Protokoll
der 5. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Krankenhausinformationssystemen
am 7. und 8. Dezember 1995 in Hildesheim

Die Sitzung fand im Hotel Bürgermeisterkapelle in Hildesheim statt.
Anwesend:

- G. Bleumer (Hildesheim)
- Dr. B. Blobel (Magdeburg)
- Dr. M. Hortmann (Bremen)
- Prof. Dr. K. Pommerening (Mainz)
- M. Schnabel (München)
- M. Schunter (Hildesheim)
- W. Thoben (Oldenburg)

Entschuldigt:

- Dr. K.-H. Elsässer (Heidelberg)
- V. Lieder (Dresden)
- Dr. J. Paczkowski (Troisdorf)
- Dr. H. Ruelius (Göttingen)
- Prof. Dr. K. Sauter (Kiel)

Tagesordnung:
1. Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Die EU-Datenschutz-Richtlinie
5. Firewall-Konzept der Universitätsklinik Mainz
6. Ziele und weiteres Vorgehen der Arbeitsgruppe
7. Pseudonyme Abrechnung im Gesundheitswesen
8. Musterkonzept für ein sicheres KIS
9. Verschiedenes

Der Vorsitzende begrüßt die Teilnehmer und dankt den Herren Bleumer und Schunter für die Organisation der Sitzung. Er verteilt eine aktualisierte Adressenliste der Mitglieder.

TOP 1. Festlegung der Tagesordnung

Die mit der Einladung verschickte Tagesordnung wird zunächst angenommen. Später wird einvernehmlich der Punkt "Ziele und weiteres Vorgehen der Arbeitsgruppe" aufgenommen.

TOP 2. Protokoll der vorigen Sitzung

Das Protokoll der 4. Sitzung der Arbeitsgruppe wird in der vorliegenden Form angenommen.

TOP 3. Mitteilungen und Berichte

a) Herr Pommerening und Herr Hortmann weisen auf neue Internet-Ressourcen hin, insbesondere sind aktuelle Berichte von der Konferenz der Datenschutzbeauftragten und der Text der EU-Datenschutzrichtlinie im WWW zu finden. Zeiger findet man in der Ressourcen-Liste der Arbeitsgruppe:

- http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz/Ressourcen.html

b) Der Konferenzband von dem Workshop in Magdeburg ist inzwischen erschienen:

- Bernd Blobel (Hrsg.): Datenschutz in medizinischen Informationssystemen. DuD-Fachbeiträge Band 23, Vieweg, Braunschweig/Wiesbaden 1995, ISBN 3-528-05517-0.

c) Die GMDS hat eine Arbeitsgruppe "Krankenhausinformationssysteme" gegründet, die als Dachorganisation aller dieses Gebiet tangierenden Arbeitsgruppen dienen soll; Sinn ist die Koordination und Kooperation dieser Arbeitsgruppen, auch in Bezug auf Öffentlichkeitsarbeit. Bezüglich der bestehenden Gruppen gilt das Subsidiaritätsprinzip, jedoch sollen aus diesen Gruppen regelmäßig Berichte eingeholt werden. Unsere Arbeitsgruppe ist durch die Herren Blobel und Pommerening vertreten. Geplant wird ein Symposium "Erfahrungsberichte zu Krankenhausinformationssystemen", das jährlich im Mai in Göttingen stattfinden soll.

d) Die Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF) hat eine Kommission "Medizinisches Forschungsgeheimnis" gegründet. Ziel ist die Erleichterung medizinischer Forschung durch freien Zugriff auf personenbezogene medizinische Daten aller Art aus allen Quellen (auch von Krankenkassen und Sozialleistungsträgern). Als Ausgleich soll das ärztliche Berufsgeheimnis durch ein Forschungsgeheimnis ergänzt werden im Sinne eines gesetzlichen Geheimnisschutzes für personenbezogene medizinische Forschungsdaten. Herr Pommerening ist in diese Kommission berufen worden; die GMDS wird dort außerdem durch Herrn Rienhoff vertreten.

Als Ergebnis der Diskussion ergibt sich einvernehmlich als Standpunkt der Arbeitsgruppe:

- Es darf keine Datensammlung ohne vorherige Zweckbestimmung geben. Zweckungebundenes spontanes Forschen ist weder zulässig noch sinnvoll.
- Es darf keine Weitergabe personenbezogener Daten ohne Einwilligung des Betroffenen geben, auch nicht an medizinische Forscher.
- Ein eventuell nötiger Datenabgleich zur Zusammenführung von Fällen ist nach Möglichkeit mit Hilfe von Pseudonymen durchzuführen. Klartextdaten werden dazu in der Regel nicht benötigt.
- Nach den EU-Richtlinien gilt das Arztgeheimnis für alle, die personenbezogene medizinische Daten zur Kenntnis bekommen. Ein speziell zu formulierendes Forschungsgeheimnis ist damit gegenstandlos.
- Eine weitere Aufweichung des Datenschutzes ist nicht hinnehmbar. Die bestehenden gesetzlichen Grundlagen sind ausreichend, um sinnvoll epidemiologische und klinische Studien durchführen zu können.

Herr Blobel weist in diesem Zusammenhang darauf hin, dass sich das Gesundheitssystem zur Zeit sehr schnell in Richtung "Shared Care" entwickelt: Ein Fall wird von verschiedenen Instanzen behandelt, die zugehörigen Daten entsprechend mitgeteilt; in Zukunft wird es die

über mehrere Organisationen verteilte Krankenakte geben. Die Zweckbindung der Daten an den Behandlungsfall muss hierbei strikt eingehalten werden. Die hiermit zusammenhängenden Probleme sollten auch in der Arbeitsgruppe behandelt werden, so dass ihr Name in "Datensicherheit im Gesundheitswesen" geändert werden sollte.

e) Auf der GMDS-Jahrestagung in Bochum trug Herr Blobel über "Modellierung und Realisierung sicherer offener medizinischer Informationssysteme", Herr Pommerening über "Pseudonyme - ein Kompromiss zwischen Anonymisierung und Personenbezug" vor.

f) Herr Pommerening und Herr Blobel veranstalteten am 29.11.95 in der Akademie für Medizinische Informatik in Heidelberg ein eintägiges Seminar über "Datenschutz in verteilten und offenen Systemen".

g) Die Herren Hortman und Schunter nahmen an der Trust-Center-Tagung am 27. und 28.9.1995 in Siegen teil. Herr Hortmann weist auf einen Vortrag von Pfitzmann über mehrseitig sichere Schlüsselerzeugung hin.

h) An der IMIA WG 4 Security Working Conference "Communicating Health Information" in Helsinki vom 30. September bis 3. Oktober nahmen die Herren Blobel und Bleumer teil. Herr Bleumer trug über die Kosten der kryptographischen Infrastruktur im Medizinbereich vor; der Artikel ist im WWW unter

- http://www.informatik.uni-hildesheim.de/~sirene/BiBl95.ps.gz

zu finden (ab Januar). Herr Blobel stellte ein Poster über Modellierung und Design von sicheren offenen Informationssystemen aus. Als Fazit der Veranstaltung stellt er dar: Die technischen Voraussetzungen zur Verwirklichung von sicheren Systemen sind vorhanden. Als überfällig gefordert wird ein ethischer Codex für die Verarbeitung von Daten. Ein großes Defizit wird im Bereich der Sensibilisierung und der Weiterbildung der Anwender gesehen.

i) Auf der Jahrestagung der DGkDK (Deutsche Gesellschaft für klinische Datenverarbeitung und Kommunikation) am 25./26.11.95 in Kreischa bei Dresden hat Herr Blobel einen Vortrag gehalten.

j) Die Herren Bleumer und Blobel haben an der MEDINFO in Vancouver teilgenommen und vorgetragen. Sie berichten von großem Interesse an den Sitzungen, die Sicherheitsfragen zum Thema hatten.

k) Herr Hortmann berichtet über eine Lösung zur Einbindung von PGP in WWW-Browser. Genaueres wird noch bekannt gegeben.

l) Die Herren Hortmann und Blobel berichten, daß die Spitzenverbände der Krankenkassen, die Bundesärztekammer, die kassenärztliche Bundesvereinigung und die Krankenhausgesellschaft im Rahmen der Ausführungsbestimmungen für die Datenübermittlung den Einsatz von asymmetrischen Chiffrierverfahren vorgesehen haben. Die Firma Debis ist bundesweit mit der Erarbeitung des Konzepts beauftragt worden.

TOP 4. Die EU-Datenschutz-Richtlinie

Herr Blobel verteilt Kopien einer Arbeit von Louveaux und Poullet "The European Legal framework for data protection and privacy". Herr Pommerening weist noch einmal auf die online-Verfügbarkeit der Richtlinie hin (siehe TOP 1). Herr Blobel erläutert wesentliche Punkte mit Hilfe einiger Folien. Änderungen gibt es bei der Zweckbindung und der Weiterverarbeitung. Neu sind Regelungen zur Datenqualität. Der Begriff des Dateneigentums wird dagegen überhaupt nicht verwendet. Der Patient als Quelle der Daten ist "Datensubjekt", der Arzt als "Datenurheber" genießt ein Urheberrecht an den Daten. Insbesondere ist das Konzept der Patientenakte im Eigentum des Patienten, etwa auf einer Karte, damit nicht zu vereinbaren.

Die EU-Richtlinie muss adäquat in deutsches Recht abgebildet werden, ist aber bisher nicht rechtlich verbindlich. Die Arbeitsgruppe kommt überein, sich, soweit Spielraum besteht, an der EU-Richtlinie zu orientieren, da diese zukunftsweisend ist.

TOP 5. Firewall-Konzept der Universitätsklinik Mainz

Herr Pommerening weist auf das neue Buch

- D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls O'Reilly, 1995, ISBN 1-56592-124-0.

hin, das eine sehr detaillierte und praxisnahe Anleitung gibt. Es ist in der Ressourcen-Liste der Arbeitsgruppe aufgeführt. Dort gibt es auch eine kleine Marktübersicht mit Anbieter-Adressen und Pointer auf Firewall-Informationen im WWW.

Herr Pommerening erläutert einige grundsätzliche Aspekte der Planung des Firewall-Systems der Mainzer Klinik.

- Interaktive Dienste (telnet, ftp, Zugriff auf News-, WWW- und Medline-Server) sollen nur von der Klinik in die Außenwelt möglich sein, nicht umgekehrt. Ausnahmen können zugelassen werden, unterliegen dann aber einer strengen Überwachung.
- Email soll in beiden Richtungen unbeschränkt möglich sein.
- Erlaubt ist nur das TCP/IP-Protokoll; andere Protokolle (z. B. Novell-IPX) werden gesperrt.
- Dienste, die nur im lokalen Netz benötigt werden und gefährliche Sicherheitslücken haben, werden gesperrt. (Beispiele: tftp, finger, NFS, NIS, X).
- Modem- und ISDN-Strecken, die den Firewall umgehen, sind verboten.
- Redundanz in den Sicherheitsmaßnahmen ist erwünscht.

Die dem Stand der Technik entsprechende Konfiguration ist "Außennetz <-> Router <-> Gateway-Rechner <-> Router <-> Innennetz". Der Gateway wird auf einem Intel-Rechner unter Linux mit dem frei verfügbaren TIS-fwtk (Firewall Toolkit) realisiert. Dieses Vorgehen ist möglich, wenn genügend gute Unix-Kenntnisse vorhanden sind; andernfalls ist der Einsatz eines kommerziellen Firewall-Systems vorzuziehen. Die Hauptarbeit steckt aber in der Konfiguration, so daß die Arbeitseinsparung durch ein kommerzielles System eher gering ist. Besonders kompliziert ist die Einrichtung geeigneter Nameserver.

TOP 6. Ziele und weiteres Vorgehen der Arbeitsgruppe

Dieser Punkt wird auf Vorschlag von Herrn Bleumer kurzfristig in die Tagesordnung aufgenommen. Als Aufgabengebiete der Arbeitsgruppe werden genannt:

- Datenschutz in Gesundheitspolitik und Recht,
- Organisation, Struktur, Integration von Datenschutz und Datensicherheit,
- systematische, akademische Darstellung der Probleme und Lösungsvorschläge,
- technische und technologische Umsetzung.

Ziele der Arbeitsgruppe in diesen Gebieten sind:

- Datensicherheitsempfehlungen für das Gesundheitswesen,
- Modellprojekte,
- Konzepte für Beratung, Ausbildung, Schulung,
- Richtlinien für die Anwendung im laufenden Betrieb.

Dabei sind natürlich nach Möglichkeit die in SEISMED geleisteten Vorarbeiten zu berücksichtigen. Ansprechpartner sind:

- Verantwortliche für Datenverarbeitung im Gesundheitswesen, Politiker, Krankenhaus-Manager,
- die GMDS als wissenschaftliche Fachgesellschaft,
- Software-Hersteller und Entwicklungsgruppen.

Eigentliches Ziel ist die Umsetzung von Datenschutz- und Sicherheitsmaßnahmen in der Praxis der Anwendung. Es bestehen aber noch Defizite bei der Einsicht der Verantwortlichen in die Notwendigkeiten. Der bisherige Ansatz, zunächst ein umfassendes Konzept zu erstellen, wird daher in der Priorität etwas zurückgestellt; stattdessen sollen geeignete Teile so schnell wie möglich den geeigneten Ansprechpartnern vermittelt werden. Herr Blobel wird den "politischen" Teil, der an die erste Gruppe ("Verantwortliche") gerichtet ist, nach Möglichkeit noch in diesem Jahr ausarbeiten und nach Abstimmung mit der Arbeitsgruppe in geeigneten Zeitschriften publizieren. Da in Sachsen-Anhalt ein Pilotprojekt zur kassenärztlichen Abrechnung ansteht, werden die Herren Bleumer und Schunter analog mit dem Vorschlag zur pseudonymen Abrechnung (s. TOP 7) verfahren, möglichst bis Januar.

Dieser Plan für das weitere Vorgehen wird einstimmig angenommen. Es soll versucht werden, auch Vertreter von Systemherstellern zur Mitarbeit in der Arbeitsgruppe zu gewinnen.

TOP 7. Pseudonyme Abrechnung im Gesundheitswesen

Der überarbeitete Entwurf "Datenschutzorientierte Abrechnung medizinischer Leistungen" wurde den teilnehmenden Arbeitsgruppenmitgliedern von Herrn Bleumer bereits Anfang der Woche zugesandt. Herr Bleumer stellt ihn vor. In der Diskussion werden folgende Anregungen oder Änderungsvorschläge vorgebracht:

- Transaktionspseudonyme für den Patienten (einmal verwendbar) bieten durch ihre Unverkettbarkeit optimalen Datenschutz. Ob die Krankenkassen für statistische Zwecke die Verkettbarkeit benötigen, ist noch zu klären; in diesem Fall wären Personenpseudonyme als Kompromiss einzuführen. Das Konzept soll aber zunächst Transaktionspseudonyme vorsehen.

- Die Übertragbarkeit und Mehrfachverwendbarkeit der Pseudonyme ist durch geeignete technische oder kryptografische Vorkehrungen zu verhindern.
- Die kassenärztliche Vereinigung vertritt die niedergelassenen Ärzte gegenüber den Kassen und hat das Vertrauen der Ärzte. Sie wäre also insbesondere geeignet, um die bei Missbrauchsverdacht nötige Aufdeckung eines Pseudonyms vorzunehmen. Ein eventueller Regress bei Budget-Überschreitung könnte ebenfalls über die KV ablaufen, ohne die Identität des Arztes der Krankenkasse zu offenbaren.
- Da in der dritten Stufe der Gesundheitsreform die Budget-Überwachung vorgesehen ist, sind für die Ärzte Personenpseudonyme nötig, die aber quartalsweise gewechselt werden könnten. Die Aufdeckung muss für ein Jahr gesichert sein.
- Krankenhäuser treten den Kassen gegenüber als Einheit auf, so dass für die dort angestellten Ärzte ein Gruppenpseudonym sinnvoll wäre.

TOP 8. Musterkonzept für ein sicheres KIS

Es wird nach dem Beschluss unter TOP 6 verfahren. Herr Blobel wird das entsprechend ausgearbeitete Manuskript per Email verschicken.

TOP 9. Verschiedenes

Das nächste Treffen der Arbeitsgruppe soll am 25. und 26. April 1996 in München stattfinden.

Protokoll: (Prof. Dr. K. Pommerening, M. Schunter, 14.12.95)

email: Pommerening@imsd.uni-mainz.de