Protokoll
der 7. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Krankenhausinformationssystemen
am 5. und 6. Dezember 1996 in München

Die Sitzung fand im Besprechungsraum des Instituts für Medizinische Statistik und Epidemiologie der Technischen Universität München (Klinikum rechts der Isar) statt.

Anwesend:

- Dr. B. Blobel (Magdeburg)
- C. Höfler (Erlangen)
- Dr. M. Hortmann (Bremen)
- Dr. H. Lautenbacher (Tübingen)
- H. Leitgeb (Salzburg)
- Prof. Dr. K. Pommerening (Mainz)
- M. Schnabel (München)
- Frau Spiridonov (München) als Gast

Entschuldigt:

- G. Bleumer (Hildesheim)
- P. Messerer (Ludwigshafen)
- Dr. J. Paczkowski (Troisdorf)
- M. Pöll (Innsbruck)
- Prof. Dr. K. Sauter (Kiel)
- Dr. K.-H. Schicketanz (Mainz)
- M. Schunter (Hildesheim)
- M. Schurer (Tübingen)
- W. Thoben (Oldenburg)
- Dr. B. Wentz (Erlangen)

Tagesordnung:

1. Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. SEISMED-Guidelines und internationale Richtlinien
5. Anleitung für das Management
6. Benutzung von PGP im WWW
7. Sicherheitskonzepte im Klinikum rechts der Isar
8. Pseudonyme Abrechnung im Gesundheitswesen
9. Programm für die KIS 97
10. Weiteres Vorgehen der Arbeitsgruppe
11. Verschiedenes

Der Vorsitzende begrüßt die Teilnehmer und dankt Herrn Schnabel für die Organisation der Sitzung.

TOP 1. Festlegung der Tagesordnung

Die mit der Einladung verschickte Tagesordnung wird angenommen.

TOP 2. Protokoll der vorigen Sitzung

Das Protokoll der 6. Sitzung der Arbeitsgruppe wird in der vorliegenden Form angenommen.

TOP 3. Mitteilungen und Berichte

a) Herr Pommerening weist auf einige neue Internet-Ressourcen hin, die auch über die WWW-Seite der AG erreichbar sind:

- Stellungnahmen und Empfehlungen der Landesdatenschutzbeauftragten
- Dokument zur CORBA-Sicherheit (308 Seiten, Postscript-Format) der OMG
- Computerviren in Original-Software
- Internet und Recht (The German Cyberlaw Project)
- BvD (Berufsverband der Datenschutzbeauftragen Deutschlands e.V.)
- DVD (Deutsche Vereinigung für Datenschutz e.V.)
- Das Österreichische Datenschutzgesetz (mit Kommentar)
- Die Snake-Oil-FAQ (Encryption Software to Avoid)
- Skript Arbeitnehmerdatenschutz

b) Herr Pommerening berichtet von neuen Angriffsmethoden auf Chipkarten, die die bisher angenommene Sicherheit dieser Geräte als illusorisch entlarvt haben: die »Differential Fault Attack« von Biham und Shamir sowie direkte physische Angriffe von Kuhn und Anderson.

c) Herr Blobel berichtet aus der HL7-Arbeitsgruppe Datensicherheit, für die die Hauptarbeit in Magdeburg geleistet wird. Es sind Lösungen analog zu EDIFACT/X.12 vorgesehen (Einbau einer Sicherheitskomponente in die Messages mit Authentisierung, Verschlüsselung und elektronischer Unterschrift). Bisher gibt es diese Komponenten in keiner Implementierung, d. h., HL7-Kommunikation ist offen lesbar. Ergebnisse werden bis Ende 1997 erwartet.

d) Herr Blobel berichtet über das HPC-Projekt. Im Teilprojekt Quasi-Niere sollen im Januar 25000 Patientenkarten ausgegeben werden, deren Zusammenarbeit mit der HPC bis Mitte 97 sichergestellt werden soll. Im Teilprojekt GISI ist die Implementierung wegen technischer Probleme bei der Integration mit MUMPS in Frage gestellt. In Magdeburg ist die Integration in die (Oracle-basierte) Anwendung gelöst; erste HPCs werden noch in diesem Jahr ausgegeben, die Funktionsfähigkeit soll Ende Februar 97 erreicht sein. Bis Mitte 1998 sollen ca. 1000 Karten ausgegeben sein. Vom Magdeburger Teilprojekt wird auch der Einsatz bei »Bayern online« mitbetreut.

e) Herr Blobel ist zum Leiter der CORBAmed Security Group ernannt worden.

f) Herr Pommerening stellt das von Herrn Schicketanz als Datenschutzbeauftragtem entwickelte »Konzept für die organisatorische Gliederung der Institution des Datenschutzbeauftragten im Universitätsklinikum Mainz« vor. In Magdeburg hat jede Struktureinheit einen eigenen Datenschutzbeauftragten (mit geringem Arbeitszeitanteil); in München ist die Situation ähnlich.

g) Tagungen und Vorträge:

- Sommerakademie LfD Schleswig-Holstein 26.8.96 in Kiel - Herr Hortmann nahm an einer Podiumsdiskussion über »Verschlüsselung von Daten in der Verwaltung« teil.
- Auf der MIE 96 trug Herr Blobel über »A regional clinical cancer documentation system ...« vor.
- Auf der GMDS 96, 15.-19.9.96 in Bonn trug Herr Blobel über »Unterstützung des `Shared Care' durch verteilte sichere Informationssysteme und Telematikanwendungen« vor. Herr Blobel und Herr Pommerening leiteten die Sitzung »Sicherheit und Datenschutz in Netzwerken«.
- Auf dem HL7-Workshop der GI 23.9.96 in Klagenfurt trug Herr Blobel über »Datensicherheitsaspekte beim standardisierten Datenaustausch im Gesundheitswesen« vor.
- GMDS-AG »Archivierung von Krankenunterlagen« 7.-8.11.96 in Berlin - Herr Pommerening trug über »Datenschutz und -sicherheit in elektronischen Dokumentenmanagement- und Archivierungssystemen« vor.
- BVMI-Arbeitstagung Telemedizin 15.-16.11.96 in Berlin - Herr Pommerening trug über »Datenschutz und Datensicherheit in öffentlichen Netzen im Gesundheitswesen« vor.
- Toward an Electronic Health Record Europe '96, 14.-17.11.96 London - Herr Blobel trug über »An object-oriented security approach involving HL7 and CORBAmed standards« vor.

h) Künftige Veranstaltungen:

- AG Krankenhausökonomie, Köln 23.1.97 - Vortrag Pommerening »Datensicherheit im Krankenhaus«.
- KIS 97, Heidelberg, 10.-11.4.97 - siehe TOP 9.
- 5. Deutscher IT-Sicherheitskongreß, BSI, Bonn 28.-30.4.97.
- APIS Jahrestagung 1997, Lübeck 5.-7.5.97 - Vortrag Pommerening »Sicherheitsaspekte in vernetzten Systemen«.
- MIE 97, Porto Carras 25.-29.5.1997 - Vortrag Blobel über CORBA.
- 42. Jahrestagung der GMDS, Ulm 15.-18.8.97
- Seminar »Datenschutz in der Medizin« der Akademie MI, Heidelberg 14.11.97, geleitet von Frau Wellbrock und Herrn Pommerening. (Ein in diesem Jahr geplantes Seminar mit Herrn Reimer und Frau Hahne-Reulecke fiel mangels Beteiligung aus.)

TOP 4. SEISMED-Guidelines und internationale Richtlinien

Die SEISMED-Guidelines liegen in Form von drei Bänden vor:

- Management Guidelines,
- Technical Guidelines,
- User Guidelines,

die in großen Teilen identisch sind, wobei die Technical Guidelines die vollständigste Version darstellen. Die Einführung und die Anleitung zu den kryptographischen Mechanismen wurden von Herrn Bleumer geschrieben. Die Guidelines enthalten eine Anleitung in 13 Stufen zur Erstellung eines Sicherheitskonzepts; dieses wird durch das Software-Werkzeug SIDERO unterstützt. Eine Anpassung an die deutschen Verhältnisse wäre wünschenswert und könnte

Aufgabe der AG sein. Der Abschnitt über Netzwerk-Sicherheit ist sehr knapp geraten; laut Herrn Blobel ist eine Neufassung im Rahmen des ISHTAR-Projekts in Vorbereitung.

TOP 5. Anleitung für das Management

Der Artikel der Autoren Blobel und Pommerening wird unter dem Titel »Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens« in der Zeitschrift »führen und wirtschaften im Krankenhaus« Anfang 1997 erscheinen.

TOP 6. Benutzung von PGP im WWW

Herr Hortmann stellt ein Netscape plug-in vor, das gestattet, PGP-verschlüsselte WWW-Seiten zu lesen. Da die Verwendung vorläufig nur unter UNIX möglich ist, wird das Thema zurückgestellt. Die Arbeitsgruppe bleibt bis auf weiteres bei der Version 2.3a von PGP, da diese außerhalb der USA programmiert wurde und deshalb auch im Behördenbereich problemlos verwendet werden kann. PGP-Frontends gibt es laut Herrn Hortmann u. a. für Pegasus, Eudora und Z-Mail.

TOP 7. Sicherheitskonzepte im Klinikum rechts der Isar

Frau Spiridonov von der Netzgruppe des Klinikums rechts der Isar stellt das Sicherheitskonzept und konkrete Maßnahmen vor. Angesprochen werden u. a. die Probleme: Trennung von Kliniknetz und Wissenschaftsnetz, externe Verbindungen, Fernwartung, Datenschutzverantwortung in den Fachabteilungen, Kosten und Nutzen organisatorisches Maßnahmen, räumliche Sicherheit, Chipkarten-Anwendungen.

TOP 8. Pseudonyme Abrechnung im Gesundheitswesen

Der Artikel »Datenschutzorientierte Abrechnung medizinischer Leistungen« der Autoren Bleumer und Schunter soll in DuD Heft 2/97 erscheinen.

TOP 9. Programm für die KIS 97

Geplant sind für diese Tagung zwei Hauptvorträge zum Thema »Datenschutz und Datensicherheit« sowie ein 2-stündiger Workshop.

TOP 10. Weiteres Vorgehen der Arbeitsgruppe

Als Aufgaben für die nächste Zeit werden genannt:

- Sammlung von Datenschutzkonzepten, Verpflichtungserklärungen und Betriebsvereinbarungen verschiedener Institutionen und Verarbeitung zu Musterdokumenten. Dabei ist auch an den nicht-universitären Bereich und an die Patienten-Information zu denken.
- Erstellung von Leitlinien und Checklisten; Grundlage dafür sollten die SEISMED Guidelines sein.
- Empfehlungen und Checklisten zu verschiedenen Einzelfragen, z. B. zum Umgang mit Standard-Software. Hier könnte die Form einer FAQ-Liste (»Frequently Asked Questions« wie im Usenet üblich) sinnvoll sein.

- Schulungsunterlagen und eigene Schulungsaktivitäten. Dabei sollte nach Zielgruppen unterschieden werden, z. B. Datenschutzbeauftragte, System-/Netzadministratoren, Mediziner, ...

TOP 11. Verschiedenes

a) Herr Leitgeb weist auf die Loseblattsammlung »Praxishandbuch für den betrieblichen Datenschutzbeauftragten« von H. Abel, WEKA-Fachverlag Augsburg, ISBN 3-8111-8090-8, hin.

b) Das nächste Treffen soll am 12. und 13. Mai 1997 in Magdeburg stattfinden.

Protokoll: Prof. Dr. K. Pommerening, 22.4.1997, letzte Änderung: 5.5.1997

E-Mail: Pommerening@imsd.uni-mainz.de