Protokoll
der 10. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Gesundheitsinformationssystemen
am 28./29. September 1998 in Krefeld

Die Sitzung fand im Hause der Thyssen Informatik statt.

Sitzungszeit: Montag, 28.9.1998, 14.15 bis 18.30 Uhr,
Dienstag, 29.9.1998, 9.30 bis 12.15 Uhr.

Anwesend: H. Baumann (Erlangen)
Dr. T. Berger (Krefeld)
Dr. B. Blobel (Magdeburg)
Prof. Dr. K. Pommerening (Mainz)
M. Sergl (Mainz)

Gäste: H. Breuer (Krefeld)
A. Kretschmer (Kempen)

Entschuldigt: J. Erdmann (Berlin)
Dr. B. Hornung (Marburg)
Dr. M. Hortmann (Bremen)
Dr. Z. Kardasiadou (Hannover)
Dr. R. Killmann (Erlangen)
Prof. Dr. K. Sauter (Kiel)
M. Schnabel (München)
J. Walther (Krefeld)
S. Wolf (Kiel)

Tagesordnung:
1. Begrüßung und Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Sicherheit von Windows NT
5. Fernwartung
6. Zugriff auf Patientendaten im Krankenhaus
7. Trustcenter im Krankenhaus
8. IT-Sicherheit an klinischen Arbeitsplätzen
9. Datenschutz-FAQ
10. Verschiedenes

TOP 1. Begrüßung und Festlegung der Tagesordnung

Herr Pommerening begrüßt die Teilnehmer und dankt den Herren Walther und Berger für die Organisation der Sitzung. Die Tagesordnung wird in der mit der Einladung verschickten Form angenommen. In der Sitzungspause am ersten Tag ist eine Besichtigung des Rechenzentrums der Thyssen Informatik vorgesehen.

TOP 2. Protokoll der vorigen Sitzung

Das Protokoll der 9. Sitzung wird in der vorliegenden Form angenommen.

TOP 3. Mitteilungen und Berichte

a) Die Startseite der AG hat die neue Adresse http://info.imsd.uni-mainz.de/AGDatenschutz

b) Herr Pommerening berichtet von der Fachtagung KIS 98. Der von ihm veranstaltete Workshop über »Sicherheitskonzepte für das Krankenhausnetz und die externe Kommunikation« war mit etwa 60 Teilnehmern gut besucht. Ferner gab es einen Vortrag von O. P. Schäfer über die Health Professional Card. Die Beiträge sind im Tagungsband zu finden:

G. Herrmann u. a. (Hrsg.):
Praxis der Informationsverarbeitung im Krankenhaus.
ecomed, Landsberg 1998,
ISBN 3-609-51570-8.
Die Folgetagung KIS 99 wird am 6. und 7. Mai in Dortmund stattfinden.

c) Herr Pommerening war am 10. September zum Arbeitskreis Gesundheit der Datenschutzbeauftragten des Bundes und der Länder als Sachverständiger eingeladen. Thema war die Ausgestaltung der Zugriffsrechte auf Patientendaten im Krankenhaus. Die Ergebnisse sind in den Entwurf zu TOP 6 eingeflossen.

d) Herr Pommerening weist darauf hin, dass inzwischen einige Fälle von Einbrüchen mit PC-Diebstahl in Krankenhäusern bekannt geworden sind. Das ist ein wichtiges Argument für die Frage, ob auch bei der Datenspeicherung eine Verschlüsselung ratsam ist. Herr Blobel weist daraufhin, dass im ISHTAR-Projekt eine Inzidenz-Datenbank eingerichtet wurde.

e) Herr Blobel berichtet, dass inzwischen die erste Zertifizierungsstelle nach dem Gesetz zur digitalen Signatur zugelassen worden ist: das Telekom Trust Center. Als weitere sollen demnächst Debis und TC TrustCenter folgen.

f) Herr Blobel berichtet, dass die HPC für das Magdeburger Tumorregister bis Mitte 1999 flächendeckend mit 1024-Bit-Schlüsseln eingeführt wird. Bei Bayern online steht die probeweise Einführung bevor. Die generelle Einführung wird sich aber mindestens bis 2000 verzögern; insbesondere ist die Spezifikation noch nicht endgültig festgelegt.

g) Herr Kretschmer weist auf das WWW-Angebot der Data Security Consult hin.

h) Herr Blobel berichtet von verschiedenen HL7-Meetings in den USA. Ziel ist der Aufbau einer Sicherheitsarchitektur. Als kurzfristige Alternative ist das `Secure mailing' auf MIME-Basis vorgesehen, mittelfristig wird eine offene Architektur und die ANSI/CEN-Standardisierung angestrebt. In den CORBA-Arbeitsgruppen wird zurzeit das Sicherheitsmodell erweitert mit dem Ziel, vom Systemverwalter unabhängig zu werden.

i) Herr Blobel trug auf der Chipkarten-Konferenz im März in München vor. Auf der MedInfo in Seoul hielt er einen Vortrag über »Security in Distributed Health Information Systems« und

war am Tutorial der IMIA-WG4 sowie an der »Meet the Experts«-Sitzung beteiligt. Ferner nahm er an mehreren anderen Konferenzen teil und hielt einige weitere Vorträge.

j) Im Rahmen des MEDSEC-Projekts wird in Magdeburg eine Software zur Sicherheitskonzeption nach Standards entwickelt, die Herr Blobel vorstellt. Ferner wurden dort Security Enhancements für HL7, XML, EDIFACT, X12 und xDT implementiert.

k) Neue Veröffentlichungen aus der AG sind im entsprechenden Verzeichnis auf dem WWW-Server der AG aufgeführt.

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

- Zwischenbericht der Enquete-Kommission »Zukunft der Medien in Wirtschaft und Gesellschaft« zum Thema »Sicherheit und Schutz im Netz«.
- Empfehlung der Kassenärztlichen Vereinigung Bayern: »Ärztliche Schweigepflicht, Datenschutz in der Arztpraxis, Sicherheit der Praxis-EDV«.
- Bericht der AG »Verwaltungen und Kliniken im Hochschulnetz« des Bayerischen Staatsministeriums für Unterricht, Kultus, Wissenschaft und Kunst: »Sicherheit in Verwaltungs- und Kliniknetzen, Anforderungen - Möglichkeiten - Empfehlungen«.
- Viele neue Angebote beim BSI, insbesondere eine Reihe von Empfehlungen, die auch als Faltblätter vorliegen, sowie die OCOCAT-Studie »Analyse der Risiken ausführbarer Web-Contents«, die für TOP 8 von Bedeutung ist.

Von Interesse für die AG ist auch die Mail-Liste `med-priv@it-sec.de`, die sich mit Datenschutzfragen in der Medizin befasst. Anmeldung an: `majordomo@it-sec.de`, Subject: egal, Text: `subscribe`

TOP 4. Sicherheit von Windows NT

Herr Pommerening berichtet, dass die Empfehlung der AG weite Kreise gezogen hat; beginnend mit dem Heise-News-Ticker, wurde sie unter anderem von der Computer-Zeitung, der iX, und der Mainzer Allgemeinen Zeitung zitiert. Ferner erhielt er viel zustimmende und einige ablehnende Mail, die zum Teil an die AG weitergeleitet wurde. Die aufgeworfene Frage nach der Produkthaftung ist komplex und liegt außerhalb der Kompetenz der AG; es ist aber nicht zu sehen, warum Softwarefirmen, die ihre Produkte für NT statt für Linux ausliefern, hierdurch einen Vorteil hätten.

In letzter Zeit wurde im Online-Text der Empfehlung die Liste der Links aktualisiert. Die AG beschließt als weitere Änderung die Streichung der nicht sinnvollen Empfehlung, den Namen des Administrators zu ändern.

TOP 5. Fernwartung

Anforderungen an die Fernwartung werden in den Sicherheitsempfehlungen zu Modem-Verbindungen im Krankenhaus der AG formuliert. Hierzu gibt es zwei Klarstellungswünsche:

a) Herr Killmann fragt, ob für telemedizinische Anwendungen wirklich grundsätzlich ein Modemserver und RAS gefordert werden sollten. Hierzu stellt die AG klar, dass der Fall, wo ein Krankenhaus bisher keine Modem-Anschlüsse oder nur die als Ausnahme genehmigten hat und nur an einer Stelle Telemedizin betreiben will, unter »begründete Ausnahmefälle«

einzuordnen ist. Was verhindert werden soll, ist die unregulierte Ausuferung von Modem- (oder ISDN-) -Anschlüssen. Die Begründung eines Ausnahmefalls bedeutet, dass die zentral zuständige Stelle im Krankenhaus von der Einrichtung Kenntnis bekommt, bei ihr mitwirkt und die Auswirkungen unter Kontrolle behält. Und wenn ein Modemserver da ist, sollte er auch verwendet werden; reicht er nicht, ist er entsprechend auszubauen.

b) Herr Baumann weist darauf hin, dass der berechtigte Personenkreis für Fernwartungszugriffe bei großen Firmen im Voraus nicht genau festzulegen ist, z. B. wenn das Problem bis hin zu einem zuständigen Entwickler eskaliert werden muss. Eine komplette Liste des Elite-Personals der Firma im Krankenhaus zu hinterlegen, ist datenschutzrechtlich problematisch. Nach Ansicht der AG ist bei der Rechtsgüterabwägung der Schutz der Patientendaten über den Schutz von Personaldaten zu stellen. Andererseits ist die Weitergabe von Daten im Rahmen der Fernwartung ohnehin nur dann datenschutzrelevant, wenn es sich um sensible Daten handelt, nicht aber, wenn die Daten anonymisiert sind. Die AG stimmt überein, eine entsprechende Ergänzung in die Empfehlung aufzunehmen.

Für die Vertragsgestaltung liegt bisher ein Muster vor. Herr Pommerening will noch weitere Muster sammeln und daraus einen Vorschlag zusammenstellen. Dieser soll dann von der AG per E-Mail diskutiert werden. Andere Probleme des Outsourcings stehen auf dem Arbeitsprogramm der AG.

TOP 6. Zugriff auf Patientendaten im Krankenhaus

Herr Pommerening berichtet, dass er den Entwurf der Empfehlung mit dem Arbeitskreis »Gesundheit« der Datenschutzbeauftragten des Bundes und der Länder ausführlich diskutiert hat und die vorgelegte Fassung im wesentlichen den dortigen Konsens wiedergibt mit der Ausnahme von länderspezifischen Besonderheiten, die in einer allgemeinen Empfehlung nicht abgedeckt werden können. Eingeflossen sind ein Arbeitspapier von Frau Dr. Wellbrock und Herrn Wehrmann vom Hessischen LfD sowie der aktuelle Entwurf von Herrn Hornung für das Datenschutzkonzept des Universitätsklinikums Marburg, das wiederum eine Reihe von Formulierungsvorschlägen von Herrn Blobel aufgenommen hat. Der Entwurf wird im Detail durchgegangen. Dabei werden neben leichten Formulierungsänderungen die folgenden wesentlichen Punkte erarbeitet.

- In die Präambel wird als Zusatz aufgenommen: »Auch Papierakten und -archive müssen datenschutzkonform gehandhabt werden; die folgenden Empfehlungen beziehen sich aber nur auf elektronisch gespeicherte Patientendaten. «
- Unter »Grundsätze« soll im zweiten Abschnitt das Prinzip der Erforderlichkeit explizit erwähnt werden, auch als »Prinzip der minimalen Rechte« oder »need-to-know«-Prinzip, wobei der letztere Ausdruck nicht in dem missverständlichen Sinne zu verstehen ist, dass der Zugreifende selbst bestimmt, was er benötigt.
- Im ersten Absatz von »2. Daten und Patientenakten« wird auf analoge Regelungen für den Fall des Shared Care hingewiesen.
- Abschnitt 3 wird neu formuliert; Herr Blobel wird einen Vorschlag per E-Mail machen.
- In Abschnitt 4 wird für die genetischen Daten ein eigener Aufzählungspunkt eingeführt. Da diese Daten auch Informationen über Angehörige enthalten, sind sie unter Datenschutzgesichtspunkten gesondert zu behandeln; z. B. ist der Patient nicht alleine freigabeberechtigt.
- Um Verwechslungen mit den bei einer Notaufnahme benötigten Daten zu vermeiden, wird vorgeschlagen, den Begriff »Notfalldaten« durch »Risikodaten« zu ersetzen. Die

AG verwirft diesen Vorschlag, da die Terminologie eingebürgert ist. Herr Blobel verweist darauf, dass ein Notfalldatensatz international definiert ist.

- Eine VIP-Regelung ist in den EU-Richtlinien vorgesehen. Danach sind die Patientenakten prominenter Personen mit einer VIP-Kennzeichnung zu versehen und nur unter besonderen Einschränkungen freizugeben. Ob für Klinikmitarbeiter eine analoge Regelung zu schaffen ist, ist in der AG noch umstritten. Herr Pommerening wird einen Vorschlag zur Diskussion stellen.

Die weitere Diskussion der Vorlage entfällt aus Zeitgründen. Sie soll per E-Mail stattfinden. Formulierungsvorschläge sind bis zum 15. November an Herrn Pommerening zu schicken. Er wird daraus eine neue Beschlussvorlage erstellen, die bis 20. Dezember als beschlossen gilt, sofern dann nicht noch gravierende Meinungsverschiedenheiten bestehen.

TOP 7. Trustcenter im Krankenhaus

Der Tagesordnungspunkt wird aus Zeitmangel auf die nächste Sitzung verschoben.

TOP 8. IT-Sicherheit an klinischen Arbeitsplätzen

Der Tagesordnungspunkt wird aus Zeitmangel auf die nächste Sitzung verschoben.

TOP 9. Datenschutz-FAQ

Der Tagesordnungspunkt wird aus Zeitmangel auf die nächste Sitzung verschoben. Herr Pommerening wird möglichst bald einen Entwurf auf dem zugangsbeschränkten Teil des WWW-Servers der AG bereitstellen.

TOP 10. Verschiedenes

Die nächste Sitzung soll in der 16. oder 17. Woche 1999 (die letzten beiden Wochen im April) stattfinden. Herr Pommerening weist darauf hin, dass die Neuwahl der AG-Leitung fällig ist.

Protokoll: Prof. Dr. K. Pommerening, 19.10.1998, letzte Änderung: 19.10.1998
E-Mail: Pommerening@imsd.uni-mainz.de