE [Erklärung s. Einschub nach diesem Absatz], ein NHS-weites Netzwerk einzuführen (das potentiell alle NHS-Computer in der Primär- und Sekundärversorgung, in Einkaufs- und Versorgungsorganisationen, sowohl innerhalb wie außerhalb des NHS, verbindet) haben die Risiken der Vernetzung für die Vertraulichkeit von identifizierbaren Patienteninformationen zur Gänze enthüllt.

[NHS: der National Health Service in Großbritannien. Im Kürzel NHSE steht "E" für "Executive", die Zentralverwaltung von mehreren tausend Personen, von der ein großer Teil die "Information Management Group" ist, die unter anderem versucht, alle Computersysteme im NHS unter ihrer Kontrolle zu behalten - rja]

Eine effektive Sicherheitspolitik ist eine essentielle Grundvoraussetzung.

Die sorgfältige Untersuchung des NHS-weiten Netzwerks - sein Potential für Nutzen und Schäden - hat die Unzulänglichkeit des NHS-Ansatzes gezeigt. Als Dienst sowohl am Berufsstand als auch an der Öffentlichkeit hat die Ärztevereinigung einen international anerkannten Experten für Datensicherheit beauftragt, Vorschläge für die Sicherheit in klinischen Informationssystemen zu entwickeln.

Dieser Bericht, den der NHS-Vorstand bereits erhalten hat, wird hier zur Beratung mit den breiteren ärztlichen Gemeinschaften und den Gemeinschaften der anderen Gesundheitsberufe, der Informatiker und Sicherheitsfachleute präsentiert. Würden die in ihm enthaltenen Prinzipien angenommen, so stünde damit eine sichere und für Ärzte und Patienten ethisch akzeptable Basis für den Gebrauch von Informationstechnologien im NHS zur Verfügung.

DR. A. W. MACARA

Vorsitzender der British Medical Association

11. Januar 1996

1 Einführung

Das Vorhaben, ein landesweites NHS-Netzwerk einzuführen, hat zu Besorgnis wegen dessen Sicherheit geführt. Ärzte und Angehörige anderer klinischer Berufsgruppen befürchten, daß die Vertraulichkeit für Patienten gefährdet werden könnte, wenn persönliche Gesundheitsinformationen in weiterem Umfang verfügbar gemacht werden [ACH95]. Das Problem ist nicht auf den NHS beschränkt; es geht auch Kliniker in Gefängnissen, Einwanderungsbehörden, gerichtsmedizinischen Laboratorien und im privaten Sektor des Gesundheitswesen an. Jedenfalls hat das NHS-Netzwerk die Thematik öffentlich bewußt gemacht.

Allgemein ist man sich einig darüber, daß die Sicherheit elektronischer Patientenakten dem bei papiernen Akten angewendeten Standard entsprechen oder ihn übertreffen muß. Das Fehlen von Klarheit über die richtigen Ziele für den Schutz hat jedoch zu Verwirrung geführt. Die British Medical Association hat daher den Autor gebeten, die Risiken einzuschätzen und eine Sicherheitspolitik für klinischen Informationssysteme aufzustellen.

1.1 Geltungsbereich der Sicherheitspolitik

Eine Sicherheitspolitik für Informationen besagt, wer Zugang zu welchen Informationen haben darf; Zugang umfaßt Aktivitäten wie das Lesen, Schreiben, Anfügen und Löschen von Daten. Sie geht aus einem Bedrohungsmodell hervor und formt wiederum die detaillierteren Aspekte des Systemdesigns. Um effektiv zu sein, muß sie auf dem richtigen Abstraktionsniveau verfaßt werden; sie darf den Leser nicht mit unnötigen Einzelheiten spezifischer Geräte belasten. Sie muß die wichtigen Problemen angehen und Ablenkungen vermeiden.

Eine mögliche Ablenkung ist die genaue Bedeutung von Begriffen wie "Kliniker", "Patient" und "System". Man kann sich lange dabei aufhalten, was passieren kann, wenn ein Klinker eine Aufgabe an einen Studenten delegiert, oder wenn ein Patient minderjährig oder verstorben ist. Diese Fragen können schwierig sein, für unsere Zwecke sie sind aber unwichtig; daher werden wir sie lieber schon hier anstatt im Hauptteil der Sicherheitspolitik erklären.

1.2 Definitionen

Mit "**persönlichen Gesundheitsinformationen**" oder gleichbedeutend "**identifizierbaren klinischen Informationen**" meinen wir Informationen, die den Gesundheitszustand, die medizinische Krankengeschichte oder medizinische Behandlungen (ob vergangen oder zukünftig) eines Menschen in einer Form betreffen, die es ermöglicht, daß der Mensch von jemand anderem als dem behandelnden Kliniker identifiziert werden kann [RAC+93].

Mit "**Kliniker**", oder gleichbedeutend "**klinischer Berufsausübender**" [clinical professional] oder "**in einem Gesundheitsberuf Tätiger**" [healthcare professional] meinen wir eine zur Berufsausübung zugelassene Person wie einen Arzt, eine Krankenpflegeperson, einen Zahnarzt, einen

Physiotherapeuten oder einen Apotheker, der im Rahmen seiner Berufspflichten Zugang zu persönlichen Gesundheitsinformationen hat und dem eine berufliche Verpflichtung zur Verschwiegenheit auferlegt ist. Wir schließen Ärzte im öffentlichen Gesundheitsbereich mit ein, auch wenn sie technisch gesehen vielleicht nicht klinisch tätig sind.

Der Leser kann den Access to Health Record Act von 1990 für eine gesetzliche Definition von "Healthcare Professional" zu Rate ziehen, sollte sich dabei aber darüber im klaren sein, daß dieses Gesetz kontrovers ist: es gibt eine Debatte darüber, ob Psychotherapeuten, Personal von telefonischen Beratungsdiensten, Ausübende im Bereich der Komplementärmedizin und Sozialarbeiter in die Vertrauensgrenze hineingenommen werden sollen. Wie auch immer, die Grenze muß irgendwo sein, und wo sie genau liegt, hat kaum eine Auswirkung auf unsere Politik. Sozialarbeiter, Studenten, Mitarbeiter von Wohlfahrtseinrichtungen und Empfangspersonal dürfen natürlich Zugang zu persönlichen Gesundheitsinformationen unter der Aufsicht eines Angehörigen eines Gesundheitsberufes haben; aber dieser bleibt für deren Verhalten verantwortlich. Der Einfachheit halber schließen wir solche Delegationen nicht in unsere Sicherheitspolitik ein; aber auf der Ebene des detaillierten Designs ist es ratsam, daß die Systembauer Delegationen auf intelligente Weise unterstützen.

Unser Gebrauch des Wortes "**Patient**" wird ein Kürzel für "das betroffene Individuum oder den Vertreter des Individuums" sein, im Sinne des Gesetzentwurfs, den die British Medical Association im Frühjahr 1996 durch einen Abgeordneten ins Parlament einbringen konnte [BMA95; der Entwurf wurde von der konservativen Regierung blockiert, die neue Labour Regierung, im Amt seit Mai 1997, will ein eigenes Datenschutzgesetz ins Parlament einbringen - rja]. In den meisten Fällen ist das der tatsächliche Patient; aber wenn der Patient ein kleines Kind ist, kann es ein Elternteil oder Vormund sein, der an seiner statt handelt. Es gibt Regeln für bewußtlose oder verstorbene und noch komplexere Regeln für geistig behinderte Patienten. Diese Regeln können von früher ausgedrückten Wünschen des Patienten abhängen, und sie unterscheiden sich in verschiedenen Teilen des Vereinigten Königreichs [Som93]. Wir werden diesen Bereich nicht weiter diskutieren.

Um einer knappen Ausdrucksweise willen werden wir annehmen, daß der Kliniker weiblich ist und der Patient männlich. Das Thema der feministischen versus grammatikalischen Sichtweise wird in der Computer-Sicherheitsliteratur traditionell so gelöst, daß definitive Geschlechterrollen zugeordnet werden, wobei Frauen mindestens einen so hohen Status bekommen wie Männer. Unsere Wahl soll nicht heißen, daß die Klinikerin einen höheren Status als der Patient in der therapeutischen Partnerschaft zwischen beiden innehat.

Mit "**System**" meinen wir im allgemeinen die Gesamtheit von Hardware, Software, Kommunikations- und manuellen Vorgängen, die ein zusammenhängendes System zur Informationsverarbeitung ausmachen [mit Kommunikationsvorgängen sind Ordnung, Disziplin, usw. gemeint; "man muß einem Unix-Systemadministrator vertrauen können, da er mit dem System alles machen kann. Also ist er ein Teil des Systems und sogar der 'Trusted Computing Base'" - rja]. Es kümmert uns nicht, ob das System aus einer einzigen großen Grundstruktur [mainframe] mit tausenden von Terminals besteht, aus tausenden von PCs, die durch einen Satz von sogenannten Protokollen und verteilten Anwendungen verbunden sind, oder sogar aus tausenden von Angestellten, die Papierblätter umherbewegen. Es geht uns nur um den Nettoeffekt der Informationsverarbeitung; das ist auch der Sinn der kürzlich erschienenen EU-Direktive zum Datenschutz [EU95].

Aus dem Kontext dürfte klar werden, ob wir über die Gesamtheit der miteinander verbundenen klinischen Systeme sprechen oder von dem Subsystem, das den Erfordernissen eines bestimmten Individuums oder Behandlungsteams dient.

1.3 **Worauf verzichtet wird** [Disclaimers]

Erstens behandelt dieses Dokument nur die klinischen Aspekte von Informationssicherheit und nicht die zugehörigen geschäftlichen Aspekte wie die kommerzielle Vertraulichkeit von Käufer- und Anbieter-Vertragsdaten und die rechtliche Verläßlichkeit von elektronischen Akten vor Gericht.

Zweitens bestreiten wir nicht, daß es Sicherheitsgewinne durch die Computerisierung von medizinischen Aufzeichnungen geben kann: das Verschlüsseln von Akten, die übermittelt werden, kann eine viel stärkere Vertraulichkeit gewährleisten als die Postdienste; Systeme zum Aufspüren von Eindringversuchen können Zugangsvorgänge aufzeichnen und sie auf verdächtige Muster hin analysieren; und Datensicherungen an anderen Orten können effektiven und wirtschaftlichen Schutz vor Feuer und Überschwemmung bieten.

Wir müssen jedoch erst unsere Prioritäten für den Schutz verstehen, bevor diese Techniken effektiv angewendet werden können, und eine Sicherheitspolitik ist ein wichtiger Schritt zum Schaffen und Klären eines solchen Verständnisses.

2 Bedrohungen und Verletzlichkeiten

In diesem Abschnitt diskutieren wir die Bedrohungen der Sicherheit von persönlichen Gesundheitsinformationen, die von der Computerisierung und insbesondere vom Verknüpfen der vielen Praxis- und Krankenhauscomputer herrühren, in denen gegenwärtig klinische Aufzeichnungen gespeichert werden. Zuerst gehen wir die Sicherheitsziele durch, dann überlegen wir, was leicht schiefgehen kann, und schließlich legen wir unsere Sicherheitsprioritäten fest.

2.1 Die ethische Basis von klinischer Vertraulichkeit

Der hippokratische Eid schloß das Prinzip der medizinischen Vertraulichkeit in die ärztliche Berufsethik ein. Eine moderne Formulierung ist im Büchlein "Good Medical Practice" [GMC1] zu finden, das der General Medical Council herausgegeben hat:

> "Patienten haben ein Recht darauf, zu erwarten, daß Sie keine persönlichen Informationen weitergeben, die Ihnen in der Ausübung Ihrer Berufspflichten bekannt werden, außer wenn sie der Weitergabe zustimmen."

Dies wurde im GMC-Büchlein "Confidentiality" [Vertraulichkeit] noch weiter ausgeführt, das festlegt, daß Ärzte, die vertrauliche Informationen aufzeichnen oder verwahren, sicherstellen müssen, daß diese wirksam gegen unzulässige Offenbarung geschützt werden. Noch detailliertere Unterweisungen können in Büchern gefunden werden, die von der British Medical Association [Som93] und vom Königlichen Staatsverlag [HMSO; Her Majesty's Stationary Office][DGMW94] veröffentlicht wurden.

Sowohl die Regierung als auch die Verbände der Gesundheitsberufe sind übereingekommen, daß elektronische Gesundheitsakten mindestens so gut wie papierne geschützt werden müssen; das Datenschutzgesetz macht die niedergelassenen Ärzte und andere für die persönlichen Gesundheitsinformationen, die sie sammeln, verantwortlich; und eine neue EU-Direktive macht der Regierung die Auflage, die Verarbeitung von Gesundheitsdaten zu verbieten, außer wenn derjenige, den die Daten betreffen, seine ausdrückliche Zustimmung gegeben hat, und unter gewissen anderen Bedingungen [EU95].

Das grundlegende ethische Prinzip ist, wie vom General Medical Council und von der EU festgelegt, daß der Patient der Teilhabe an seinen Daten zustimmen muß. Vertraulichkeit ist ein Privileg des Patienten, daher kann nur er auf sie verzichten [DGMW94]; und die Zustimmung dazu muß eine informierte, freiwillige und kompetente sein [Som93]. Folglich müssen Patienten zum Beispiel davon in Kenntnis gesetzt werden, daß ihre Informationen von Mitgliedern eines Behandlungsteams (wie dem in einer Allgemeinpraxis oder einer Krankenhausabteilung) geteilt werden können.

Im Laufe der Zeit hat sich eine Anzahl von Ausnahmen zu dieser Regel entwickelt, und diese schließen gesetzliche Erfordernisse und aus pragmatischen Gründen geforderte Ausnahmen ein; sie haben zu tun mit der Bekanntgabe von Abtreibungen, Geburten, manchen Todesfällen, bestimmten Erkrankungen, unerwünschten Medikamentenwirkungen, Verletzungen, die nicht auf einen Unfall zurückzuführen sind,

der Fahrtauglichkeit und mit Offenlegungen gegenüber Rechtsbeiständen im Verlauf eines Rechtsstreits [DGMW94]. Es gibt eine Kontroverse zur Forschung; die Zentralverwaltung des National Health Service [NHSE, NHS Executive] behauptet, daß ein Patient dadurch, daß er sich in Behandlung begibt, implizit der Verwendung seiner Akten in der Forschung zustimmt, während die Gesundheitsberufe diese Sicht nicht akzeptieren [Mac94]. Diese Debatte hat jedoch keine großen Auswirkungen auf die Sicherheitspolitik, die hier dargestellt wird.

Schließlich gibt es noch die Frage, ob ein Patient der Speicherung seiner Akte in einem Computersystem überhaupt zustimmen muß oder nicht. Es ist unethisch, einen Patienten zu diskriminieren, der verlangt, daß Aufzeichnungen über ihn auf Papier festgehalten werden; seine Befürchtungen können sehr wohl gerechtfertigt sein, wenn er im öffentlichen Leben steht, ein Ziel für Mordversuche ist oder wenn er aus anderen Gründen von fähigen und motivierten Gegnern bedroht wird. Im Umgang mit manchen derartigen Fällen hat man Pseudonyme verwendet, so daß die wahre Identität des Patienten nie einem Computersystem ausgesetzt wurde.

2.2 Andere Sicherheitserfordernisse bei klinischen Informationen

Außer um die Vertraulichkeit von klinischen Informationen sind wir um deren Integrität und Verfügbarkeit besorgt.

Wenn Informationen verfälscht sind, können Klinikerinnen falsche Entscheidungen treffen, die Patienten schaden oder sie sogar umbringen. Wenn Informationen in dem Sinne unverläßlich sind, daß sie möglicherweise verfälscht worden sein könnten (selbst wenn das nicht geschehen ist), dann haben sie als Grundlage für klinische Entscheidungen verminderten Wert. Außerdem gibt es die medizinrechtlichen Bedenken, daß in Gesundheitsberufen Tätige, die ihr Handeln rechtfertigen sollen, sich vielleicht nicht auf Computeraufzeichnungen als Beweismaterial verlassen können; und unlängst hat es eine Kontroverse darüber gegeben, ob es genügt, eine elektronische Akte alleine zu haben, oder ob Papier- oder Mikrofiche-Akten als Sicherungskopien gehalten werden sollen.

Wenn Informationssysteme in dem einfacheren Sinne unverläßlich sind, daß Informationen gelegentlich wegen eines Systemversagens oder wegen Sabotage nicht verfügbar sein können, so verringert dies ebenfalls ihren Wert und schränkt den Gebrauch ein, den man vernünftigerweise von ihnen machen kann.

Es ist daher klug, nach Wegen zu suchen, wie man die Integrität bestimmter Aufzeichnungen garantieren kann, und Angriffen vorzubeugen, welche die Verfügbarkeit des Systems beeinträchtigen können.

2.3 Bedrohungen für die klinische Vertraulichkeit

Viele öffentliche und private Organisationen haben verstreute manuelle Aufzeichnungssysteme durch zentralisierte oder vernetzte Computersysteme ersetzt, die besseren Zugang zu den Daten gewähren. Deren Erfahrung ist, daß die hauptsächliche neue Bedrohung von Insidern kommt. Zum Beispiel geben

die meisten der großen Banken im Vereinigten Königreich mittlerweile jedem Kassierer Zugang zum Konto jedes Kunden; Zeitungen berichten, daß Privatdetektive Kassierer bestechen, um Informationen über Konten zu erhalten, die sie für etwa 100 Pfund weiterverkaufen [LB94]. Diese Praxis wurde mit einer kürzlich erlassenen Novelle des Datenschutzgesetzes unter Strafe gestellt, aber es hat trotzdem noch keine Strafverfolgungen gegeben, von denen wir gehört hätten.

Mit den Auswirkungen des Aggregierens von Daten in großen Datenbanken hätte man rechnen können. Die Wahrscheinlichkeit, daß Informationen unzulässigerweise offenbart werden, hängt von zwei Dingen ab: von ihrem Wert und von der Anzahl von Personen, die Zugang zu ihnen haben. Das Aggregieren von Akten erhöht beide Risikofaktoren zugleich. Es kann außerdem eine wertvolle Ressource schaffen, die selbst wiederum politischen Druck für eine Legalisierung des Zugangs erzeugt, der von Interessenten kommt, die behaupten, daß sie die Informationen benötigen [Smu94].

Es ist unwahrscheinlich, daß es sich mit Systemen im Gesundheitsbereich anders verhält. Gegenwärtig hängt die Sicherheit von der Fragmentation und dem Verstreutsein ab, die zu manuellen Aufzeichnungssystemen gehören. Diese Systeme können bereits von Privatdetektiven verletzt werden, die einfach anrufen und so tun, als ob sie einem anderen Anbieter von Gesundheitsleistungen angehören. Eine kürzlich von einer Zeitung durchgeführte Untersuchung hat gezeigt, daß man die Akten der meisten Leute für lediglich 150 Pfund beziehen kann [RL95]. Es sind auch Vorfälle bekannt, in denen es speziell um Computersysteme ging:

- nachdem ein Praxiscomputer gestohlen worden war, erhielten zwei prominente Damen Erpresserbriefe, in denen gedroht wurde, Abtreibungen zu veröffentlichen;

- es gibt fortgesetzt Mißbräuche von Systemen für Medikamentenverordnungen [JHC94];

- ein Mann aus Merseyside auf sexueller Pirsch, der sich "Dr. Jackson" nennt, gewinnt das Vertrauen von jungen Frauen, indem er am Telefon die medizinische Anamnese von deren Familie diskutiert und dann versucht, Treffen zu vereinbaren. Die Polizei glaubt, daß er im Gesundheitswesen beschäftigt oder ein Computerhacker ist [Tho95].

Die interimistischen Richtlinien, die gleichzeitig mit diesen Grundsätzen herausgegeben wurden [And96], geben Rat, wie man solche Attacken auf manuelle und Computer-Systeme unwahrscheinlicher machen kann. Die Einführung der Vernetzung wird jedoch das Risikoprofil verändern, da gegenwärtig in Großbritannien betriebene Gesundheitsnetzwerke in ihrer Ausdehnung begrenzt sind, ob nun geographisch oder in ihrer Funktion. Sie zu einem nationales Netzwerk mit vollen Funktionen zu verbinden, wird das Potential für Unheil sehr stark vermehren.

Einfach gesagt, wir mögen nicht sehr besorgt darüber sein, daß die Empfangsdame eines Allgemeinarztes Zugang zu den Akten von 2.000 Patienten hat; aber wir wären in der Tat sehr besorgt, wenn 32.000 Empfangsdamen alle Zugang zu den Akten von 56.000.000 Patienten hätten. Die Gefahr des Aggregierens von Akten und die Wahrscheinlichkeit, daß daraus Mißbrauch resultieren wird, wird von den Erfahrungen in den USA bestätigt, wo die Vernetzung etwas weiter fortgeschritten ist als in Großbritannien:

- eine Harris-Umfrage zur Privatheit von Gesundheitsinformationen hat gezeigt, daß 80% von denen, die geantwortet haben, um die Vertraulichkeit von medizinischen Informationen besorgt waren, und ein Viertel hatte persönliche Mißbrauchserfahrungen [GTP93]

- 40 Prozent der Versicherer geben Gesundheitsinformationen an Kreditgeber oder Werbefirmen ohne Zustimmung ihrer Kunden weiter [CR94]; und mehr als die Hälfte von Amerikas 500 größten Firmen gab zu, Gesundheitsaufzeichnungen zu benutzen, um Einstellungs- und andere Personalentscheidungen zu treffen [Bru95];

- ein Banker in einer staatlichen Gesundheitskommission hatte Zugang zu einer Liste aller Patienten in seinem Bundesstaat, bei denen Krebs diagnostiziert worden war. Er glich sie mit seiner Kundenliste ab und forderte die Kredite der Patienten zurück [HRM93];

- eine Pharmafirma in den USA erhielt Zugang zu einer Datenbank mit den Verordnungen von 56 Millionen Leuten, indem sie eine Gesundheits-Systemhaus [health systems company; macht Abrechnungen - avh] kaufte. Jetzt plant sie, in der Datenbank eine Schleppnetzsuche nach Patienten anzustellen, deren Verordnungen die Vermutung nahelegen, daß sie unter einer Depression leiden, die sich in einigen anderen leichteren Beschwerden wie Rückenschmerzen und Schlaflosigkeit ausdrückt. Dann sollen deren Ärzte dazu gebracht werden, Prozac [ein Antidepressivum - avh] zu verschreiben [See95];

- ein Kreditschutzunternehmen baut ein Netzwerk, um mit Gesundheitsdaten zu handeln. Es sponsort einen Gesetzentwurf im US-Kongreß, der die Offenbarung gegenüber beliebigen Interessenten ohne Patientenzustimmung erleichtern und das Recht von Patienten, zu klagen, wenn unautorisierte Offenbarung zu Schaden führt, beseitigen würde. Das ist ein Beispiel dafür, wie eine Informationsressource politischen Druck für die Legitimisierung des Zugangs bringen kann. Dieser wird von Gruppen bekämpft, die sich für die bürgerlichen Freiheiten und für Patienten einsetzen.

Das Problem wurde vom Amt der US-Regierung für Technikfolgenabschätzung [Office of Technology Assessment] untersucht. Es bestätigte, daß die Hauptbedrohungen der Privatheit in computerisierten Patientenaktensystemen vielmehr von Insidern als von Outsidern kommen, und daß sie durch die Datenaggregation verschärft werden, die durch vernetzte Computersysteme begünstigt wird [OTA93]. Andere Begleiterscheinungen der Datenaggregation sind die Zunahme von Behauptungen, daß man die Informationen benötige, und Behandlungen, die mehr das Interesse des geldgebenden Konzerns als das des Patienten im Auge haben [Woo95].

Die britische Regierung gibt zu, daß es für den breiten Zugang zu identifizierbaren klinischen Aufzeichnungen keine ethische Grundlage gibt. Nicht einmal eine Klinikerin (geschweige denn jemand aus der Verwaltung) darf, ohne daß dies erforderlich wäre, Zugang zu persönlichen Gesundheitsinformationen haben. In den Worten von David Bellamy gesagt, dem Principal Medical Officer im Gesundheitsministerium:

> "Es ist eine weitverbreitete Sichtweise [...] daß ich als Arzt mit einem anderen Arzt alles

mögliche von einem Patienten besprechen kann, weil ein Arzt eine Verpflichtung hat, kraft seiner ethischen Auflagen die Vertraulichkeit zu wahren. Das ist einfach nicht wahr und nicht mehr wasserdicht. Selbst wenn es den Berufsausübenden hilft, wenn sie einzelne Patienten mit ihren Kollegen besprechen, dürfen sie ausschließlich auf der Grundlage jener Informationen diskutieren, die der Kollege dafür unbedingt wissen muß." [WHC95, S. 16]

Es gibt häufig Behauptungen von Versicherern, Sozialarbeitern, Polizisten und Verwaltern, daß es für sie "erforderlich" ist, persönliche Gesundheitsinformationen zu erfahren. Wenn solche Behauptungen überprüft werden, kann es hilfreich sein, im Kopf zu behalten, daß die Notwendigkeit für einen Chirurgen, den HIV-Status eines Patienten zu wissen - so daß er zusätzliche Vorsichtsmaßnahmen ergreifen kann, um Nadelstichverletzungen zu vermeiden - nicht genügt, um sich über das Recht des Patienten auf die Privatheit seines Status hinwegzusetzen. In einem kürzlich durchgeführten Gerichtsverfahren wurde befunden, daß nicht einmal der HIV-Status eines Arztes offenbart werden darf: das kleine Risiko für die Gesundheit von Patienten wiegt nicht das öffentliche Interesse an der Vertraulichkeit auf, die es infizierten Personen ermöglicht, Hilfe zu suchen [DGMW94].

Die British Medical Association akzeptiert nicht, daß die "Notwendigkeit zu Wissen" ["need-to-know"] eine akzeptable Basis für Entscheidungen über die Zugangskontrolle sei. Wie die Dokumente der EU und des General Medical Council deutlich machen, ist es die Einwilligung des Patienten, die zählt. Das Konzept von der "Notwendigkeit zu Wissen" ["need-to-know"] impliziert und ermutigt um der verwaltungsmäßigen Vereinfachung willen die heimliche Erosion des Patientenprivilegs. Auf jeden Fall verleihen Notwendigkeiten keine Rechte: die Notwendigkeit für die Polizei, zu wissen, ob ein Verdächtiger die Wahrheit sagt, verleiht ihr nicht das Recht, ihn zu foltern. Es ist auch nützlich, empirische Untersuchungen über Einstellungen von Patienten im Kopf zu behalten, die starken Widerstand gegen das Mitteilen von persönlichen Gesundheitsinformationen an Verwaltungspersonal des NHS, Sozialarbeiter und Statistiker der Regierung belegen [Haw95].

2.4. Andere Bedrohungen der Sicherheit von klinischen Informationen

Zusätzlich zu den Bedrohungen der Vertraulichkeit von klinischen Informationen kann deren Integrität und Verfügbarkeit in Computersystemen gefährdet sein. Das ist oft in Arten und Weisen der Fall, die nicht unmittelbar offensichtlich sind.

- Softwarefehler ["bugs"] und Hardwareversagen verfälschen gelegentlich Mitteilungen. Zwar versagen auch Post-, Fax- und Telefonsysteme, doch sind die Arten von deren Versagen auffälliger als die von Computer-Mitteilungssystemen. Es ist zum Beispiel möglich, daß eine Softwarefehler die Ziffern in einem Laborbericht verändert, ohne daß dies so stark geschieht, daß der Bericht zurückgewiesen würde.

  Es gibt regelmäßig Zeitungsgeschichten über verlegte Gebärmutterhalsabstriche und von Schwangerschaften, die in der irrtümlichen Annahme abgebrochen werden, daß das Kind ein Down-Syndrom (Mongolismus) hat. Wir wissen nicht, wie viele davon auf Computerfehler im

Gegensatz zu Fehlern bei manueller Bearbeitung zurückzuführen sind, aber die Erfahrungen in anderen Bereichen legen die Annahme nahe, daß beim Fehlen starker Integritätskontrollen etwa eine von 10.000 Mitteilungen falsch wäre. Für einen Allgemeinarzt könnte das ein falsches Laborergebnis alle paar Jahre und eine gefährliche Behandlung während der gesamten Berufslaufbahn heißen. Mit schlecht gestalteter Software könnten die Zahlen bedeutend höher sein.

- Höhere Irrtumsraten könnten aus der sich ausbreitenden Praxis resultieren, Laborergebnisse als unstrukturierte elektronische Post (Email) - Mitteilungen zu versenden, die manchmal automatisch ausgewertet werden. Ein Szenario aus [Mar95] ist plausibel: eine Laborkraft setzt einen Kommentar vor ein numerisches Ergebnis, aber das System des Allgemeinarztes nimmt an, daß der erste Wert, den es antrifft, das Ergebnis ist und übernimmt es in die elektronische Patientenakte, was zu einer falschen Behandlung führt.

- Viren haben bereits klinische Informationen zerstört, und man könnte sich vorstellen, daß ein Virus geschrieben würde, das böswillige Veränderungen in Akten vornimmt.

- Ein böswilliger Angreifer könnte auch Mitteilungen manipulieren. Es ist leicht, Emails zu schicken, die so aussehen, als ob sie von jemand anderem kommen, und mit etwas mehr Aufwand ist es möglich, Post zwischen zwei Benutzern abzufangen und zu modifizieren.

- Auf jeden Fall wird die Mehrzahl der böswilligen Angriffe von Insidern ausgeführt werden [OTA93], aus Motiven wie dem Löschen einer Aufzeichnung eines Kunstfehlers [Ald95], dem Unterhalten einer Sucht oder um geradewegs einen Diebstahl oder Betrug zu begehen. Verschreibungsbetrug geschieht bereits bei manuellen Systemen, und beim Fehlen verbesserter Kontrollen kann man erwarten, daß er weitergehen wird.

- Angriffe gegen Systemintegrität könnten durch eine Erosion der Vertraulichkeit wahrscheinlicher gemacht werden. Wenn klinische Aufzeichnungen auf breiter Ebene verfügbar und für Zwecke wie Entscheidungen über Einstellungen und Kredite benutzt würden (wie in den USA [Woo95]), dann gäbe es starke Motive, sie zu verändern.

- Eine Erosion des öffentlichen Vertrauens würde auch die Qualität des Inputs verschlechtern, da manche Patienten sensible Fakten für sich behalten würden. Die öffentliche Besorgnis in den USA hat inzwischen ein solches Niveau erreicht, daß eine im ganzen Land erscheinende Zeitung ihre Leser dazu angehalten hat, vorsichtig beim Offenbaren sensibler Gesundheitsinformationen zu sein [USA95].

- Wir könnten gleiche Effekte zu sehen bekommen, wenn einige Systemkomponenten für andere Zwecke als den Gesundheitsbereich ausgelegt sind oder werden. Wenn zum Beispiel eine Gesundheitskarte als Identitätsnachweis verwendet werden würde [DPR95], dann würden sowohl Kriminelle als auch Personen oder Gruppen, die um die bürgerlichen Freiheiten besorgt sind, versuchen, deren Sicherheitseinrichtungen zu knacken, und Patienten würden unabhängig von allen Versicherungen der Regierung annehmen, daß die Polizei Zugang zu den Daten hat.

Aus allen diesen Gründen sollten die Vertraulichkeits- und Integritätseigenschaften klinischer Systeme nicht isoliert voneinander betrachtet werden.

2.5 Schutzprioritäten

Ein üblicher Fehler in Angelegenheiten der Computersicherheit ist es, den Blick ganz auf "schillernde", aber wenig wahrscheinliche Bedrohungen zu richten, wie zum Beispiel die Möglichkeit, daß ein fremder Nachrichtendienst Abhörtechnik einsetzen könnte, um die elektromagnetische Streustrahlung von Computermonitoren zu entschlüsseln. Obwohl derartige Angriffe möglich sind, können sie in der Praxis außer acht gelassen werden, da ein fähiger und motivierter Gegner billigere und verläßlichere Wege finden würde, um an Informationen heranzukommen (z.B. Einbruch oder Bestechung).

Ein anderes Beispiel ist die Publicity, die gelegentliche Angriffe von Hackern auf das Internet erhalten. Es ist richtig, daß fähige Hacker den Verkehr auf verschiedene Weisen manipulieren und dabei Erfolg haben können, sich durch Techniken des Paßwort-Schnüffels und Adressen-Schwindelns in Systeme einzuloggen. Jedoch ist die Häufigkeit solcher Angriffe gering, und kompetente Anbieter von Internetdiensten bedienen sich einer elektronischen Brandmauer [firewall], um sie schwierig zu machen. Es gibt das viel größeres Risiko, daß das Computersystem physisch aus der Praxis gestohlen wird; über 10% der Allgemeinärzte haben einen Computerdiebstahl erlebt [PK95].

Wir müssen daher einen Unterschied machen zwischen Verletzlichkeiten (Dinge, die schiefgehen könnten) und Bedrohungen (Dinge, bei denen wahrscheinlich ist, daß sie schiefgehen). Es ist zu beachten, daß andere Autoren diese beiden Wörter mit den umgekehrten Bedeutungen verwenden. Wie auch immer, solche Dispute sind für unsere gegenwärtigen Anliegen nur am Rande von Bedeutung.

Die Reichweite [scope] von Bedrohungen variiert und wird von uns als die Anzahl der betroffenen Individuen definiert. Es gibt globale Bedrohungen der Privatheit, Integrität oder Verfügbarkeit von persönlichen Gesundheitsinformationen der gesamten Bevölkerung, wie zum Beispiel den bereits existierenden schwarzen Markt für persönliche Gesundheitsinformationen; die meisten Bedrohungen sind hingegen lokal begrenzt und beeinträchtigen die Privatheit, Integrität oder Verfügbarkeit von klinischen Aufzeichnungen, die von einem Behandlungsteam gehalten werden. Beispiele sind der Diebstahl von Geräten, Feuer, Virusbefall und die Offenbarung von Aufzeichnungen gegenüber Dritten durch nachlässiges Personal.

Lokale Bedrohungen können durch mehr oder weniger gut verstandene Techniken im Rahmen gehalten werden, wie zum Beispiel durch Training des Personals, Sicherungskopien an einem anderen Ort und regelmäßige unabhängige Überprüfungen; der Großteil der Sicherheitsbemühungen einer Praxis oder einer Krankenhausabteilung wird ihnen gewidmet sein. Allgemeine Richtlinien sind vom Gesundheitsministerium herausgegeben worden [NHS95], während die British Medical Association ihre eigenen Richtlinien [And96] zu Maßnahmen herausgegeben hat, die getroffen werden sollen, um den ernstesten Bedrohungen entgegenzuwirken, die wir zur Zeit kennen.

Auf der Ebene der Sicherheitspolitik ist es mittlerweile unsere Priorität, daß lokale Angriffe sich nicht

zu globalen entwickeln oder daß sie nicht bereits bestehende globale Bedrohungen durch die schlecht beratene Aggregation von Daten oder durch die Vernachlässigung des Prinzips der Patientenzustimmung verschärfen. Die Prinzipien der Sicherheitspolitik, die wir von allen kommunizierenden klinischen Systemen erzwungen haben wollen, müssen Angelegenheiten wie der Aggregation und der Zustimmung Priorität geben.

2.6 Beispiele für Aggregationen in NHS-Systemen

Die Aggregation von persönlichen Gesundheitsinformationen kann sich auf verschiedenste Arten und Weisen ergeben, von denen manche zweifellos aus wohlmeinender Absicht geschehen, während andere von außerklinischem Druck getrieben sind. Zu den Beispielen aus gegenwärtigen und geplanten NHS-Systemen gehört folgendes:

- der geplante NHS-Abrechnungsdienst für Vertragsdaten aus stationären Behandlungen wird Informationen über Krankenhausbehandlungen von Patienten im ganzen Land enthalten. Anfragen der BMA, ob sie sich eine Übersicht über die funktionalen Spezifikationen dieses Systems verschaffen dürfe, wurden mit der Versicherung abgewiesen, diese Informationen befänden sich nicht in einem öffentlichen Datennetz [not in the public domain];

- die Verwaltungsregister enthalten sensible Informationen wie die frühere Registrierung von Patienten in Arztpraxen wegen empfängnisverhütender Dienste und Beziehungen zu Behandlungseinrichtungen für psychisch Kranke;

- mindestens zwei Systeme sind entwickelt worden, die es den Gesundheitsbehörden ermöglichen, "Item-of-Service-Claims" [in Großbritannien die über Pauschalen hinaus einzeln vergüteten Leistungen - avh], Verschreibungen und Vertragsdaten zu verknüpfen, um eine 'Schatten'-Patientenakte außerhalb der klinischen Kontrolle zu schaffen [AIS95][DL95];

Die genannten Systeme sind in Auftrag gegeben worden, obwohl es eine Übereinkunft zwischen dem NHS-Vorstand und den Berufsverbänden gab, daß elektronische Patientenakten mindestens so sicher sein sollen wie papierne Akten, und trotz bestehender Richtlinien der GMSC/RCGP Joint Computer Group, die festlegen, daß kein Patient für jemand anderen als seinen Hausarzt aus Daten identifizierbar sein soll, die ohne seine informierte Zustimmung an eine äußere Organisation geschickt werden [JCG88].

Ein strategisches Ziel der Information Management Group der NHS-Zentralverwaltung ist eine von allen gänzlich geteilte Patientenakte; so wie wir es sehen, soll die Sammlung von Daten vom Hausarzt die Triebkraft sein, und die Hausarztsysteme sollen von NHS-Systemen abgefragt werden. Diese Ziele stehen jedoch in klarem Konflikt zu der ethischen Position sowohl der British Medical Association [Som93] als auch zu den oben erwähnten Richtlinien der Joint Computer Group.

Eine Zustimmung der Patienten zum Teilen von persönlichen Gesundheitsinformationen mit dem Verwaltungspersonal des NHS liegt nicht vor; vielmehr zeigt eine Untersuchung, daß die meisten

Patienten es ablehnen, persönliche Gesundheitsinformationen mit diesem zu teilen [Haw95]. Daß diese Informationen in großen Aggregationen gesammelt werden sollen, über die nicht einmal die in Gesundheitsberufen Beschäftigten die Kontrolle haben, ist extrem gefährlich; wie die Erfahrung aus den USA gezeigt hat, wird die bloße Existenz einer solchen potentiell wertvollen Ressource starken politischen Druck für einen legitimisierten Zugang durch Strafverfolgungsbehörden, Versicherungen und andere erzeugen.

Dieses Dokument gehört zur Antwort der British Medical Association darauf. Sein primärer Zweck ist es, klinisch Arbeitenden zu helfen, ihren ethischen und rechtlichen Verantwortlichkeiten nachzukommen, indem sie geeignete Systeme auswählen und sie sicher betreiben. Es versucht zu definieren, welcher Art von Systemen man vernünftigerweise persönliche Gesundheitsinformationen anvertrauen kann. In diesem Sinne werden wir auf dem in diesem Abschnitt entwickelten Bedrohungsmodell aufbauen und daraus eine Sicherheitspolitik für klinische Informationssysteme entwickeln. Diese besteht aus einem kompakten Satz von Prinzipien, die, wenn sie sachgemäß implementiert worden sind, die Patientenzustimmung in kommunizierenden Computersystemen wirksam erzwingen.

3 Die Sicherheitspolitik

Das Prinzip der Zustimmung und die Regeln, die zu dessen Interpretation verwendet werden, sind gut verankert - sie haben sich aus Jahrhunderten klinischer Erfahrung herausgebildet und werden von Datenschutzgesetzen unterstützt. In diesem Abschnitt drücken wir sie in der Form einer Sicherheitspolitik aus - einem Satz von Prinzipien, die bestimmen, welche Person in einem Computersystem Zugang zu welchem Objekt haben kann [which subject can access which object]. Sie enthalten nichts, das radikal neu wäre, sondern sie drücken Prinzipien des gesunden Menschenverstandes noch einmal in der modernen Sprache der Computersicherheit aus.

Die Sicherheitspolitik deckt ganz allgemein klinische Systeme ab. Manche Klinikerinnen werden zusätzliche Anforderungen haben, und diejenigen, die mehr als einen identifizierbaren Patienten gleichzeitig behandeln (wie Kinderpsychiater, Embryologen und Personen, die am menschlichen Genom forschen) sind mit besonders subtilen Gefahren konfrontiert. Zum Beispiel können Zugangsrechte, die von Betroffenen genossen werden [data subjects], es diesen ermöglichen, Informationen von anderen einzusehen; auch gibt es in vielen Fällen besondere rechtliche Anforderungen. Designer von Systemen, die solche Aktivitäten unterstützen, sollten weitere Beratung einholen.

Eine Bemerkung zu Struktur von Patientenakten

Grundsätzlich gibt es zwei Arten, wie man elektronische klinische Aufzeichnungen organisieren kann. Die erste spiegelt das bestehende papiergestützte System wieder; jede Klinikerin führt eine Akte in ihrem Computer (oder manuellen Karteisystem), und Informationen werden zwischen ihnen in Form von Zusammenfassungen (wie zum Beispiel Überweisungs- und Entlassungsbriefen) übermittelt. Die zweite geht von der Annahme aus, daß es zu jedem Patienten eine einzelne elektronische Akte gibt, die vor der Geburt angelegt und nach der Autopsie geschlossen wird, und die alles enthält, was aus der Zeit dazwischen von klinischem Interesse ist.

Nachfolgend werden wir mit der Annahme des ersten Paradigmas beginnen, da es in der tatsächlichen klinischen Praxis vorherrscht und der Umgang damit viel einfacher ist. Wenn wir erst einmal eine Sicherheitspolitik für diesen Fall entwickelt haben, werden wir den anderen Ansatz diskutieren, der "patientengestützte Akten" genannt worden ist, der aber in Wirklichkeit bedeuten kann, daß die Akten in irgendeinem Zentralregister gehalten werden. Zum Schluß werden wir kompromißhafte Ansätze betrachten, zum Beispiel den, wo detaillierte Aufzeichnungen in den Systemen der Klinikerinnen gehalten werden, wobei aber eine zentrale Zusammenfassung mit Verweisen zu jenen Aufzeichnungen zusammengestellt wird.

3.1 Zugangskontrolle

In einem Computersystem hat jeder Benutzer Zugang zu bestimmten Objekten [each subject has access to certain objects]. Diese Zugangsinformation kann benutzergebunden oder objektgebunden gespeichert werden [may be stored by subject or object]. Im ersten Fall werden die Zugangsgenehmigungen Berechtigungen genannt. Sie könnten die Form haben "Dr. Jones darf die Akten lesen von Farid

Abdullahi, James Adams, Wendy Adams, Henry Addenbrooke, ..." Wenn die Genehmigungen mit den Objekten gespeichert werden, nennt man sie Zugangskontrollisten, und sie könnten die Form haben: "Das ist die Akte von Farid Abdullahi und sie darf gelesen werden von Dr. Jones, Dr. Smith und Schwester Young". Der letzte Ansatz führt zu einfacheren technischen Lösungen, da die Anzahl der Patienten pro Arzt viel größer ist als die Anzahl der Ärzte pro Patient.

Bei normalem Ablauf darf jede Klinikerin mit Zugang zu einer Akte sie nicht nur lesen, sondern ihr auch Informationen hinzufügen (mit dem Löschen von Informationen werden wir uns später beschäftigen). Unser erstes Prinzip ist daher:

> **Prinzip 1**: Jede personenbezogene klinische Akte soll mit einer Zugangskontrolliste versehen sein, die die Personen oder Personengruppen benennt, die die Akte lesen und ihr Daten anfügen dürfen. Das System soll verhindern, daß irgend jemand, der nicht auf der Liste steht, in irgendeiner Weise Zugang zur Akte findet.

In vielen gängigen Systemen sind die Zugangskontrollisten implizit enthalten. Wenn eine Akte in einer Praxisdatenbank vorhanden ist, dann können alle Ärztinnen in der Praxis sie lesen und ihr Dinge anfügen. Mit der Einführung von vernetztem Arbeiten müssen jedoch Zugangskontrollisten explizit und mit einer ganze Bandbreite von Systemen verträglich gemacht werden, und sie müssen von Mechanismen durchgesetzt werden, die nicht nur technisch effektiv sind, sondern auch Vertretungssituationen und die gemeinsame Patientenbetreuung unterstützen.

Um das zu erleichtern, können auch Gruppen anstelle von individuellen Namen verwendet werden. Wenn zum Beispiel Dr. Jones, Dr. Smith und Schwester Young zusammen das Personal der Praxis in Swaffham sind, dann können die Akten, zu denen sie alle Zugang haben, einfach mit "Swaffham" gekennzeichnet werden. Diese Idee gehörte als inhärenter Bestandteil zur Entwicklung von Betreuung in der Gemeinde [Community Care]; die Teams bestanden aus Ärztinnen, Schwestern und dem Personal von sozialen Diensten, und wenn man begann, festzulegen, welche Informationen man miteinander teilen würde, wurde eine schriftliche Einwilligung dazu eingeholt. Auf diese Weise wußten die Patienten, wem sie mit ihrer Unterschrift ihr Vertrauen gaben.

Manchmal jedoch bestehen die einzig sinnvollen Gruppen aus einer großen Zahl von Personen. In großen Krankenhäusern und in "community health trusts" können es hunderte von Pflegepersonen sein, die zum Dienst auf einer bestimmten Station oder in einer bestimmten Einrichtung eingeteilt sind. Dann können einige besondere Beschränkungen beim Definieren von Gruppen erforderlich werden; zum Beispiel kann die Gruppe "alles diensthabende Personal auf derselben Station, auf der der Patient ist" sein. Solch ein Ansatz wäre das elektronische Äquivalent des herkömmlichen "Kurvenwagens" der Station, aber mit dem zusätzlichen Vorteil, daß man Aufzeichnungen darüber haben kann, wer was eingesehen hat.

Wann immer Gruppen verwendet werden - ob nun einfache Gruppen mit einigen wenigen Klinikerinnen oder komplexe mit Ortsangaben und anderen Beschränkungen - es muß immer eine Aufzeichnung

darüber geführt werden, welche Einzelperson eine Akte gelesen oder ihr irgend etwas angefügt hat. Wir werden die Zuschreibungen unten ausführlicher besprechen; hier betonen wir bloß, daß Gruppen keine virtuellen Klinikerinnen sind, sondern Mechanismen, die das Kartographieren der Zugangsberechtigungen zwischen identifizierten Klinikerinnen und identifizierten Patientinnen vereinfachen. Die Systemgestalter sollten im Kopf behalten, daß eine bestimmte Systembenutzerin zu vielen verschiedenen Gruppen gehören kann: sie kann zugleich eine Patientin, eine Ärztin, eine Ausbilderin, eine Auszubildende, eine Praxismanagerin und eine Gutachterin für eine Gesundheitsverwaltung [health authority, terminus technicus aus dem britischen Gesundheitswesen] sein. Wenn man nicht Vorsorge trifft, wie mit dieser Komplexität umgegangen werden soll, wird der resultierende Umgang wahrscheinlich kein guter sein; ad hoc-Methoden sollten vermieden werden.

Zum Beispiel kann nicht akzeptiert werden, daß eine Gruppe ein Paßwort hat, das vom ganzen Personal der Station geteilt wird, oder wenn ein Terminal unter dem Namen des Facharztes ständig eingeloggt gelassen wird. Solche Mißbräuche bedeuten, daß Handlungen keinen Einzelpersonen mehr zugeordnet werden können, und das kann schlimme Folgen haben. Wir kennen den Fall, daß ein psychiatrischer Patient ein Stationsterminal verwendet hat, um mit Mordabsicht Verschreibungsdaten zu verändern.

Wenn ein Patient sich zum ersten Mal in einer Praxis anmeldet oder auf andere Weise eine Beziehung zu einem Behandlungsteam eingeht und eine Akte für ihn angelegt wird, sollte er Informationen über die Politik der Zugangskontrolle des Teams erhalten. Er muß auch die Gelegenheit erhalten, Einwände zu erheben und zu verlangen, daß seine Akte auf eine oder mehrere namentlich festgelegte Klinikerinnen beschränkt wird. Aus diesem Grund müssen auf Berufsrollen aufbauende Systeme trotzdem noch Zugangskontrollisten mit stärkeren Zugangsbeschränkungen unterstützen, und zwar insbesondere solche, die nur eine einzige namentlich genannte Klinikerin enthalten (zusammen mit dem Patienten natürlich).

Eine solche Liste könnte im Fall von hochsensiblen Daten sogar die Grundeinstellung des Systems sein. Die Entscheidung über die tatsächliche Sensibilität einer Akte hängt vom betroffenen Patienten oder der betreffenden Patientengruppe ab. Zu den von vornherein hochsensiblen Daten gehören psychiatrische Aufzeichnungen, Aufzeichnungen über durch Geschlechtsverkehr übertragbare Krankheiten und alle Informationen, die Dritte gegeben haben oder die Dritte betreffen (siehe [GC95], S. 44, für eine vollständigere Liste). Wie auch immer, jemand, der in einer Kampagne über AIDS aktiv ist, mag vielleicht seinen HIV-Status öffentlich machen, während für einen Zeugen Jehovas vielleicht schon eine Bluttransfusion zutiefst beschämend ist. Also bleibt die Zustimmung des Patienten das oberste Gebot, und niemand darf der Zugangskontrolliste hinzugefügt werden, ohne daß der Patient benachrichtigt wird. Wir werden Benachrichtigungen unten noch detaillierter besprechen.

Schließlich gibt es auch einige Anwender, wie Kontrollpersonal und Forscher, die überhaupt keinen Schreibzugang zur primären Akte haben. Wir werden die mit ihnen zusammenhängenden speziellen Probleme weiter unten besprechen, aber der Einfachheit halber werden wir in dieser Sicherheitspolitik keine gesonderten Vorkehrungen für einen ausschließlichen Lesezugriff vorschlagen. Wir werden vielmehr annehmen, daß diese Personen vollen Zugang zu einer temporären Kopie der Originalakte erhalten; und das ist in Wirklichkeit ein besseres Modell dafür, wie sie tatsächlich arbeiten.

3.2 Einrichten einer Akte

Anstatt zu versuchen, mit Objekten umzugehen, die multiple Zugangskontrollisten haben, werden wir annehmen, daß es multiple Akten gibt. Ein Patient könnte zum Beispiel haben:

- eine allgemeine Akte, die allen Klinikerinnen in der Praxis offensteht;
- eine hochsensible Akte über die Behandlung einer Depression, die nur dessen individueller Hausärztin offensteht;
- eine Akte über dessen Herzerkrankung, die allem Notfallpersonal offensteht und von der eine Zusammenfassung auf einem Notfallausweis aus Papier oder Plastik eingetragen werden könnte.

Das ist das logische Äquivalent zum Führen einer Akte mit drei verschiedenen Feldern, von denen jedes seine eigene Zugangskontrolliste hat. Es ist jedoch viel einfacher, mit den einzelnen Akten umzugehen.

Die Klinikerin kann also eine neue Akte anlegen, wenn ein schon vorhandener Patient etwas Hochsensibles mit ihr besprechen möchte, oder wenn ein Patient sich neu bei ihr registrieren läßt, oder wenn ein Patient von anderswo zugewiesen wurde. Die Zugangskontrolliste auf einer neuen Akte geht wie folgt:

> **Prinzip 2**: Eine Klinikerin kann eine Akte mit ihr selbst und mit dem Patienten auf der Zugangskontrolliste einrichten. Falls ein Patient überwiesen wurde, kann sie eine Akte mit ihr selbst, dem Patienten und der (den) zuweisenden Klinikerin(nen) auf der Zugangskontrolliste einrichten.

3.3 Kontrolle

Abgesehen vom Patienten selbst dürfen nur Klinikerinnen Zugang zu persönlichen Gesundheitsinformationen haben. Die Gründe dafür, die Umgrenzung für den Vertrauensbereich [trust perimeter] mit der Grenze der Berufsstände [professional boundary] zusammenfallen zu lassen, sind sowohl traditionell als auch praktisch; die klinischen Berufe sind der Ansicht, daß die zivil- und strafrechtlichen Mechanismen für einen angemessenen Schutz nicht ausreichen. Wenn ein Ärztin eine Akte einer Sozialarbeiterin gäbe, die sie dann einem Dritten überließe - oder sie auch nur in einem unsicheren lokalen Computersystem der Gemeindeverwaltung speichern würde, in das "hineingehackt" würde [geschehen in Salzburg Ende 1997 - avh] - dann könnte immer noch die Ärztin zur Rechenschaft gezogen werden und ihr stünde kein Rechtsweg zur Verfügung.

Letztlich traut man nur Klinikerinnen zu, daß sie das Prinzip der informierten Zustimmung konsequent durchsetzen, und die Kontrolle über jegliche identifizierbare klinische Akte muß bei der individuellen

verantwortlichen Klinikerin liegen. Das kann die niedergelassene Ärztin des Patienten sein oder die Ärztin, die einer Klinikabteilung vorsteht.

> **Prinzip 3**: Eine der Klinikerinnen auf der Zugangskontrolliste muß als verantwortlich markiert sein. Nur sie darf die Zugangskontrolliste verändern, und sie darf dieser ausschließlich andere im Gesundheitswesen Beschäftigte [other Healthcare Professionals] hinzufügen.

Wo Verwaltern Zugang gewährt wurde, wie in den USA, war das Ergebnis Mißbrauch. In Großbritannien ist das Spannungsverhältnis zwischen klinischer Vertraulichkeit und administrativem "Wissenmüssen" ["need-to-know"] durch Regelungen abgemildert worden, nach denen Organisationen des National Health Service, die Gesundheitsleistungen einkaufen, "Schutzhäfen" ["safe-havens"] - geschützte Räume unter der Kontrolle einer unabhängigen Klinikerin - haben müssen, wohin Akten im Falle administrativer Meinungsverschiedenheiten gesandt werden können [NHS92]. Verwaltungssysteme, in denen persönlichen Gesundheitsinformationen bearbeitet werden könnten, müssen "safe-haven"-Prozeduren unterstützen; zum Beispiel könnten die klinischen Teile von Patientenakten so verschlüsselt werden, daß nur die Klinikerin, die für den "safe-haven" verantwortlich ist, sie entschlüsseln kann. Solche Systeme müssen auch den oben erwähnten Richtlinien der Joint Computer Group entsprechen [JCG88; Nachtrag von Anfang 1998: "Schutzhäfen" sind inzwischen obsolet, da die neuen Computersysteme in den Health Authorities den Verwaltungsangestellten ohnehin den online-Zugang zu allen Akten ermöglichen - rja].

Wenn von Dritten wie einem Sozialarbeiter, einem Anwalt, einem Polizeibeamten, jemandem, der eine Sicherheitsüberprüfung durchführt, einem Versicherer oder Arbeitgeber Informationen gewünscht und im Einklang mit den Gesetzen zur Verfügung gestellt werden können, dann müssen die Informationen auf Papier übermittelt werden. Das spiegelt die gegenwärtige Praxis wieder: im oben erwähnten Szenario der Betreuung in der Gemeinde wurden die Aufzeichnungen, die von Ärztinnen, Krankenschwestern und Sozialarbeiterinnen gemeinsam benutzt wurden, aus Sorge um die Sicherheit auf Papier statt in einer Datenbank gehalten.

Man sollte auch bedenken, daß Computeraufzeichnungen nicht als Beweismaterial zu gebrauchen sind, wenn sie nicht zusammen mit einer papiernen Bescheinigung vorgelegt werden, die vom Systembesitzers oder -betreiber unterzeichnet ist; direkter elektronischer Zugang hat wenig Beweiswert, und eine unterschriebene Feststellung auf Papier kann am besten die Anforderungen an die Glaubwürdigkeit von Beweismaterial erfüllen.

3.4 Einwilligung und Mitteilung

Wenn andere Klinikerinnen an die Zugangskontrolliste angefügt werden sollen, muß die Einwilligung des Patienten eingeholt und muß ihm jede Hinzufügung mitgeteilt werden. Im normalen Arbeitsablauf kann ein Plakat oder eine Box mit Faltblättern, gut sichtbar im Anmeldebereich der Praxis oder des Krankenhauses plaziert, dieses Erfordernis in Bezug auf die unmittelbaren Kolleginnen der Klinikerin abdecken. Das gilt, solange es effektive Wege gibt, um den wenigen Patienten gerecht zu werden, die

darauf bestehen, daß Aufzeichnungen über sie nur der einen behandelnden Klinikerin zugänglich sind. Das Hinzufügen anderer Klinikerinnen zur Zugangskontrolliste, zum Beispiel wenn ein Patient ins Krankenhaus eingewiesen wird, sollte normalerweise vorher mit dem Patienten besprochen werden. Wenn jedoch Informationen mitgeteilt werden, obwohl die Zustimmung fehlt, zum Beispiel wenn eine Hausärztin einer Unfallabteilung Informationen unter Notfallbedingungen übermittelt, dann muß eine Mitteilung erzeugt und dem Patienten zugeschickt werden. Dies liegt in der Verantwortung der Hausärztin; wenn sie bloß annähme, daß das Krankenhaus dies dem Patienten mitteilen würde, dann handelte sie grob fahrlässig. Illegale Informationshändler beziehen oft persönliche Gesundheitsinformationen, indem sie vortäuschen, mit der Notfallbehandlung von Patienten zu tun zu haben; detaillierte Anleitungen für das Design von Notfallprozeduren gibt es in [And96], wo die Notwendigkeit betont wird, die Identität des Anrufers zu verifizieren (wie z.B. durch das Zurückrufen nach einer Nummer, die im Arztregister steht) und dem Patienten immer Mitteilung zu machen.

Das Mitteilen stellt eine "End-zu-End"-Überprüfung dar, die das Management nicht durch das Vereinnahmen von Prüfern oder von Personen, deren Karriere von der sie beschäftigenden Organisation abhängt [im Orig.: regulators; z.B. leitende Ärzte, betriebliche Datenschutzbeauftragte u.a. - rja] verletzen kann. Auch könnte zum Beispiel ein Krankenhausangestellter von einem illegalen Informationshändler bestochen werden, damit er unter der falschen Behauptung, daß der Patient bewußtlos eingeliefert worden sei, bei einer Allgemeinpraxis um Zugang zu der Akte eines Patienten anfragt. Die Rückruf-Kontrolle wäre in diesem Fall nicht wirksam, aber die Mitteilung an den Patienten ermöglicht, daß der Angriff entdeckt und untersucht werden kann.

Das Erfordernis der Mitteilung ergibt sich also aus dem Prinzip der Einwilligung. Es hilft auch, Betrug in der Privatpraxis unter Kontrolle zu halten, da Geldmittel für Gesundheitsleistungen begrenzt sein mögen und Patienten mit teuren Behandlungserfordernissen sich als andere Patienten ausgeben können, wenn ihre Budgets auslaufen.

Vom Erfordernis der Mitteilung gibt es keine Ausnahmen. Selbst wenn eine Ausübende eines klinischen Berufs gesetzlich verpflichtet ist, Informationen an Dritte weiterzugeben, muß der Patient immer noch benachrichtigt werden. Wenn Staatsanwaltschaften oder Gerichte Zugang erhalten oder wenn vermuteter Kindesmißbrauch mit Sozialdiensten diskutiert wird, kann die Mitteilung verzögert werden, falls es vernünftige Gründe für die Annahme gibt, daß sie den Verdächtigen veranlassen würde, zu fliehen, Beweismaterial zu manipulieren oder Zeugen einzuschüchtern. Der Patient muß aber schließlich trotzdem benachrichtigt werden.

> **Prinzip 4**: Die verantwortliche Klinikerin muß dem Patienten Mitteilung von den Namen auf der Zugangskontrolliste seiner Akte machen:
>
> - wenn die Akte eingerichtet wird,
> - bei allen nachfolgenden Hinzufügungen und
> - immer, wenn die Verantwortung weitergegeben wird.
>
> Die Einwilligung des Patienten muß ebenfalls

eingeholt werden, außer im Notfall und bei gesetzlichen Ausnahmen.

Es ist auch die Frage, wie oft man benachrichtigen soll. Das Gefühl von befragten Klinikerinnen und Klinikern war, daß die Mitteilung jährlich mit einem Brief erfolgen sollte, wenn keine Verletzung der Regeln oder ein verdächtiges Aktivitätsmuster entdeckt worden ist. Ganz so einfach geht es aber nicht. Unlängst wurden Hausärztinnen aufgefordert, Frauen zu benachrichtigen, die gewisse Kontrazeptiva verwenden; dies warf die Frage auf, wie man es bei jungen Mädchen halten soll, die ohne Wissen der Eltern Kontrazeptiva einnehmen, und bei Frauen, deren Ehemänner vasektomiert sind [Vasektomie: Durchtrennung der Samenstränge - avh] und welche die Pille in einer neuen außerehelichen Beziehung einnehmen. Die bereits in Ambulanzen für Geschlechtskrankheiten praktizierte Lösung ist, daß die Klinikerin am Beginn der Beziehung zwischen der Patientin und ihr fragt, wie Mitteilungen zugestellt werden sollen.

Ein schwierigeres Problem gibt es, wenn die Patient-Klinikerin-Beziehung aufhört hat, zu bestehen. Dazu kann es kommen, wenn eine Privatpraxis aufgelöst wird, ein Patient stirbt oder er ins Ausland geht. Es wurde Besorgnis geäußert, daß der OPCS [Office of Population Censuses and Surveys, heute Office of National Statistics] Emigrationsdaten aus Akten speichern könnte, die von Hausärztinnen entsprechend den gegenwärtigen Regelungen zur Aufbewahrung an Familien-Gesundheitsbehörden übergegeben werden; es wurde vorgeschlagen, daß der Datenschutzbeauftragte alle "toten" elektronischen Akten in Verwahrung nehmen solle. Das wirft jedoch die Frage auf, wer den Bewacher im Auge behält.

Schließlich muß es ein effektives Beschwerdeverfahren geben, das dazu führt, daß Missetäter bestraft werden, ob durch Entlassung, durch ein berufsständisches Disziplinarverfahren oder durch Strafverfolgung. Was soll ein Patient tun, wenn er in seinem jährlichen Bericht entdeckt, daß jemand, den er nie konsultiert hat, seine Akte gelesen hat? Soll er zuerst zu seiner Hausärztin gehen, oder sich mit dem General Medical Council der Sache annehmen, mit einer Art von Ombudsmann, mit dem Datenschutzbeauftragten, dem zuständigen Parlamentsabgeordneten, der Presse oder gar der Polizei? Eine Lösung dieser Frage könnte vom Erfolg der Kampagne der British Medical Association für ein Gesetz abhängen, das die Vertraulichkeit von Gesundheitsinformationen festschreibt [BMA95].

3.5 Fortbestand

Es gibt Vorschriften, wie lange Aufzeichnungen aufbewahrt werden müssen. Die meisten primären Patientenakten müssen acht Jahre lang aufgehoben werden, aber Aufzeichnungen über Krebs müssen aufbewahrt werden, so lange der Patient lebt, und Aufzeichnungen über Erbkrankheiten dürfen noch länger aufbewahrt werden. In jedem Fall diktiert die Vernunft, daß der Zugang zu den Akten erhalten wird, bis die Frist abgelaufen ist, innerhalb derer eine Klage wegen eines Kunstfehlers eingebracht werden kann. Unser nächstes Prinzip ist daher

Prinzip 5: Niemand soll klinische Informationen löschen können, bevor der vorgesehene Zeitraum abgelaufen ist.

Diese Regeln sind jedoch noch nicht ganz ausgearbeitet, weshalb unser Wort "vorgesehen" eine Reihe von offenen Fragen einschließt:

- unsere Formulierung erlaubt die Zerstörung alter Akten, schreibt sie aber nicht vor; es gibt viele Fälle (z.B. chronische Erkrankungen), in denen es angemessen ist, Akten länger zu behalten als das Gesetz es vorschreibt;

- das sechste Prinzip des Datenschutzgesetzes [DPA84] stellt fest, daß persönliche Informationen "nicht länger aufgehoben werden sollen, als es notwendig ist". Das kann bedeuten, daß die Akte zerstört werden soll, wenn die Klinikerin nicht mehr diejenige ist, welche die primäre Akte führt (z.B. wenn der Patient verzogen ist). Es kann aber sein, daß die Klinikerin, bevor sie die Akte zerstört, die Sicherheit möchte, daß die Akte wenn nötig verfügbar gemacht werden kann (z.B. im Fall einer Rechtsstreits);

- die Zustimmung des Patienten ist nicht unwandelbar, sondern vielmehr ein andauernder Dialog zwischen dem Patienten und der Klinikerin [Som93]. Es ist daher gut möglich, daß ein Patient seine Zustimmung zurückzieht und darauf besteht, daß eine Akte zerstört wird. Wir haben noch von keinem solchen Fall gehört; vielleicht könnte mit solchen Fällen so umgegangen werden, daß man die primäre Akte für den Rest der gesetzlich vorgeschriebenen Zeit zu einer Klinikerin nach der Wahl des Patienten transferiert;

- bei zeitweiligen Kopien von Akten wird der angemessene Zeitraum kürzer sein. Wenn zum Beispiel eine Allgemeinpraxis einer nächtlichen Vertretung den Zugang gestattet, dann ist es typischerweise eine Bedingung, daß alle Kopien von Akten innerhalb einer festgelegten Zeit gelöscht werden. Gleiche Überlegungen gelten für Kopien von Akten in "Schutzhäfen" [Erklärung s. 3.3], bei einem Prüfer oder einem Forscher; zum Beispiel sollte die Zustimmung dazu, daß Akten der Forschung zur Verfügung gestellt werden, alle fünf Jahre erneuert werden [Som93]. Aktenkopien bei Forschen sollten folglich diesen Zeitraum nicht überdauern (und normalerweise viel früher zerstört werden). Das Design und die Durchsetzung solcher Anforderungen an die Flüchtigkeit von Akten [volatility requirements] haben Auswirkungen auf die Aggregationskontrolle, die unten diskutiert werden.

Akten zu erhalten ist keine ganz einfache Sache; wir wollen nicht, daß auf der Grundlage von Informationen gehandelt wird, die als unrichtig erkannt worden sind, wie beispielsweise einfache Irrtümer und später revidierte Diagnosen. Wir wollen jedoch nicht das spurlose Ausradieren von Fehlern erleichtern, da dies den Wert der Akte als Beweismittel zerstören würde. So sollten die Informationen (wie in vielen Finanzsystemen) besser durch Anfügen als durch Löschen auf den neuesten Stand gebracht werden, und es sollten die jüngsten Versionen zuerst der Aufmerksamkeit der Klinikerin nahegebracht werden. Löschungen sollten Akten vorbehalten sein, deren Zeit abgelaufen ist.

Ein gleichwertiger Ausdruck des obigen Prinzips kann in den derzeit gültigen Anforderungen für die Zulassung von Praxissystemen gefunden werden, die festlegen, das System dürfe "nicht gestatten, daß

Akten ... verändert oder gelöscht werden, wenn nicht ein sicherer Mechanismus vorgesehen ist, der diese Akten genau so rekonstruieren kann, wie sie an einem jeglichen bestimmten Tag in der Vergangenheit waren" [RFA93].

3.6 Zuschreibung

Als nächstes müssen wir sicherstellen, daß alle erfolgten Zugänge zu den Akten (ob für Lesevorgänge, Anfügungen oder Löschungen) richtig zugeschrieben werden können.

> **Prinzip 6**: Jeder erfolgte Zugang zu klinischen Akten soll in der Akte mit dem Namen des Betreffenden, Datum und Zeit eingetragen werden. Ein solcher "Audit-Vermerk" muß auch bei jeder Löschung erfolgen.

Die unter den gegenwärtigen Anforderungen für die Zulassung entwickelte Systeme zeichnen typischerweise alle Schreibzugänge auf; selbst wenn Material aus der Hauptakte entfernt wird, gibt es einen "Audit-Vermerk", der es ermöglicht, den Stand der Akte so zu rekonstruieren, wie er zu jedem beliebigen Zeitpunkt war, und alle Änderungen jemandem zuzuschreiben [RFA93]. Wenn dies richtig implementiert worden ist, wird das den gleichen Effekt haben, wie wenn man Schreibzugänge auf "Nur Hinzufügen" beschränkt und alle Hinzufüge-Vorgänge mit dem Namen der Klinikerin kennzeichnet. Die neuen Anforderungen bestehen darin, daß Lesezugänge aufgezeichnet werden, so daß das Brechen der Vertraulichkeit verfolgt und bestraft werden kann; und daß über Löschvorgänge aufgezeichnet werden, so daß die absichtliche Zerstörung von belastendem Material jemandem zugeschrieben werden kann.

Bei manchen Anwendungen gibt es besonders strenge Anforderungen an die Zuschreibbarkeit. Zum Beispiel muß eine "Nicht Wiederbeleben"-Notiz in der Akte eines stationären Patienten vom verantwortlichen Facharzt unterschrieben sein, und sie bedarf auch der Zustimmung des Patienten, sofern dieser in der Lage ist, sie zu geben [Som93]. Wenn solche lebenswichtigen Funktionen automatisiert werden, müssen die Mechanismen - einschließlich derer, welche die Zuschreibung ermöglichen - mit derselben Sorgfalt und nach denselben Standards technisch ausgeführt werden, die man bei lebenserhaltenden Systemen erwartet.

Es gibt auch Anforderungen an die Zuschreibung, die selten in Anspruch genommen werden. Zum Beispiel haben Patienten mit nur wenigen Ausnahmen Lesezugang zu allen ihren Akten, und sie können Einwände anfügen, wenn sie welche haben. Diese Wünsche sind selten, weshalb sie typischerweise durch manuelle Mechanismen unterstützt werden. Ein übliches Vorgehen ist, daß die Klinikerin alle Aufzeichnungen ausdruckt, zu denen der Zugang gewünscht wird, und bei Einwänden gibt sie den Kommentar des Patienten ein und händigt diesem eine Kopie der aktualisierten Akte als Beleg aus. Wir haben keine Bedenken gegen eine solche Vorgangsweise. Wir bestehen nicht darauf, daß alle Sicherheit in der Software liegt; uns geht es um den Nettoeffekt aller Verarbeitungsvorgänge, der automatisierten und der manuellen.

3.7 Informationsfluß

Wenn sich zwei Akten mit verschiedenen Zugangskontrollisten auf denselben Patienten beziehen, dann darf ohne erneute Zustimmung ausschließlich Information von der weniger sensiblen zur sensibleren Akte fließen dürfen:

> **Prinzip 7**: Information, die einer Akte A entnommen wurde, darf an eine Akte B dann und nur dann angefügt werden, wenn die Zugangskontrolliste von B in der von A enthalten ist.

Die technischen Mechanismen, die man braucht, um ein solches Prinzip zu erzwingen, sind in Standardtexten zur Computersicherheit beschrieben, zum Beispiel bei Amoroso [Amo94]: Die Zugangskontrolliste für einen Zugangsvorgang selbst soll an die Schnittstelle der Zugangskontrollisten der Akten, die dabei gelesen werden, gesetzt werden, und es soll nur möglich sein, in eine Akte zu schreiben, deren Zugangskontrolliste in der des Zugangsvorgangs enthalten ist.

Wenn sich zwei Akten mit verschiedenen Zugangskontrollisten auf denselben Patienten beziehen, ist die schwierige Frage, ob die Existenz der sensiblen Akte in der anderen ausgewiesen werden soll. Das ist eines der fortwährenden Dilemmata, über die es noch keinen Konsens gibt [GC95]. Wenn die Existenz von verborgenen Informationen ausgewiesen wird, ob nun explizit oder durch die verdächtige Abwesenheit von Teilen der Akte, dann können daraus Schlüsse gezogen werden. Zum Beispiel haben Ärzte in den Niederlanden Krankenakten aus den Computersystemen entfernt, wann immer der Patient eine Krebsdiagnose erhielt. Das Ergebnis war, daß Versicherer und Pensionsfonds wußten, wann immer sie eine leere Akte sahen, daß der Betreffende mit hoher Wahrscheinlichkeit an Krebs litt [Cae95]. Sichtbare Ausweisungen haben auch zu einem Fall in Großbritannien geführt, in dem gegenwärtig ermittelt wird.

Wenn keine Kennzeichnungen angebracht werden, entstehen andere Probleme. Stellen wir uns zum Beispiel vor, ein ambulanter psychiatrischer Patient geht zu einem AIDS-Test und möchte das Ergebnis geheim gehalten haben. Bevor das Ergebnis bekannt ist, bedingt der Streß einen psychischen Zusammenbruch und sein Psychiater bringt eine Markierung an, daß der Patient nicht mehr fähig ist, seine Akten einzusehen. Der Psychiater weiß jedoch nichts vom Test und teilt folglich der Ambulanz für Geschlechtskrankheiten den neuen Status des Patienten nicht mit. Es ist nicht möglich dieses Problem durch ein weltweit lesbares Register der gegenwärtig nicht zum Lesen ihrer Akten fähigen Patienten zu lösen, da psychische Beeinträchtigung sowohl vertraulich als auch eine Funktion der jeweiligen Umstände ist. Eine andere Konsequenz des Nicht-Ausweisens von verborgenen Daten ist, daß es schwieriger ist, Patienten mit einem Münchhausen-Syndrom [nach dem Lügenbaron; Bezeichnung für Patienten, die ständig Krankheiten erfinden, um ins Krankenhaus zu kommen - avh] zu entdecken und mit ihnen umzugehen.

Wir erwarten, daß die Klinikerinnen sich für diskrete Kennzeichnungen entscheiden werden, die lediglich das Vorhandensein von verborgenen Informationen anzeigen. Diese werden für die Klinikerin ein Anlaß sein, zu fragen "gibt es noch etwas, daß Sie mir sagen möchten und das vielleicht wichtig sein könnte", wenn erst einmal etwas Vertrauen aufgekommen ist.

Auf jeden Fall sollten Systementwickler sorgfältig überlegen, wie Sensibilitäts-Eigenschaften bei voneinander abhängigen Akten bzw. von Aktenkopie zu Aktenkopie weitergegeben werden können, und welche Auswirkungen dies auf die Systemintegrität hat.

Schließlich muß es noch einen Mechanismus geben, der die Weitergabe von Daten ermöglicht, die anonymisiert worden sind. Wir werden dieses Thema im Modell der Sicherheitspolitik selbst nicht abhandeln, so wie wir hier auch nicht darauf eingehen, wie man Informationen in Systemen mit mehreren Ebenen so behandelt, daß deren Herkunft nicht erschlossen werden kann [im Orig.: downgrading of information]. Wir raten jedoch, daß das Weitergeben einer Akte, die man für anonym hält, einen bewußt zu setzenden Akt der verantwortlichen Klinikerin erfordern und dokumentiert werden soll.

3.8 Aggregationskontrolle

Die Verwendung von Zugangskontrollisten und starken Regeln für die Benachrichtigung helfen gegen Bedrohungen durch Datenaggregationen. Beides ist aber nicht ganz ausreichend, um diese zu verhindern. Eine Klinikerin mit Verantwortung für einen "Schutzhafen" [Erklärung s. 3.3] könnte der Zugangskontrolliste von Millionen von Krankenhauspatienten hinzugefügt werden, was sie verletzlich gegenüber Verlockungen oder Drohungen von illegalen Informationshändlern macht.

> **Prinzip 8**: Es muß effektive Maßnahmen geben, mit denen die Aggregation (Ansammlung) von persönlichen Gesundheitsinformationen verhindert wird. Insbesondere müssen Patienten eine spezielle Benachrichtigung erhalten, wenn irgendeine Person, die als jemand vorgeschlagen wird, der der Zugangskontrolliste hinzugefügt werden kann, bereits Zugang zu den persönlichen Gesundheitsinformationen einer großen Anzahl von Personen hat.

Manche Krankenhaussysteme enthalten persönliche Gesundheitsinformationen von einer Million oder mehr Patienten, wobei alle Benutzer Zugang haben. Die typische Kontrolle ist gegenwärtig eine Erklärung, daß unberechtigter Zugang zur Entlassung des Arbeitnehmers führen wird; aber oft wird dies nur sporadisch durchgesetzt, und es wird immer wieder über Zwischenfälle wie den Fall Jackson (s. 2.3) berichtet. Ganz allgemein sind Krankenhaussysteme meistens alt und werden dürftig verwaltet [AC95a,b].

Krankenhaussysteme, die allen Klinikerinnen und Klinikern Zugang zu allen Daten ermöglichen, sollten nicht mit Netzwerken verbunden werden. Es ist schlimm genug, wenn 2000 Leute Personal Zugang zu einer Million Akten haben; aber die Aussicht, daß 200 solcher Krankenhäuser zusammengeschlossen werden, womit 400.000 Leute Personal Zugang zu den Krankenhausakten eines Großteils der Bevölkerung erhalten, ist inakzeptabel.

Es wird jedoch unvermeidlich Mechanismen für Klinikerinnen geben, durch die sie an Akten von außerhalb ihres Behandlungsteams herankommen, auch wenn diese manuell geführt werden. Diese Mechanismen müssen sorgfältig gestaltet werden. Wie oben erwähnt könnte ein korrupter Mitarbeiter fälschlich behaupten, daß ein Patient sich im Urlaub selbst im Krankenhaus hat aufnehmen lassen, und sich eine Kopie der Akte schicken lassen wollen. Schon ein einfaches elektronisches Postsystem (email-System) würde es ermöglichen, solche Anfragen im industriellen Umfang zu wiederholen.

Die primäre Kontrolle solcher Bedrohungen ist die Benachrichtigung. Eine wichtige sekundäre Kontrolle ist jedoch, irgendwo eine Zählung laufen zu lassen, wer zu welcher Akte außerhalb des eigenen Teams Zugang hatte. Benutzer, die viele Akten oder eine Anzahl von Akten außerhalb des üblichen Musters einsehen, sind vielleicht nur faul oder nachlässig, doch sie könnten bereits dadurch sich und die Patienten ihrer Kolleginnen einem möglichen Nachteil aussetzen.

In Anbetracht der Spannungen zwischen klinisch tätigen Personen und Verwaltern in Fragen der Privatheit sollten sowohl der Ort für diese Zählung als auch der Modus der Bestimmung der Personen, die darauf Einfluß haben, sorgfältig ausgewählt werden: dabei könnten zum Beispiel die klinischen Disziplinargremien oder die Berufsverbände der Gesundheitsberufe einbezogen werden. Es wäre auch sinnvoll, sich an derselben Stelle mit Berichten von anderen Computermißbräuchen zu beschäftigen. Die Beteiligung der klinischen Verbände könnte mit verhindern helfen, daß die zentrale Sicherheitsfunktion von bürokratischen Interessen vereinnahmt würde. Damit könnte das Prinzip der Zustimmung erhalten werden.

Es gibt Anwendungen, bei denen eine gewisse Aggregation unvermeidlich ist, zum Beispiel Impfprogramme für Kinder. Systeme, die diese unterstützen, wird man intelligent gestalten müssen.

Wie oben erwähnt können Akten für Forschungs- und Prüfzwecke aggregiert werden, vorausgesetzt sie werden ausreichend anonymisiert. Es gibt den Vorschlag, daß Akten anonymisiert werden können, indem man die Namen durch NHS-Nummern und Diagnosen mit Read-Codes ersetzt [RSM92; der Read-Code ist eine von Dr. Read aufgestellte britische Diagnoseverschlüsselung - rja], und eine Reihe von Systemen scheint in der Annahme, daß dies akzeptabel sei, so ausgelegt worden zu sein. Es ist aber nicht akzeptabel; wie oben erwähnt machen es die GMSC/RCGP-Richtlinien zur Bedingung, daß kein Patient für jemand anderen als für dessen Hausärztin aus den Daten identifizierbar sein darf, die ohne die informierte Zustimmung des Patienten an eine externe Organisation geschickt werden [JCG88].

Daten zu anonymisieren ist schwierig, besonders wenn sie verknüpfbare Informationen enthalten: wenn ein Angreifer Suchanfragen an eine Datenbank stellen kann wie "zeige mir alle Frauen mit zwei Töchtern im Alter von 13 und 15 Jahren, die beide unter einem Ekzem leiden", dann kann er Einzelpersonen identifizieren. Die Grenzen der Verknüpfbarkeit und Techniken zum Verhindern des Erschließens von Daten sind als "statistische Sicherheit" bekannt und detailliert im Zusammenhang mit Volkszählungen beforscht worden [Den82]. Wenn es um rein statistische Forschung geht, dann können diese Techniken angewendet werden; wo sie nicht praktikabel sind, könnte Forschern der Zugang zu verknüpfbaren Daten in einem geschützten Raum gewährt werden [Boe93].

3.9 Die Trusted Computing Base (TCB, Vertrauenswürdige Einrichtung zur Datenverarbeitung)

> [Anmerkung des Übersetzers: die in der Computerliteratur gängige, aber falsche deutsche Übersetzung von "Trusted Computing Base" als "Sichere Computereinrichtung" wird hier bewußt nicht verwendet. "Sicher" ist eine Zuschreibung, die recht statisch wirkt und mehr das Objekt im Blick hat. "Vertrauenswürdig" lenkt die Aufmerksamkeit mehr auf den Urteilsakt der Personen, die Vertrauen schenken oder verweigern können, was dem Thema angemessener erscheint. Diese Übersetzung paßt auch besser zum dritten und vierten nachfolgenden Absatz.]

Zum Schluß müssen wir noch sicherstellen, daß die Mechanismen in der Praxis auch so wirksam sind wie in der Theorie. Das führt zur Fragen der Evaluation und Anerkennung.

In der Terminologie der Computersicherheit ist die Trusted Computing Base (vertrauenswürdige Einrichtung zur Datenverarbeitung) die Gesamtheit aller Hardware-, Software- und prozeduralen Komponenten, welche die Sicherheitspolitik durchsetzen. Das bedeutet, daß ein Angreifer, der die Sicherheit brechen will, eine oder mehrere Komponenten zu Fall bringen muß.
An dieser Stelle wollen wir erklären, was wir mit "Vertrauen" meinen. Im allgemeinen Sprachgebrauch meinen wir, wenn wir sagen, daß wir jemandem vertrauen, daß wir uns darauf verlassen, daß diese oder jene Person bestimmte Dinge tun - oder nicht tun - wird. Zum Beispiel erwartet ein Patient, der vertrauliche Informationen mit einer Klinikerin teilt, daß diese Informationen nicht ohne seine Zustimmung mit Dritten geteilt werden, und er verläßt sich darauf, daß diese Erwartung erfüllt wird.

Eine mögliche Sichtweise von solchen Beziehungen, die man für das Gestalten von Systemen wertvoll fand, definiert eine vertrauenswürdige Komponente als eine, die die Sicherheit durchbrechen kann. Somit befindet sich eine Klinikerin, die vertrauliche Informationen von einem Patienten erhalten hat, in einer Position, aus der heraus sie ihm schaden kann, indem sie jene Informationen offenbart, und der Patient ist davon abhängig, daß sie es nicht tut. Es wird in jedem Computersystem Teile geben, von denen wir in gleicher Weise abhängig sind. Wenn sie außer Kraft gesetzt werden oder Softwarefehler enthalten, dann kann die Sicherheitspolitik umgangen werden.

Die vertrauenswürdige Einrichtung zur Datenverarbeitung eines klinischen Informationssystems kann Computer-Sicherheitsmechanismen beinhalten, welche die Authentifizierung des Benutzers und eine Zugangskontrolle erzwingen, Mechanismen der Kommunikationssicherheit, um den Zugang zu Informationen bei deren Transit durch ein Netzwerk einzuschränken, Mechanismen zur Schaffung von statistischer Sicherheit, um zu gewährleisten, daß in der Forschung und bei Überprüfungen verwendete Akten keine ausreichenden Restinformationen enthalten, die eine Identifizierung von Patienten möglich machen würden, und Mechanismen, die die Verfügbarkeit gewährleisten wie Prozeduren zum Erstellen von Sicherungskopien, damit sichergestellt ist, daß Akten nicht durch Feuer oder Diebstahl vernichtet werden.

Das Design dieser Mechanismen wird detailliert im nächsten Abschnitt diskutiert. Hier stellen wir erst einmal fest, daß es nicht ausreicht, sich auf die Zusicherungen der Geräteverkäufer zu verlassen, daß ihre Produkte "sicher" seien - diese Behauptungen müssen von kompetenten Dritten überprüft werden.

Prinzip 9: Computersysteme, die persönliche

> Gesundheitsinformationen verarbeiten, sollen ein Untersystem haben, das auf effektive Weise die obengenannten Prinzipien erzwingt. Dessen Effektivität soll Gegenstand der Evaluation durch unabhängige Experten sein.

Langjährige Erfahrungen haben die Notwendigkeit der unabhängigen Evaluation gezeigt, und es gibt jetzt ein europäisches Schema, ITSEC [EU91], nach dem nationale Einrichtungen für Computersicherheit (im Fall von Großbritannien CESG/GCHQ) kommerziellen Laboratorien die Lizenz erteilen, Sicherheitsprüfungen durchzuführen. Die unabhängige Evaluation ist auch eine Anforderung in anderen Ländern wie Australien [Aus95], Kanada [TCP93] und den USA [TCS85]. Da Schemata wie ITSEC eher für militärische Systeme ausgelegt sind und Evaluationen nach ihren Kriterien teuer sein können, führen manche Industrien ihre eigenen genehmigten Schemata durch. Zum Beispiel wird die Sicherheit von Einbruchs-Alarmanlagen von den Laboratorien der im Loss Prevention Council zusammengeschlossenen Versicherer überprüft. Gleichartige industrieweite Übereinkünfte könnten in einem angemessenen Zeitraum für klinische Systeme getroffen werden.

3.10 Klinische Akten oder Patientenakten?

Wie oben bemerkt wurde, spiegeln die meisten klinischen Informationssysteme die klinische Praxis wider, indem jedes Behandlungsteam ein Aufzeichnungssystem hat, und die Informationen fließen zwischen den Teams in Form von Zusammenfassungen (Überweisungsbriefe, Entlassungsberichte, Gutachten, Untersuchungsergebnisse usw.). Die ganze Akte kann zu einem anderen Team kopiert werden, wenn der Patient verlegt wird, aber sonst sind die Akten nicht Patienten-gestützt sondern vielmehr Klinikerin-gestützt, und zwischen den Klinikerinnen fließen nur Zusammenfassungen von Informationen.

Wie oben erwähnt hat es unlängst Interesse an einem anderen Modell gegeben, der "elektronischen Gesamt-Patientenakte" [unified electronic patient record], die alle klinischen Aufzeichnungen und Daten aus der gesamten Lebenszeit des Patienten ansammelt [MRI94]. Es ist aber kompliziert, eine Gesamt-Patientenakte sicher zu machen, und zwar aus einer Reihe von Gründen:

- wenn die Aufzeichnungen auf einer optischen Karte oder Diskette beim Patienten sind, wie kann der Verlust einer Karte wieder gutgemacht werden? Wenn aber die Aufzeichnungen (oder deren Sicherungskopien) auf einer zentralen Datenbank gehalten werden, wie würde dann die Aggregation kontrolliert?

- Aufzeichnungen von Geburten enthalten auch die persönlichen Gesundheitsinformationen der Mutter. Hierzu wird der Patient doch sicherlich keinen ungehinderten Zugang erhalten?

- wie würde man mit großen Dateien wie denen von Computertomographien und den Aufzeichnungen von langdauernden chronischen Erkrankungen umgehen?

- wie würde man Klinikerinnen den Zugang zu den Akten ehemaliger Patienten garantieren können, damit sie die von ihnen durchgeführte Behandlungen evaluieren und sich gegen Gerichtsverfahren schützen können?

- angenommen ich gehe in ein Krankenhaus und sage, daß meine Dämonen heute ganz besonders lästig sind. Wenn man mich nach meinem Namen fragt, antworte ich "John Major". Darf der Psychiater die Akte des Premierministers aufrufen und die Diagnose einer Schizophrenie anfügen? Mit anderen Worten, zwingt uns eine Patienten-gestützte Akte, die Identität von Patienten viel genauer zu überprüfen, und wenn ja, was sind davon die Implikationen für Notfallbehandlungen, für Patienten, die anonym behandelt werden wollen (wie vierzehnjährige Mädchen, die wegen postkoitaler Kontrazeption kommen), und in der Tat für die bürgerlichen Freiheiten?

- wenn ein Patient in einem Gefängnis eine Behandlung erhält, dann darf diese Tatsache, nachdem die Strafe unter den anzuwendenden Rehabilitationsregeln verbüßt worden ist, nicht mehr an einem anderen Ort aufgezeichnet werden. Also können realistischerweise medizinische Aufzeichnungen aus dem Gefängnis nirgendwo sonst gespeichert werden, und genausowenig geht das mit hochsensiblen Akten, bei denen der Zugang auf eine einzige Klinikerin beschränkt ist [s. dazu auch den Abschnitt über Speicherungen in der Haftanstalt des Münchener Polizeipräsidiums im 16. Tätigkeitsbericht des Bayerischen DSB (1994) - avh]. Was ist aber der Gewinn von einem zentralisierten System, wenn es trotzdem lokale Akten geben muß?

- eine lebenslange Akte würde wegen der wuchernden Verknüpfungen zwischen einzelnen Krankheitsepisoden das Zurückhalten von Daten durch die Patienten fördern, und sie würde sensible Aufzeichnungen (oder Markierungen, die ihre Abwesenheit kennzeichnen) für hunderte von Beschäftigten im Gesundheitswesen sichtbar machen, die irgendwann einmal während des Patientenlebens Zugang zur Akte bekämen. Wie könnten diese Verletzlichkeiten ohne teures manuelles Editieren kontrolliert werde?

Die obige Liste ist auf keinen Fall erschöpfend. Für eine Diskussion der Komplexitäten bei der Sicherheit von Patienten-gestützten Aufzeichnungssystemen siehe Griew und Currell [GC95]. Wie deren Arbeit verdeutlicht, würde uns die Verwendung von elektronischen Gesamt-Patientenakten zwingen, unserer Liste eine ganze Reihe von Prinzipien hinzuzufügen.

Es gibt auch Versuche mit Hybridsystemen. Anstatt alle Gesundheitsinformationen des Patienten in eine einzige Datei zu geben, könnte man eine zentrale Zusammenfassung haben, die Verweise auf detaillierte Dateien in den Systemen der Klinikerinnen enthält. Es gibt gegenwärtig mindestens zwei Krankenhäuser in Großbritannien, die Versuche mit Systemen machen, die auf diesem Modell basieren, wobei bei beiden offenbar alle Benutzer Zugang zu allen Akten haben; aber selbst wenn es eine geeignete Zugangskontrolle gäbe, könnte man fragen, was eigentlich an der traditionellen Akte bei der Hausärztin auszusetzen ist. Obwohl sie "Doktor-gestützt" ist, kommt sie einer lebenslangen Patientenakte am nächsten.
Auf jeden Fall liegt bei denen, die "Patienten-gestützte" Aufzeichnungssysteme vorschlagen, die Bürde, eine klare Aussage über die erwarteten Gesundheitsvorteile zu machen und zu analysieren, was die Bedrohungen, die Kosten zusätzlicher Gegenmaßnahmen und die wahrscheinlichen Effekte des Restrisikos sind.

4 Optionen für die Sicherheitsarchitektur

Die im vorangegangenen Abschnitt dargelegte Sicherheitspolitik bezieht sich auf Systeme im allgemeinen. Unser Ziel war, sie nicht mit den Details spezifischer Ausrüstungen zu belasten, sondern eine Sicherheitspolitik vorzulegen, die genausogut in einer zentralen Anlage mit einer Anzahl von Terminals verwirklicht werden kann wie in einem heterogen verteilten System, das aus einer Anzahl von Einzelsystemen besteht, die durch Kommunikationsprotokolle miteinander verknüpft sind - oder, wenn man will, sogar in Räumen voller Schreiber mit Federkielen.

Der Fall mit den heterogenen verteilten Einzelsystemen findet jedoch in Großbritannien am meisten Interesse, und in diesem Abschnitt betrachten wir einige technische Optionen, wie man ihn einrichten kann. Dieser Abschnitt will jedoch mehr andeuten als normativ sein; es ist Sache der einzelnen Hersteller von Ausrüstungen, ihre eigenen Systeme zu entwerfen und sie darauf überprüfen zu lassen, ob sie die Anforderungen der Sicherheitspolitik erfüllen. Alles, was diese Sicherheitspolitik fordert, kann mit kompetent eingesetzter Technologie erreicht werden. Die folgenden Anmerkungen können jedoch hilfreich sein, vor allem für Händler, die nicht mit modernen Techniken der Computersicherheit vertraut sind.

4.1 Compusec

[Abkürzung für Computer Security, Computersicherheit]

Compusec-Maßnahmen oder Maßnahmen zur Computersicherheit beinhalten die Zugangskontrollmaßnahmen, die in das Betriebssystem und die Anwendungssoftware eingebaut werden. Typischweise umfassen sie einen Authentfizierungsmechanismus wie Paßwörter, einen Zugangskontrollmechanismus, der entscheidet, welcher Benutzer Zugang zu welchem Objekt haben kann [which subject can access which object], und einen "Audit-Vermerk", der Auskunft darüber gibt, wer was gemacht hat. Ein Standardlehrbuch über Compusec ist Amoroso [Amo94].

Die Prinzipien unserer Politik beschreiben einigermaßen detailliert die funktionellen Anforderungen an den Zugangskontrollmechanismus. Was den Authentfizierungsmechanismus angeht, so wird dessen von uns geforderte Stärke davon abhängen, ob ein Zugang von außen möglich ist. Bei einem Netzwerk, das sich gänzlich innerhalb eines geschützten Raums befindet, werden Paßwörter genügen. Wenn ein System jedoch einen Einwähl- oder Internetzugang unterstützt, dann können die komplexeren Kontrollen erforderlich sein, die im nächsten Abschnitt diskutiert werden.

Das führt zu dem allgemeineren Problem, wo im System die Zugangskontrollen lokalisiert werden sollen. Es ist möglich, aber teuer, sie in jedes Anwendungsprogramm einzubauen; gewöhnlich werden sie auf einer niedrigeren Ebene im System billiger sein. Zugangskontrollisten werden von vielen Betriebssystemen unterstützt, wie beispielsweise von Unix, dessen Gruppen- und Einzelzulassungen dafür verwendet werden können, Akten allen Teammitgliedern beziehungsweise Einzelpersonen zugänglich zu machen. Wenn ein System verwendet wird, das Datenbanken verwaltet, dann kann es sein, daß man in der Datenbank Zugangskontrollen mit der Körnung der individuellen Patientenakten einbauen muß. Verwendet ein heterogenes verteiltes System Kryptographie als primäre Kontrolle, dann

könnte die Zugangskontrolle zum großen Teil in den Mechanismen zur Schlüsselverwaltung eingebettet sein.
Die automatische Erzwingung des siebten Prinzips (Information, die der Akte A entnommen wurde, darf an Akte B dann und nur dann angefügt werden, wenn die Zugangskontrolliste von B in der von A enthalten ist) ist sehr wichtig. Wenn ein Programm Daten von einer identifizierbaren klinischen Akte übernimmt, dann sollen die übernommenen Daten die gleiche Zugangskontrolliste haben wie die Originaldaten, oder eine Teilmenge von ihr. Eine Zusammenfassung einer Akte ist genauso sensibel wie das Original. Einer der Vorteile von diesem Mechanismus ist es, daß er sowohl versehentliche als auch absichtliche Sicherheitsverletzungen verhindern hilft. Zum Beispiel passiert es recht häufig, daß persönliche Mitteilungen versehentlich an eine elektronische Aussendungsliste oder Internet-Nachrichtengruppe [mailing list or newsgroup] geschickt werden. Das System sollte verhindern, daß einer Klinikerin auf diese Weise persönliche Gesundheitsinformationen entweichen.

Schließlich liegt es dort, wo Akten für Prüf- oder Forschungszwecke anonymisiert werden, in der Verantwortung der Klinikerin, sicherzustellen, daß der Anonymisierungsvorgang im betreffenden Kontext wirksam ist. Aus diesem Grund sollte es einer absichtlichen Handlung der Klinikerin bedürfen, um die Daten freizugegeben. Wie die Anleitung der Joint Computer Group klarmacht, ist es inakzeptabel, daß Aufzeichnungen zu einer Gesundheitsbehörde oder pharmazeutischen Firma gesandt werden auf das Versprechen hin, daß sie anonymisiert würden, wenn sie erst einmal dort sind.

4.2 Comsec

[Abkürzung für Communication Security, Kommunikationssicherheit]

Der Hauptzweck von Comsec-, oder Kommunikationssicherheits- Maßnahmen ist es, sicherzustellen, daß Zugangskontrollen nicht umgangen werden, wenn eine Akte von einem Computer zu einem anderen übertragen wird. Das kann zum Beispiel geschehen, wenn Daten als Klartext zu einem System übertragen werden, das deren Zugangskontrolliste verfälscht oder das nicht das Prinzip der informierten Zustimmung erzwingt. Es kann auch geschehen, wenn als Klartext versandte Daten durch das Anzapfen von Leitungen aufgefangen oder wenn klinische Informationen in einer Email-Nachricht versehentlich an eine Aussendungs- oder Nachrichtenliste [mailing list/newsgroup] geschickt werden.

In zweiter Linie liegt der Zweck von Comsec-Mechanismen darin, die Integrität von Daten beim Transit durch ein Netzwerk zu schützen. Manche Mitteilungen wie zum Beispiel Pathologieberichte sind lebenswichtig; und es gibt auch eine Kontroverse, ob elektronische Akten als Klartext für rechtliche Belange angemessen sind. Es ist daher bei vielen Anwendungen wünschenswert, daß zusätzlich die Integrität von Mitteilungen geprüft wird.

Klinikerinnen sollten nicht annehmen, daß einem Netzwerk vertraut werden kann, wenn es nicht unter deren direkter Kontrolle steht und vollständig von einem geschützten Raum umgeben ist, wie das bei einem lokalen Netzwerk (LAN, local area network) der Fall sein kann, das die Computer in einer Praxis verbindet. Weitverkehrsnetzen (WAN, wide area networks) wie dem Internet und dem NHS-weiten Netzwerk darf man nicht vertrauen. Erinnern wir uns daran, daß einem Netzwerk zu vertrauen gleichbedeutend damit ist, zu sagen, daß es die Systemsicherheit durchbrechen kann.

Vertrauliches Material von Patienten einer Systemkomponente auszusetzen, die nicht unter klinischer Kontrolle oder unter der effektiven Kontrolle einer vertrauenswürdiger Dritter [trustworthy third party] steht, ist in einem Maße unvernünftig, das daran grenzt, unethisch zu sein.

Ein geeignetes Mittel, um Informationen in einem Netzwerk zu schützen, wird durch die Kryptographie zur Verfügung gestellt. Moderne kryptographische Systeme gestatten es den Benutzern, getrennte Schlüssel zum Ver- und Entschlüsseln zu haben, und der Verschlüsselungs-Schlüssel kann veröffentlicht werden, während der Entschlüsselungs-Schlüssel geheimgehalten wird. Ebenso wird ein Benutzer getrennte Schlüssel zum Unterschreiben und für die Verifikation der Unterschrift haben; der Schlüssel für die Unterschrift wird geheimgehalten, während der Schlüssel zum Verifizieren der Unterschrift veröffentlicht wird, so daß jeder eine unterschriebene Nachricht verifizieren kann. Ein Standardlehrbuch über Kryptographie ist das von Schneier [Sch95].

Digitale Unterschriften gestatten die Schaffung von Vertrauensstrukturen. Zum Beispiel könnte der General Medical Council alle Ärzte zulassen, indem er deren Schlüssel unterzeichnet, und andere klinische Berufsausübende könnten in gleicher Weise von ihren eigenen Körperschaften beglaubigt werden. Das ist der Ansatz, den die französische Regierung bevorzugt [AD94]. Eine Alternative wäre es, von der Basis her ein Netz von Vertrauensstrukturen aufzubauen, indem die Benutzer gegenseitig ihre Schlüssel unterzeichnen. Wenn sich beide Ansätze auf halbem Wege träfen, könnte dazu die Zulassung der Schlüssel durch eine ranghöhere Klinikerin in jeder natürlich gewachsenen Gemeinschaft gehören.

Alle diese Optionen haben ihre Stärken und Schwächen und werden gegenwärtig diskutiert. Das stärkste Argument der Zentralisten ist anscheinend, daß man, selbst wenn die Zulassung im wesentlichen lokal geschähe, trotzdem einen zentralen Dienst für den Verkehr über Bereichsgrenzen (cross-domain traffic) hinweg braucht. Sie könnten auch argumentieren, daß dieser zentrale Dienst computerisiert sein sollte, denn wenn man nur einen "Fingerabdruck" des Schlüssels [key fingerprint - durch eine als unumkehrbar geltende "Hash-Funktion" verkürzte Fassung des öffentlichen Schlüssels einer Person, z.B. beim Programm PGP oder bei den Zertifikaten in neueren Browsern - rja] neben dem Namen jeder Klinikerin im betreffenden Berufsregister hätte, dann würde das die Klinikerinnen noch nicht in die Lage versetzen, Unterschriften auf mitgeschickten Datenobjekten zu verifizieren.

Eine einzige Zulassungsstelle wäre jedoch ein einziger Punkt, an dem das System versagen kann, und elektronische Vertrauensstrukturen sollten auch die tatsächlichen Vertrauens- und Machtverhältnisse im Anwendungsbereich widerspiegeln [Ros95]. In der Medizin ist die Macht hierarchisch verteilt, doch sie neigt dazu, örtlich und kollegial zu sein und nicht zentralisiert und bürokratisch. Wenn diese Wirklichkeit nicht respektiert wird, dann könnten die Bereiche von Verwaltung und Sicherheit sich voneinander entfremden, und man könnte zum Schluß ein Sicherheitssystem haben, das von den Klinikerinnen als zentrale Zumutung betrachtet wird und nicht als etwas Vertrauenswürdiges, das dem Berufsstand gehört und von ihm kontrolliert wird.
Die meisten veröffentlichten Standards für das Management und die Zertifizierung von Schlüsselsystemen beziehen sich auf das Bankwesen, doch klinische Systeme haben zusätzliche Erfordernisse; man könnte zum Beispiel eine Zählung der Gesamtanzahl der Patientenakten haben wollen, auf die eine Klinikerin außerhalb ihres Teams in einem bestimmten Zeitraum zugegriffen hat, und

das könnte gut durch den Beglaubigungsmechanismus erzwungen werden.
Jedenfalls kann, wenn jede Klinikerin erst einmal in geeigneter Weise beglaubigtes Schlüsselmaterial erhalten hat, die Integrität von Zugangskontrollisten und anderen Informationen in einem Netzwerk durch einen Satz von Regeln erzwungen werden, der aussehen könnte wie folgt:

1. Persönliche Gesundheitsinformationen dürfen ein klinisches System nicht verlassen, wenn sie nicht mit einem Schlüssel verschlüsselt wurden, von dem man vernünftigerweise annehmen kann, daß er einer Klinikerin gehört, die auf der Zugangskontrolliste dieser Informationen steht;

2. lebenswichtige Informationen, die durch ein Netzwerk übertragen wurden, sollten mit Vorsicht behandelt werden, wenn sie nicht mit einem Schlüssel unterschrieben worden sind, von dem man vernünftigerweise annehmen kann, daß er einer zuständigen Klinikerin gehört;

3. vernünftigerweise an den oben beschriebenen Kontext zu glauben bedeutet, daß der Besitz des Schlüssels durch persönlichen Kontakt, durch persönliches Bekanntmachen oder auf eine andere vertrauenswürdige Weise verbürgt worden ist;

4. entschlüsselte Informationen müssen in einem vertrauenswürdigen System gespeichert werden, das eine Zugangskontrolliste hat, die nur den Namen des Patienten enthält, den Namen der Klinikerin, deren Schlüssel die Informationen entschlüsselt hat, und gegebenenfalls den(die) Namen der Klinikerin(nen), die sie unterzeichnet hatte(n).

Sorgfältiger Überlegung bedürfen die Umstände, unter denen die Handlungen des Entschlüsselns und Unterschreibens ausgeführt werden. Wenn das System eine Unterschrift ohne Anwesenheit des Unterfertigten ausführen kann, dann kann es sein, daß die Unterschrift nicht rechtsverbindlich ist [Wri91]. Das stimmt mit dem Prinzip überein, daß Akten, wenn man über Bereichsgrenzen hinweg arbeitet, gegeben werden müssen und man sie sich nicht einfach holen kann; Zugangswünschen sollte nie automatisch stattgegeben werden, sondern sie müssen eine absichtliche Handlung einer Klinikerin erfordern.

Comsec-Techniken können in beschränkteren Anwendungen eingesetzt werden. Die mit diesem Dokument veröffentlichten Richtlinien [And96] behandeln sinnvolle Praktiken für den Schutz von Verbindungen zu Filialen einer Praxis durch Rückrufprozeduren. Ein anderes Beispiel könnte sein, daß eine Klinikerin einen tragbaren Computer zusammen mit einem Mobiltelefon benutzen möchte, um auf einem nächtlichen Hausbesuch Akten einzusehen. Manche Mobiltelefone (besonders solche, die GSM-Technik verwenden) bieten einen Grad von Sicherheit, der akzeptabel sein kann, während andere leicht abzuhören sind. Wenn ein unsicheres Medium verwendet wird, dann wäre es ratsam, die Daten durch Mechanismen auf der Anwendungsebene wie zum Beispiel Verschlüsselung zu schützen.

Verschlüsselung und Rückruf sind nicht die einzigen Comsec-Optionen. Eine andere ist, in den Anwendungen, in denen dies einfach geht, die Daten zu anonymisieren. Zum Beispiel könnte ein System, das Labordaten an Hausärzte liefert, den Patientennamen mit einer einmalig verwendeten Seriennummer ersetzen, die genügend Redundanz enthält, um versehentliche Verwechslungen unwahrscheinlich zu

machen. Dann könnten die Laborwerte im Klartext (mit geeigneten Integritätsprüfungen) übertragen werden.

Der allerwichtigste Faktor, um ein funktionierendes Sicherheitssystem zu erhalten, ist weniger die Wahl der Mechanismen als vielmehr die Sorgfalt, die auf die Gewährleistung von deren gutem Zusammenwirken beim Kontrollieren der tatsächlichen Bedrohungen verwendet wird.

4.3 Evaluation und Akkreditierung

Die Trusted Computing Base (vertrauenswürdige Einrichtung zur Datenverarbeitung) ist die Gesamtsumme aller Hardware-, Software- und prozeduralen Komponenten, die einzeln oder in Kombination die Sicherheitspolitik durchbrechen könnten. Ihre Gestaltung ist Sache der Systemhersteller, doch die Erfahrung zeigt: je kleiner sie ist, umso besser. Bei kleinen Sicherheitssystemen ist die Überprüfung billiger, und die Wahrscheinlichkeit des Auftretens von Softwarefehlern [bugs], welche die Sicherheit beeinträchtigen, ist geringer.

Prozedurale Mechanismen wie die Paßwortverwaltung, das Konfigurations-Management und die Erstellung von Sicherungskopien sind ein integraler Bestandteil, und wenn ein System untersucht wird, muß der Prüfer die Frage stellen, ob es wahrscheinlich ist, daß es sicher von einer Klinikerin bedient werden kann, deren Computerfertigkeiten und Ordnungsliebe in Verwaltungsdingen unterdurchschnittlich sind. Es gibt faule und nachlässige Klinikerinnen und Kliniker, so daß eine positive Beurteilung nicht ausgefertigt werden darf, wenn es bequemer ist, das System unsicher zu betreiben. Prüfer sollten auch die Dinge berücksichtigen, die vom menschlichen Design abhängen, wie die Qualität der Handbücher und der Schulungen sowie das Durchführen von Integritätschecks bei der manuellen Dateneingabe.

Die Evaluationsebene sollte davon abhängen, was welchen möglichen Gefährdungen ausgesetzt ist. Wir schlagen ITSEC-Ebene E2 vor bei bis zu 50.000 Patientenakten und E4 für 50.000 bis 1.000.000 Patientenakten. Systeme, die persönliche Gesundheitsinformationen von bedeutend mehr als 1.000.000 Personen enthalten, sollten nicht gebaut werden.

Wenn ein System von einem Käufer installiert wird, müssen zuletzt die verantwortlichen Klinikerinnen sicherstellen, daß alle relevanten Einschulungen abgeschlossen wurden und daß jegliche notwendigen Pläne, Prozeduren und Materialien - von einem Desaster-Wiederherstellungsplan über Informationsbroschüren bis zu Patienten-Einwilligungsformularen - bereitgestellt und getestet worden sind, bevor identifizierbare klinische Patienteninformationen in das System eingegeben werden. Die Entscheidung, Informationen auf diese Weise Gefährdungen auszusetzen, sollte eine bewußte ärztliche Entscheidung sein, das Restrisiko zu akzeptieren, und sie sollte schriftlich von den verantwortlichen Klinikerinnen dokumentiert werden. Erst wenn diese Anerkennung [accreditation exercise - in Analogie zur Anerkennung eines neuen militärischen Kommunikationssystems durch den verantwortlichen General - rja] abgeschlossen ist, soll ein System mit dem Schlüsselmaterial ausgestattet werden, das zur Kommunikation mit anderen Systemen erforderlich ist.

4.4 Europäische und globale Standardisierung

Die Sicherheitspolitik und die Richtlinien, die in diesem Dokument umrissenen sind, stimmen, soweit dies dem Autor bekannt ist, weitgehend mit der Arbeit an Europäischen und anderen Standards überein. Wir haben erfahren, daß eine Europäische Standardisierungsgruppe für Sicherheit und Privatheit von Medizinischer Informatik (CEN TC 251/WG6) an einem Entwurf arbeitet, der die Verschlüsselung von persönlichen Gesundheitsinformationen in großen Netzwerken vorschreibt; Verschlüsselung wird von den Datenschutzbehörden in Schweden seit einigen Jahren verlangt, und eine Reihe von Ländern baut vertrauenswürdige Zertifizierungsstellen auf, welche die Schlüssel der Beschäftigten in Gesundheitsberufen beglaubigen werden.

Die Verwendung von digitalen Unterschriften wird auch in einem Bericht an das Gesundheitsministerium von Ontario diskutiert [Smu94]. Verwiesen werden kann auch auf den australischen Standard für Privatheit von Gesundheitsinformationen [Aus95], den Interimistischen Code des Königlichen Australischen Kollegs der Allgemeinmediziner für den Umgang mit computerisierten medizinischen Aufzeichnungen in der Allgemeinpraxis [RAC+93], den Neuseeländischen Privatheits-Code für Gesundheitsinformationen [NZ94] und den Bericht des Amtes der Vereinigten Staaten für Technikfolgenabschätzung [OTA93]. Sie alle leisten auf unterschiedliche Weise einen Beitrag zu unserem Verständnis der Bedrohungen, des Prinzips der Einwilligung, der technischen Optionen und der pragmatischen Standards für die beste Praxis in anderen Ländern.

Auch die Hersteller und Lieferanten werden ermutigt, sich die beste europäische Praxis zu eigen zu machen, was sehr wichtig sein kann, wenn das europäische Datenschutzrecht erst einmal in britischen Gerichten durchgesetzt wird. Dies wird, egal was sonst die Folgen sein werden, die Betonung der Patientenzustimmung verstärken.

5 Schlußfolgerungen

Wir haben die Bedrohungen für die Vertraulichkeit, Integrität und Verfügbarkeit von persönlichen Gesundheitsinformationen im Licht der Erfahrungen in Großbritannien und in Übersee beschrieben und eine Sicherheitspolitik für klinische Informationen vorgelegt, die es ermöglicht, das Prinzip der Patientenzustimmung in der Art von heterogenem verteiltem System durchzusetzen, das gegenwärtig in Großbritannien gebaut wird.

Klinikerinnen, die Einkaufsentscheidungen treffen, werden ermutigt, Systeme zu bevorzugen, bei denen die Übereinstimmung mit dieser Sicherheitspolitik geprüft wurde. Wo noch kein geprüftes System erhältlich ist, sollten Käuferinnen berücksichtigen, in welchem Ausmaß zur Verfügung stehende Produkte die hier vertretenen Prinzipien unterstützen und ob der Hersteller es auf sich nehmen wird, einen Weg der Nachrüstungen [an upgrade path] hin zu einem geprüften System zu gehen.

Wo keines der verfügbaren Produkte einen akzeptablen Grad von Computer- und Kommunikationssicherheit gewährt, gibt die britische Ärztevereinigung (British Medical Association) ihren Mitgliedern zu bedenken, daß dem NHS-weiten Netzwerk (oder in der Tat jedem anderen unsicheren Netzwerk) klinische Informationen auszusetzen, mit denen die Identifizierung von Patienten möglich ist, oder sogar verschlüsselte klinische Informationen an ein nicht vertrauenswürdiges System zu senden, in einer Weise unvernünftig ist, die daran grenzt, unethisch zu sein.

Danksagungen

Beim Verfassen dieses Dokuments kamen wertvolle Beiträge von einer Reihe von im Gesundheitswesen Beschäftigten, darunter Fleur Fisher, Tony Griew, Simon Jenkins, Grant Kelly, Stuart Horner, Hilary Curtis, Simon Fradd, John Williams, Iain Anderson, William Anderson, Roger Sewell, Mary Hawking, Ian Purves, Paul Steventon, Steve Hajioff, Stan Shepherd, Jeremy Wright und David Watts; von einer Reihe von Computerwissenschaftlern, unter ihnen Stewart Lee, Roger Needham, Mark Lomas, Bruce Christianson, Ian Jackson, Mike Roe, Jeremy Thorp, Roy Dainty und Ian Keith; und von Philosophen, darunter Beverly Woodward, Ann Somerville and Keith Tayler.

6 Literatur

[Ald95] "Nurse sacked for altering records after baby's death", K Alderson, The Times 29 November 95 p 6

[Amo94] Fundamentals of Computer Security Technology, E Amoroso, Prentice Hall 1994

[And96] "Clinical System Security --- Interim Guidelines", RJ Anderson, in British Medical Journal v 312 no 7023 (13th January 1996) pp 109--111

[Aus95] `Australian Standard 4400: Personal privacy protection in health care information systems', Standards Australia, 1995

[AC95a] `Setting the Records Straight --- A Study of Hospital Medical Records', Audit Commission, June 1995

[AC95b] `For Your Information --- A Study of Information Management and Systems in the Acute Hospital', Audit Commission,, July 1995

[ACH95] `Keeping Information Confidential', Association of Community Health Councils for England and Wales, May 1995

[AD94] "Security of Health Information Systems in France: what we do will no longer be different from what we tell", FA Albert, L Duserre, International Journal of Biomedical Computing v 35 (supplement, 1994) pp 201--204

[AIS95] `AIS --- Advanced Information System', FHS Computer Unit, 1995

[Boy94] `Draft guidance for the NHS on the confidentiality, use and disclosure of personal health information', N Boyd, Department of Health, 10 August 1994

[Bru95] "Is your health history anyone's business?" McCall's Magazine 4/95 p 54, reported by M Bruce on Usenet newsgroup comp.society.privacy, 22 Mar 1995

[BMA95] `A Bill Governing Collection, Use and Disclosure of Personal Health Information', British Medical Association 1995

[Cae95] WJ Caelli, personal communication, July 1995

[CR94] "Who's reading your medical records?" Consumer Reports, Oct 94 pp 628--632 [zur elektronischen Version von S. 629 des Artikels]

[DGMW94 `How to Keep a Clinical Confidence', B Darley, A Griew, K MsLoughlin, J Williams, HMSO 1994

[DL95] Data Logic product information at http://www.datlog.co.uk/

[DPA84] `Data Protection Act', HMSO 1984

[DPR95] `Identity Cards: A Consultation Document CM2879 --- Response of the Data Protection Registrar', October 1995

[EU91] `Information Technology Security Evaluation Criteria', EU document COM(90) 314 (June 1991)

[EU95] `On the protection of individuals with regard to the processing of personal data and on the free movement of such data (final)', Directive of the European Parliament and the Council, adopted by the Council on 24 July 1995

[Gil95] "MDU Muddle re Death Pills", C Gilbert, gp-uk mailing list, 23rd October 1995

[GC95] `A Strategy for Security of the Electronic Patient Record', A Griew, R Currell, Institute for Health Informatics, University of Wales, Aberystwyth, 14th March 1995

[GMC1] `Good medical practice', General Medical Council, 178--202 Great Portland Street, London W1N 6JE

[GMC2] `Confidentiality', General Medical Council, 178--202 Great Portland Street, London W1N 6JE

[GTP93] "Privacy and Security of Personal Information in a New Health Care System", LO Gostin, J Turek-Brezina, M Powers et al., Journal of the American Medical Association v 20 (24/11/93) pp 2487--2493

[Haw95] "Confidentiality of personal information: a patient survey", A Hawker, Journal of Informatics in Primary Care, 1995 (March) pp 16--19

[HRM93] "RMs need to safeguard computerised patient records to protect hospitals", Hospital Risk Management 1993 v 9 (September) pp 129--140

[JCG88] "GMSC and RCGP guidelines for the extraction and use of data from general practitioner computer systems by organisations external to the practice", Appendix III in `Committee on Standards of Data Extraction from General Practice Guidelines' Joint Computer Group of the GMSC and RCGP, 1988

[JHC94] "Nurse Jailed for Hacking into Computerised Prescription System", British Journal of Healthcare Computing and Information Management v 1 (94) p 7

[LB94] "Your Secrets for Sale", N Luck, J Burns, The Daily Express, 16/2/94 pp 32--33

[MRI94] "Integrated Health Delivery Needs Integrated Health Record Systems", Medical Records Institute newsletter v 3 no 5 (December 94) pp 1--9

[Mac94] Letter from AW Macara to JS Metters, 31 October 1994, on `Draft guidance for the NHS on the confidentiality, use and disclosure of personal health information'

[Mar95] "Fear of Flowing", DC Markwell, Proceedings of the 1995 Annual Conference of The Primary Health Care Specialist Group of the British Computer Society, pp 36--42

[NHS92] `Handling confidential patient information in contracting: A Code of Practice', NHS Information Management Group EL(92)60, catalogue number 2009(c), news info 132

[NHS95] `The Handbook of Information Security --- Information Security within General Practice', NHS Executive Information Management Group E5209 (May 1995)

[NZ94] `Health Information Privacy Code 1994', New Zealand Privacy Commissioner, 1994/1/1

[OTA93] `Protecting Privacy in Computerized Medical Information', Office of Technology Assessment, US

Government Printing Office, 1993

[PK95] "GP Practice computer security survey", RA Pitchford, S Kay, Journal of Informatics in Primary Care, September 95, pp 6--12

[Ros95] "Institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrastrukturen", A Rossnagel, Datenschutz und Datensicherheit (5/95) pp 259--269

[RAC+93] `Interim Code of Practice for Computerised Medical Records in General Practice', Royal Australian College of General Practitioners, February 93

[RFA93] `Requirements for accreditation, general medical practice computer systems', NHS management executive 1993

[RL95] "For Sale: your secret medical records for 150 pounds", L Rogers, D Leppard, Sunday Times 26/11/95 pp 1--2

[RSM92] `Computers in Medical Audit', second edition, M Rigby, A McBride, C Shields, Royal Society of Medicine, London, 1992

[Sch95] `Applied Cryptography', B Schneier, second edition, Wiley 1995

[See95] "Marketing use of medical DB", M Seecof, Usenet newsgroup comp.risks 17.12

[Smu94] `Health Care Information: Access and Protection', RH Smuckler, Institute for Primary Care Informatics, 1994

[Som93] `Medical Ethics Today --- Its Practice and Philosophy', A Sommerville, BMA 1993

[Tho95] "Sex Stalker Plays Doctor to Trick Victims", M Thomas, PA newswire no 1236, 7/7/95

[TCP+93 `The Canadian trusted Computer Product Evaluation Criteria', Communications Security Establishment, Government of Canada, January 1993

[TCS+85] `Trusted Computer System Evaluation Criteria', US Department of Defense document 5200.28-STD, December 1985

[USA95] "Online medical records raise privacy fears", USA Today, 22/3/95 pp 1A--2A

[Woo95] "The computer-based patient record and confidentiality", B Woodward, New England Journal of Medicine v 333 no 21 (95) pp 1419--1422

[Wri91] `The Law of Electronic Commerce: EDI, Fax and Email', B Wright, Little, Brown (fourth edition with supplement) 1994

[WHC95] `Workshop on Health Care --- Confidentiality: discussing current initiatives', held at the BMA on 4th April 1995; transcript supplied by RH Pyne

Ende des Dokuments