Protokoll
der 9. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Gesundheitsinformationssystemen
am 19./20. Februar 1998 in Mainz

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

Sitzungszeit: Donnerstag, 19.2.1998, 14.00 bis 18.00 Uhr,
Freitag, 20.2.1998, 9.00 bis 12.00 Uhr.

Anwesend: H. Baumann (Erlangen)
Dr. B. Blobel (Magdeburg)
Dr. B. Hornung (Marburg)
Dr. Z. Kardasiadou (Hannover)
Prof. Dr. K. Pommerening (Mainz)
Dr. E. Scheidt (Mainz)
M. Sergl (Mainz)
J. Walther (Krefeld)

Entschuldigt: Dr. T. Berger (Krefeld)
J. Erdmann (Berlin)
Dr. M. Hortmann (Bremen)
Dr. R. Killmann (Erlangen)
Dr. J. Paczkowski (Troisdorf)
Dr. H. Ruelius (Göttingen)
Prof. Dr. K. Sauter (Kiel)
M. Schnabel (München)
Dr. K.-H. Schicketanz (Mainz)
S. Wolf (Kiel)

Tagesordnung:
1. Begrüßung und Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Bericht über EU- und Chipkartenprojekte
5. Aktuelle Fragen zu Datenschutz und Datensicherheit
6. Sicherheitskonzepte für Kliniken
7. Leitlinien
8. KIS 98
9. Verschiedenes

TOP 1. Begrüßung und Festlegung der Tagesordnung

Der Vorsitzende begrüßt die Teilnehmer und verteilt die aktuelle Mitglieder-Adressenliste. Da neue Teilnehmer anwesend sind, stellen sich die Teilnehmer kurz vor. Die Tagesordnung wird in der mit der Einladung verschickten Form angenommen.

TOP 2. Protokoll der vorigen Sitzung

Das Protokoll der 8. Sitzung wird in der vorliegenden Form angenommen. Das Signaturgesetz wurde inzwischen verabschiedet. Signaturgesetz und Signaturverordnung sind im WWW zu finden. Der Vorsitzende weist darauf hin, dass die digitale Signatur (elektronische Unterschrift) auch der Qualitätssicherung medizinischer Informationen dient.

TOP 3. Mitteilungen und Berichte

a) Herr Pommerening berichtet von der GMDS-Beiratssitzung am 14.9.1997. Der Name der AG wurde, wie beantragt, in »Datenschutz in Gesundheitsinformationssystemen« umgewandelt. Bei der Abstimmung gab es eine Gegenstimme und 7 Enthaltungen mit der Begründung, der Name sei missverständlich. Neuer Schriftleiter der Zeitschrift »Informatik, Biometrie und Epidemiologie in Medizin und Biologie« (offizielles Organ der GMDS, »Silberfisch«) ist M. Löffler aus Leipzig. Die GMDS-Jahrestagungen 1999 und 2000 sollen in Heidelberg bzw. Hannover stattfinden.

b) AG-Mitglieder nahmen unter anderem an folgenden Veranstaltungen teil:

- 6. Wiesbadener Forum Datenschutz am 9. 6. 1997 beim Hessischen Datenschutzbeauftragten (Hortmann, Pommerening). Thema war: »Datenschutz durch Kryptographie - ein Sicherheitsrisiko«?
- MIE 97. Herr Blobel trug über »Security of Healthcare Information Systems Based on the CORBA Middleware« vor. Es gab unter anderem einen Workshop über Datensicherheit mit den Schwerpunkten Karten, Trusted Third Party Services, Architektur von Krankenhausinformationssystemen.
- Health Cards 97 in Amsterdam. Herr Blobel trug über »Security Infrastructure of an Oncological Network Using Health Professional Cards« vor.
- AK Karten im Gesundheitswesen, 17. 7. 1997 in Hannover (Blobel, Hornung, Pommerening). Herr Blobel trug über den Stand der praktischen Umsetzung in Magdeburg vor.
- GMDS 97. Herr Blobel und Herr Pommerening leiteten die Sitzung »Datenschutz in Krankenhausinformationssystemen«. Herr Hornung trug über »Neue Herausforderungen und Chancen für den Datenschutz im Krankenhaus durch globale IT-Entwicklungen«, Herr Krohn über »Validierung der SEISMED Risk Analysis« vor.
- New Technologies in Hospital Information Systems in Ulm. Herr Blobel war Mitveranstalter und trug über »Security Threats and Solutions in Distributed, Interoperable Health Information Systems Using Middleware« vor.
- Toward An Electronic Patient Record '97. Herr Blobel trug über »An Object-Oriented Security Approach Involving HL7, CORBA, & DHE Standards« vor.
- Toward An Electronic Health Record Europe 97, 20.-23. Oktober 1997, London. Herr Blobel trug über »Experiences with Health Professional Cards and Trusted Third Party Services Providing Security in Distributed Electronic Records in Oncology« vor.
- Herr Pommerening war als Sachverständiger zum Workshop »Telemedizin - Datensicherheit und Datenschutz« der Enquete-Kommission »Zukunft der Medien in Wirtschaft und Gesellschaft« des Deutschen Bundestages eingeladen. Seine Stellungnahme ist im WWW zu finden.

Außerdem nahm Herr Blobel an verschiedenen Project-Board-Meetings internationaler Projekte, der IMIA Working Conference on Data Security sowie CEN- und OMG-Arbeitsgruppen teil.

c) Neue Veröffentlichungen aus der AG:

- B. Blobel: Threats and Solutions for Data Protection and Data Security in Health Care Information Systems. Toward An Electronic Patient Record (1997), Volume 5, Issue 8, pp. 1-16.
- B. Blobel: Bedrohungen und Lösungen für Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens. IT-Sicherheit, Heft 3/97, 2-8.
- B. Blobel, P. Pharow: EUROMED, ISHTAR, HANSA und MEDSEC - Europäische Health-Telematics-Projekte. DuD 21/10 (1997), 598-599.
- B. Blobel: An Object-Oriented Security Approach Involving HL7, CORBA, & DHE Standards. In: C. P. Waegemann (Edr.): Proceedings »Toward An Electronic Patient Record '97«, Volume Two, pp. 54-66. Medical Record Institute, Newton 1997.
- B. Blobel, M. Holena: Security of Healthcare Information Systems Based on the CORBA Middleware. In: C. Pappas, N. Maglaveras, J.-R. Scherrer (Edrs.): Medical Informatics Europe 97, pp. 10-14. IOS Press, Amsterdam, Washington, Tokyo 1997.
- B. Blobel: Security Requirements and Solutions in Distributed Electronic Health Records. In: L. Yngström and J. Carlsen (Edrs.): Information Security in Research and Business, pp. 377-390. Chapman & Hall, London 1997.
- B. Blobel, M. Holena: Security Threats and Solutions in Distributed, Interoperable Health Information Systems Using Middleware. In: J. Dudeck, B. Blobel, W. Lordieck, T. Bürkle (Edrs.): New Technologies in Hospital Information Systems, pp. 66-73. Series in Health Technology and Informatics Vol. 45. IOS Press, Amsterdam 1997.
- B. Blobel, P. Pharow: Experiences with Health Professional Cards and Trusted Third Party Services Providing Security in Distributed Electronic Records in Oncology. Proceedings of the Conference »Toward An Electronic Health Record Europe 97«, pp. 29-39. London 20-23 October 1997.
- B. Blobel, P. Pharow: Security Infrastructure of an Oncological Network Using Health Professional Cards. In: L. van den Broek, A. J. Sikkel (Edrs.): Health Cards 97. Series in Health Technology and Informatics Vol. 49, pp. 323-334. IOS Press, Amsterdam 1997.
- M. Hortmann: Kryptoregulierung weltweit - Überblick. DuD 21/4 (1997), 214-215.
- R. Krohn, B. Blobel: Validierung der SEISMED Risk Analysis. In: R. Muche, G. Büchele, D. Harder, W. Gauss (Hrsg): Medizinische Informatik, Biometrie und Epidemiologie GMDS 97, S. 177-180. MMV Medizin Verlag München 1997.
- K. Pommerening: Datenschutzmaßnahmen in medizinischen Informationssystemen. Zentralblatt für Gynäkologie 119 (1997), 452-456.
- K. Pommerening, B. Blobel: Datenschutz und Datensicherheit in öffentlichen Netzen im Gesundheitswesen. Forum der Medizin-Informatik 1 (1997), 10-13.

Herr Pommerening berichtet, dass sein Buch »Datenschutz und Datensicherheit« inzwischen beim Verlag vergriffen ist. Einige letzte Restexemplare können an Interessenten kostenfrei abgegeben werden.

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

- Die Gesundheitsdatenschutzseite von Andreas von Heydtwolff (Salzburg), die u. a. eine deutsche Übersetzung der BMA-Guidelines (Anderson-Modell) sowie neben deutschen auch schweizerische und österreichische Datenschutz-Informationen anbietet.
- Das BSI, das unter anderem den Tagungsband des 5. IT-Sicherheitskongress 1997, das IT-Grundschutz-Handbuch und Sicherheitsleitlinien, z. B. für Web-Server, anbietet. Auch vom BSI akkreditierte Zertifizierungsstellen (z. B. TÜVIT Essen) sind im WWW zu finden.
- Das NIST mit u. a. einem Konzept für rollenbasierte Rechtevergabe (RBAC) im Krankenhaus und Inzidenz-Reports.
- EU-Healthcare-Telematik-Programm, siehe auch European Health Telematics Observatory.
- CORBAmed-Dokumente.
- Das Projekt »Rechtstatsachenforschung im Bereich der Computerkriminalität« (Universität Bonn).
- Die DGkDK (Deutsche Gesellschaft für klinische Datenverarbeitung) mit Vorträgen über Datenschutz in der Medizin, u. a. vom sächsischen Datenschutzbeauftragten.
- Der Referentenentwurf zum BDSG.
- Einige aktuelle Tätigkeitsberichte von Landesdatenschutzbeauftragten.
- Das Roland-Berger-Gutachten »Telematik im Gesundheitswesen«. Die AG diskutiert über Sinn und Kosten solcher Gutachten.

TOP 4. Bericht über EU- und Chipkartenprojekte

Herr Blobel berichtet über den Stand der EU-Projekte, an denen das Institut für Biometrie und Informatik der Universität Magdeburg beteiligt ist. In Magdeburg werden zurzeit die TTP-Services praktisch erprobt: Schlüsselgenerierung, Kartenausgabe, Zertifikate und Registrierung von öffentlichen Schlüsseln. Es werden Chipkarten von G&D mit STARCOS PK 1.0 verwendet. Notfallzugriffe sind auch ohne Karte möglich. Schlüssel-Sicherungskopien werden für Verschlüsselungs- und Archivierungsschlüssel hinterlegt, nicht für Signaturschlüssel.

Herr Baumann berichtet über ein Chipkartenprojekt der Firma Siemens. Ziel ist, die Intranet-Sicherheit zu verbessern. Es wird die PC/SC-Schnittstelle verwendet, die neben Siemens auch von Microsoft und IBM unterstützt wird und die Unabhängigkeit vom verwendeten Chipkarten-Leser unterstützen soll. Private Schlüssel sollen die Chipkarte nicht verlassen. Untersucht wird auch, welche Probleme beim Umgang mit Chipkarten auftreten können.

TOP 5. Aktuelle Fragen zu Datenschutz und Datensicherheit

Herr Pommerening trägt über Sicherheitsprobleme in Windows NT vor. Die Arbeitsgruppe stimmt darin überein, dass die Sicherheit dieses Betriebssystems viele gravierende Mängel hat und dass die suggerierte Leichtigkeit der Administration irreführend ist. Die Arbeitsgruppe empfiehlt, aus Sicherheitsgründen Unix-Server zu verwenden; für diese ist die sichere Konfiguration zwar auch mit viel Aufwand verbunden, aber doch einfacher, und verleitet weniger zur Nachlässigkeit.

Herr Pommerening legt einen Entwurf für »Sicherheitsempfehlungen zu Windows-NT-Netzen im Krankenhaus« vor. Diese werden nach leichten redaktionellen Änderungen von der AG einhellig gutgeheißen. Sie werden im WWW veröffentlicht und über die Startseite der AG zugänglich gemacht.

TOP 6. Sicherheitskonzepte für Kliniken

Herr Pommerening berichtet über das »Rahmenkonzept für die Informationsverarbeitung« der Mainzer Universitätsklinik, die einige Passagen zu Datenschutz und Datensicherheit enthält.

Herr Hornung stellt die Entwicklung des Datenschutzkonzeptes im Universitätsklinikum Marburg vor, an der er federführend beteiligt ist und bei der besonderes Gewicht auf ein problemorientiertes methodisches Vorgehen gelegt wird.

TOP 7. Leitlinien

Die Arbeitsgruppe stimmt darin überein, nicht den Begriff »Leitlinien«, sondern »Empfehlungen« zu verwenden. Das grundsätzliche Positions-Papier »Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens« wird ab sofort im WWW bereitgestellt. Herr Pommerening macht darauf aufmerksam, dass das Roland-Berger-Gutachten einige Seiten dieser Arbeit wörtlich übernommen hat. Im WWW sind auch schon die Sicherheitsempfehlungen zum Internet-Anschluss von Krankenhäusern zu finden; weitere zu beschließende Sicherheitsempfehlungen der AG, wie die unter TOP 4 behandelten zu NT-Netzen, sollen dort ebenfalls veröffentlicht werden.

Herr Pommerening legt zwei weitere Entwürfe vor. Der eine betrifft den Zugriff auf Patientendaten im Krankenhaus und ist noch sehr roh formuliert; er soll auf der nächsten Sitzung der AG weiter behandelt werden, der aktuelle Stand ist jeweils im passwort-geschützten Teil des WWW-Servers zu finden. Der andere Entwurf behandelt »Sicherheits-empfehlungen zu Modem-Verbindungen im Krankenhaus«. Hierzu werden folgende Ergänzungen und Änderungen eingebracht:

- Für Telearbeit zu Hause sollte wegen der Beschlagnahmeproblematik kein Privat-PC, sondern ein klinikeigener PC verwendet werden; dieser sollte inventarisiert sein und unterliegt dann auch der Kontrolle durch den Datenschutzbeauftragten.
- Die Fernwartung sollte nach Hardware, Betriebssystem und Anwendungssoftware abgestuft werden.
- Die Fernwartung sollte so weit wie möglich auf einem Testsystem erfolgen.
- Bei größerem Umfang der Fernwartung ist zu erwägen, dass das Krankenhaus zu diesem Zweck einen Raum bei der Wartungsfirma mietet, von dem aus die Aktivitäten abgewickelt werden.
- Da der Zugriff auf Patientendaten nicht in jedem Wartungsfall absolut ausgeschlossen werden kann, ist im unvermeidlichen Ausnahmefall auf die vertragliche Regelung der Fernwartung zu verweisen, die insbesondere eine persönliche Verpflichtung auf das Datengeheimnis enthalten muss.
- Auch die mögliche Weiterleitung von Wartungsproblemen an übergeordnete Service-Zentren oder Software-Entwickler (»Eskalation«) sollte im Vertrag geregelt sein; bei internationalen Firmen ist hier für die eventuelle Übermittlung von Daten ins Ausland die Datenschutzgesetzgebung zu beachten.
- Der Aufbau der Fernwartungsverbindung vom Krankenhaus her kann auch folgendes Vorgehen bedeuten: Anruf vom Krankenhaus beim Fernwartungsservice, Einschalten des Modems, Einwahl durch die Firma.

Mit diesen Änderungen werden die Empfehlungen einhellig gutgeheißen; sie werden ebenfalls im WWW zugänglich gemacht.

Als weitere, in nächster Zeit zu bearbeitende Themen für Empfehlungen werden genannt:

- Trustcenter: Aufgaben, Aufbau und Organisation,
- Klinische Arbeitsplätze,
- Umgang mit Standard-Software,
- Outsourcing,
- Aufgaben und Qualifikation des Klinik-Datenschutzbeauftragten,
- Aufgaben und Qualifikation von IT-Sicherheitsverantwortlichen,

sowie die Weiterarbeit an der FAQ-Liste.

TOP 8. KIS98

Die KIS-Tagung (»Praxis der Informationsverarbeitung im Krankenhaus« - 3. Fachtagung) findet am 7. und 8. Mai in Leipzig statt. Herr Pommerening verteilt das Programm. Es wird einen 2-stündigen Workshop »Datensicherheit: Sicherheitskonzepte für das Krankenhausnetz und die externe Kommunikation« geben, geleitet von Herrn Pommerening. Im Tagungsband ist ein entsprechender Beitrag vorgesehen; Inhalt sind im Wesentlichen die von der AG erarbeiteten Sicherheitsempfehlungen.

TOP 9. Verschiedenes

Die nächste Sitzung soll am 1. und 2. 10. 1998 bei Mediagate in Krefeld stattfinden.

Protokoll: Prof. Dr. K. Pommerening, 9.4.1998, letzte Änderung: 29.4.1998
E-Mail: Pommerening@imsd.uni-mainz.de