Protokoll
der 2. Sitzung der GMDS-Projektgruppe
Datenschutz in Krankenhausinformationssystemen
am 15. und 16. März 1994 in Mainz

Die Sitzung fand im Sitzungsraum (Raum 103) des Instituts für Medizinische Statistik und Dokumentation der Johannes-Gutenberg-Universität Mainz statt.

15.3.1994, 14.00 - 18.30 Uhr: Workshop Sicherheitstechniken

Anwesend:

- Dr. B. Blobel (Magdeburg)
- M. Böttcher (Mainz)
- S. Brings (Troisdorf)
- Dr. K.-H. Elsässer (Heidelberg)
- V. Hamm (Mainz)
- Dr. M. Hortmann (Bremen)
- Dr. A. Krtschil (Mainz)
- V. Lieder (Dresden)
- M. Miller (Mainz)
- Prof. Dr. K. Pommerening (Mainz)
- K. Scheffel (Lübeck)
- Dr. K.-H. Schicketanz (Mainz)
- J. Schüz (Mainz)
- W. Schweikert (Mainz)
- W. Thoben (Oldenburg)
- G. Wetter (Mainz)
- H. Zengerling (Mainz)
- Dr. I. Zöllner (Mainz)

Vorträge:

- K. Pommerening: *Kryptografische Verschlüsselungsverfahren -- Einsatzmöglichkeiten und Bewertung*
- M. Hortmann: *Einsatz kryptographischer Chipkarten in Krankenhausinformationssystemen*
- K. Pommerening: *Kryptografische Protokolle für offene Systeme (z. B. elektronische Post)*
- M. Miller: *Datenschutzmaßnahmen für das Krebsregister Rheinland-Pfalz*
- W. Thoben: *Datenschutzmaßnahmen für das Krebsregister Niedersachsen*
- H. Zengerling: *Das Firewall-Konzept und seine Realisierung bei der Universitätsverwaltung Mainz*
- M. Hortmann: *Ein Sicherheitsmodell für Computersysteme in der Intensivmedizin (Eine Entwicklung im EG-AIM Projekt TANIT)*
- B. Blobel: *Probleme und Realisierungsvarianten des Datenschutzes in offenen medizinischen Informationssystemen -- Darstellung am Beispiel eines in ein KIS integrierten überregionalen Tumorregisters*

Herr Blobel demonstriert anschließend die kryptografisch gesicherte Verbindung zum Tumorregister Magdeburg/Sachsen-Anhalt.

Unterlagen zu den Vorträgen werden ausgeteilt.

15.3.1994, 9.15 -- 13.00 Uhr: Sitzung der Projektgruppe

Anwesend:

- Dr. B. Blobel (Magdeburg)
- S. Brings (Troisdorf)
- Dr. K.-H. Elsässer (Heidelberg)
- Dr. M. Hortmann (Bremen)
- V. Lieder (Dresden)
- M. Miller (Mainz)
- Prof. Dr. K. Pommerening (Mainz)
- K. Scheffel (Lübeck)
- Dr. K.-H. Schicketanz (Mainz)

Tagesordnung:

- 1. Berichte
- 2. Vorschläge zur Vernetzung der Projektgruppe
- 3. Workshop "Datenschutz in Krankenhausinformationssystemen" (November 1994 in Magdeburg)
- 4. Grundsatzerklärung
- 5. Europäische Richtlinien für den Datenschutz
- 6. Auswirkungen des GSG
- 7. Zugriffsrechte im KIS, Definition von Schutzstufen
- 8. Verschiedenes

TOP 1. Berichte

a) Die Teilnehmer stellen sich kurz vor. Herr Pommerening teilt mit, dass noch weitere Interessenten vorhanden sind, die aber aus Termingründen nicht teilnehmen konnten.

b) Als Tagesordnungspunkt 3 wird eingeschoben "Workshop Datenschutz in Krankenhausinformationssystemen (November 1994 in Magdeburg)"

c) Herr Schicketanz berichtet von einem Treffen des Bundesverbandes der Datenschutzbeauftragten in Ulm. Ein wesentliches Thema waren die Europäischen Richtlinien für den Datenschutz (s. TOP 5). Es wurde übereinstimmend festgestellt, dass der Datenschutz bereichsspezifisch zu gestalten ist; unter anderem besteht eine Arbeitsgruppe für Datenschutz in der Medizin. Die Projektgruppe sieht die Zusammenarbeit mit den Datenschutzbeauftragten für wesentlich an und bittet Herrn Schicketanz, den Kontakt mit der genannten Arbeitsgruppe aufrecht zu erhalten.

d) Herr Pommerening berichtet von der Fachkonferenz "Sicherheit in der Informations- und Kommunikationstechnik" (24./25.1.1994 in München). Es gibt eine Reihe von Firmen, die

brauchbare Sicherheitstechnik anbieten, aber auch immer noch einige, deren Produkte Sicherheit nur vortäuschen. Das IT-Sicherheitshandbuch des BSI wurde von Beratungsfirmen, die es versuchsweise angewendet haben, als unpraktikabel bezeichnet. Die Produktübersicht des BSI enthält inzwischen eine ganze Reihe zertifizierter Produkte, allerdings überwiegend auf ziemlich niedriger Sicherheitsstufe; Kryptoverfahren werden dort nicht benannt.

e) Am 15./16. September 1994 findet in Bonn ein Interdisziplinäres Forum "Vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung" statt, organisiert von TeleTrusT. Herr Pommerening hat seinen Wunsch zur Teilnahme angemeldet; auch Herr Blobel soll als Interessent genannt werden.

f) Für die GMDS-Jahrestagung wurde, entgegen der ursprünglichen Absicht, von Herrn Pommerening aus Zeitgründen kein Tutorium angemeldet. Herr Hortmann beabsichtigt, ein Tutorium über Chipkarten nachzumelden, sofern das noch möglich ist.

g) Herr Pommerening weist auf das *Datenschutzkonzept für UNIX-Mehrplatzanlagen* des Hamburger Datenschutzbeauftragten hin. Der Text wird auf Disketten verteilt.

TOP 2. Vorschläge zur Vernetzung der Projektgruppe

Bisher sind nicht alle Teilnehmer der Projektgruppe über elektronische Post erreichbar. Herr Hortmann bietet zu diesem Zweck die Einrichtung einer Mailbox in Bremen an. Näheres wird noch mitgeteilt. Es soll versucht werden, bei allen Beteiligten die Software PGP zu installieren, die gestattet, elektronische Post zu unterschreiben und zu verschlüsseln. Das ist ein erster Schritt, um konkrete Erfahrungen mit dem Einsatz kryptografischer Sicherheitstechnik zu sammeln. Weitere organisatorische Details werden auf der nächsten Sitzung behandelt.

Um die Verfügbarkeit von Dokumenten zu verbessern, wird Herr Pommerening in Mainz eine FTP-Server für die Projektgruppe installieren. Auch hierzu werden die Einzelheiten noch mitgeteilt.

TOP 3. Workshop "Datenschutz in Krankenhausinformationssystemen"

Herr Blobel bereitet einen internationalen Workshop "Datenschutz in Krankenhausinformationssystemen" vor, der am 2. und 3. November 1994 in Magdeburg stattfinden soll. Es sollen Experten aus Politik, Wirtschaft, Verwaltung und Wissenschaft teilnehmen. Herr Blobel stellt das Konzept vor (Tischvorlage wird ausgeteilt).

Die Projektgruppe begrüßt die Bemühungen von Herrn Blobel und unterstützt das Konzept. Zusätzlich zum vorgeschlagenen Teilnehmerkreis soll auch der Bundesbeauftragte für den Datenschutz und der Bundesverband der Datenschutzbeauftragten berücksichtigt werden; Herr Schicketanz erklärt sich bereit, den Kontakt herzustellen.

TOP 4. Grundsatzerklärung

Der Entwurf liegt in der Fassung vom 15. März 1994 vor. In einem Schreiben von Herrn Haux als Sprecher des Fachausschusses Medizinische Informatik der GI und GMDS wird folgendes weitere Vorgehen vorgeschlagen: Nach Verabschiedung in der Projektgruppe sollte die Erklärung den Abteilungsleitern für Medizinische Informatik zur Abstimmung zugeschickt werden, danach sollte ein Beschluss im Präsidium der GMDS herbeigeführt

werden. Abschließend wird der Abdruck im Mitteilungsblatt oder der GMDS-Schriftenreihe empfohlen.

Die inhaltliche Diskussion ergibt einige Verbesserungsvorschläge:

In Absatz 1 wird der Satz "Der Datenschutz muss bereichsspezifisch, insbesondere medizinspezifisch gestaltet werden" eingefügt. Der Satz "Die Vertraulichkeit des Arzt-Patienten-Verhältnisses ... " ist redundant und wird gestrichen. Die Reihenfolge "Arzt und Patient" wird umgekehrt.

Die Absätze 2 und 3 werden zusammengefasst. In dem Satz "Die Entscheidung über den Zugriff ... " wird das Wort Zugriff durch eine allgemeiner verständliche Formulierung ersetzt. Die Formulierung "am Ort ihrer Entstehung oder überwiegenden Verwendung" wird ersetzt durch "unter Verantwortung der erhebenden Stelle". Statt "es gilt das `need to know'-Prinzip" wird formuliert "nur die erforderlichen Teilinformationen aus der Krankenakte sollen dabei offenbart werden". Über die Frage der Vernichtung von Krankenakten kann aufgrund der widersprüchlichen Rechtslage keine Empfehlung gegeben werden. Hier sieht die Projektgruppe noch einen Handlungsbedarf von Seiten des Gesetzgebers.

Im Absatz 4 wird das Wort "bestmöglich" gestrichen, da es zum formulierten Prinzip der Verhältnismäßigkeit nicht passt.

Im Absatz 6 werden die beiden ersten Sätze ersetzt durch: "Die Sicherheitsmaßnahmen sollen die Aufmerksamkeit des Arztes nicht vom Patienten ablenken. Zwar sind Datenschutz-maßnahmen ohne Mitwirkung der Beteiligten nicht zu verwirklichen, aber die Belastung durch organisatorische und technische Verfahren ist zu minimieren."

In Absatz 6 werden Hinweise auf die nötige Infrastruktur, den Sicherheitsverantwortlichen und den Datenschutzbeauftragten eingefügt.

In Absatz 7, Satz 3, werden die Begriffe "Datenschutzinhalte und -ziele" eingefügt.

Im letzten Absatz wird der erste Satz ersetzt durch "Die Notwendigkeit, aber auch die Möglichkeit, funktionsfähige Sicherheitskonzepte zu entwickeln, ist gegeben". Der Passus "weitere Lippenbekenntnisse zum Datenschutz abzugeben" wird gestrichen.

Nach entsprechender Überarbeitung wird die Grundsatzerklärung in der aktuellen Version dem Protokoll beigelegt (und als ASCII-Version auf dem in Mainz einzurichtenden FTP-Server bereitgestellt). Werden innerhalb eines Monats keine wesentlichen Änderungs-vorschläge mehr gemacht, gilt das Dokument dann als verabschiedet und wird dem Fachausschuss Medizinische Informatik und dem GMDS-Präsidium zur weiteren Diskussion zugeleitet. Diesem Vorgehen wird einhellig zugestimmt.

TOP 5. Europäische Richtlinien für den Datenschutz

Die Kommission der Europäischen Gemeinschaften hat einen geänderten Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vorgelegt. Herr Schicketanz berichtet über den Inhalt dieses Vorschlags. Eine Zusammenfassung wird als Kopie verteilt. Viele der geplanten Vorschriften stimmen mit der bisherigen deutschen Gesetzgebung nicht überein. Als Besonderheiten werden hervorgehoben:

- Die Unterscheidung zwischen öffentlichem und nichtöffentlichem Bereich entfällt.
- Das Amt des Datenschutzbeauftragten ist nicht vorgesehen.
- Der Sozialbereich gehört nicht zu den sensiblen Daten.
- Bestimmte Daten, darunter auch Daten über Gesundheit und Sexualleben, dürfen grundsätzlich nicht verarbeitet werden, außer unter besonderen Voraussetzungen.
- Das Auskunftsrecht ist sehr umfassend.
- Eine grundsätzliche Meldepflicht der Verarbeitung wird eingeführt.

TOP 6. Auswirkungen des GSG

Herr Schicketanz berichtet über die Auswirkungen des GSG. Es bringt eine Ausweitung der Verdatung auf gesetzlicher Grundlage mit sich, insbesondere durch die EDV-gestützte Abrechnung zwischen Kosten- und Leistungsträgern, und enthält umfassende Ermächtigungen zur Verarbeitung von Patientendaten. Der "gläserne Patient" und der "gläserne Arzt" werden Wirklichkeit.

Die Projektgruppe sieht diese Entwicklung mit großer Besorgnis. Eine verfassungsrechtliche Überprüfung wäre dringend notwendig; das Recht auf informationelle Selbstbestimmung wird weitgehend außer Kraft gesetzt. Insbesondere die Datenübermittlung an Dritte beeinträchtigt das Vertrauensverhältnis zwischen Patient und Arzt empfindlich. Die Bemühungen der Projektgruppe um Datenschutz im Krankenhaus erscheinen vor diesem Hintergrund fast als gegenstandslos.

Herr Blobel erklärt sich bereit, auf der nächsten Sitzung detailliert über die geplanten Datenweitergaben zu berichten.

TOP 7. Zugriffsrechte im KIS, Definition von Schutzstufen

Es liegen verschiedene Musterdefinitionen vor:

- Die Definition von Schutzstufen im *Katalog der technischen und organisatorischen Maßnahmen zum Datenschutz* des staatlichen Koordinierungsausschusses Datenverarbeitung (Bayern).
- Die Zugriffsmatrix für krankenhausbetriebliche Leistungsstellen aus dem Buch *Informationssysteme und Datenschutz im Krankenhaus* von H.-J. Seelos.
- Die Definitionen von Daten, Gruppen und Rollen sowie Zugriffsrechten aus den *Interim Technical Recommendations for Data Protection in CC Computer Systems* aus dem AIM-Projekt TANIT von Herrn Hortmann.

Herr Pommerening erarbeitet daraus rechtzeitig vor der nächsten Sitzung einen Entwurf für ein Musterkonzept.

TOP 8. Verschiedenes

a) Der ursprünglich ebenfalls vorgesehene Tagesordnungspunkt " Sicherheitstechnik für KIS (Erarbeitung von Empfehlungen)" wird auf der nächsten Sitzung behandelt. Für die Erarbeitung von Empfehlungen ist es jetzt noch zu früh.

b) Als Termin für die nächste Sitzung der Projektgruppe wird der 3./4. November (im Anschluss an den Workshop) in Magdeburg geplant.

Protokoll: (Prof. Dr. K. Pommerening)