Protokoll
der 3. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Krankenhausinformationssystemen
am 10. und 11. November 1994 in Magdeburg

Die Sitzung fand im Sitzungsraum des Instituts für Biometrie und Medizinische Informatik der Otto-von-Guericke-Universität Magdeburg statt.
Anwesend:

- Dr. B. Blobel (Magdeburg)
- Dr. K.-H. Elsässer (Heidelberg)
- Dr. M. Hortmann (Bremen)
- Prof. Dr. K. Pommerening (Mainz)
- M. Schnabel (München)
- W. Thoben (Oldenburg)

Entschuldigt:

- S. Brings (Troisdorf)
- Dr. H. Lautenbacher (Tübingen)
- V. Lieder (Dresden)
- P. Messerer (Ludwigshafen)
- K. Scheffel (Lübeck)
- Dr. K.-H. Schicketanz (Mainz)
- Dr. W. Schoner (München)

Tagesordnung:

- 1. Mitteilungen und Berichte
- 2. Benutzung von PGP in der Arbeitsgruppe
- 3. Folgerungen des GSG für die Datenübermittlung
- 4. Stand der Realisierung von Schutzmaßnahmen im Magdeburger KIS
- 5. Bedrohungsanalyse für KIS
- 6. Zugriffsrechte im KIS
- 7. Sicherheitstechnik für KIS (Erarbeitung von Empfehlungen)
- 8. Festlegung der weiteren Arbeit
- 9. Verschiedenes

TOP 1. Mitteilungen und Berichte

a) Begrüßung der Teilnehmer. Herr Blobel stellt das Magdeburger Institut vor.

b) Herr Pommerening teilt mit, dass die bisherige "Projektgruppe" vom Beirat der GMDS zur "Arbeitsgruppe" ernannt worden ist.

c) Das Grundsatzpapier, das in der vorigen Sitzung beraten wurde, ist vom Vorsitzenden überarbeitet und nach dem vereinbarten Verfahren dem Präsidium der GMDS zugeleitet worden. Von dort ist bisher keine Rückmeldung erfolgt. Dennoch kann es als Grundlage für die weitere Arbeit der Gruppe dienen.

d) Bei der GMDS-Jahrestagung in Dresden hat Herr Blobel für sein Poster "Datenschutz in offenen Krankenhausinformationssystemen -- Probleme und Lösungen" einen Preis erhalten. Die Arbeitsgruppe gratuliert ihm dazu.

e) Herr Pommerening ist als Vertreter der GMDS in der IMIA Working Group 4 (`Data Protection') benannt worden. Herr Pommerening und Herr Blobel sind als Vertreter der GMDS in der EFMI Working Group 2 (`Data Protection and Security in Health Information Systems') benannt worden. Für die IMIA-Gruppe wurde bisher kein zweiter Vertreter gefunden. Herr Blobel erklärt sich bereit, auch diese Verpflichtung zu übernehmen.

f) Am 11. Juli 1994 fand in Brüssel ein `Security Workshop' statt, auf dem der gegenwärtige Stand des SEISMED-Projekts vorgestellt wurde. Teilnehmer aus unserer Gruppe waren die Herren Bleumer, Blobel, Hortmann und Pommerening. Veröffentlichungen der Ergebnisse der einzelnen SEISMED-Arbeitsgruppen wurden für den Spätherbst angekündigt. Bisher liegen vor

- High Level Security Policy,
- Guideline for Cryptographic Mechanisms.

Weitere EG-Projekte, deren Thematik die Arbeitsgruppe tangiert, sind SESAME (Sicherheit in offenen Systemen) und INFOSEC (Schaffung von Sicherheitsstandards). Herr Blobel hat im Rahmen des `Telematics Programme' (früher AIM) ein Projekt zur Benutzung von Chipkarten als Sicherheitsausweis (`Professional Card') eingereicht.

g) Am 15./16. September 1994 fand in Bonn ein Interdisziplinäres Forum mit dem Thema "Vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung" statt, veranstaltet von TeleTrusT Deutschland. Herr Pommerening nahm daran teil. Themenschwerpunkt war die Krankenversichertenkarte und mögliche Weiterentwicklungen davon. Eine interessante Einzelheit war die Demonstration des pseudonymen elektronischen Rezepts durch Herrn Struif von der GMD. Durch derartige Konzepte ließe sich auch die Datenschutzproblematik des GSG entschärfen.

h) Ebenfalls um Krankenversichertenkarten und Chipkarten ging es beim BSI-Dialog zum Thema "Patienten und ihre computergerechten Gesundheitsdaten" am 2./3. November in Boppard, an dem Herr Blobel für die Arbeitsgruppe teilnahm.

i) Herr Pommerening nahm am 13. Welt-Computer-Kongress der IFIP vom 28. August bis 2. September 1994 in Hamburg teil und trug über `Medical Requirements for Data Protection' vor. Leider war die Sitzung `Health System Protection' nur schwach besucht.

j) Der von Herrn Blobel organisierte internationale Workshop "Datenschutz in Medizinischen Informationssystemen" findet am 13./14. Februar 1995 in Magdeburg statt. Aus der Arbeitsgruppe werden ferner Herr Hortmann und Herr Pommerening teilnehmen.

h) Weitere Veranstaltungen im Jahre 1995 sind:

- VIS '95 (GI-Fachgruppentagung "Verlässliche IT-Systeme") am 5.-7. April in Rostock. Herr Pommerening wird über "Datenschutz in Krankenhausinformationssystemen" vortragen.
- 4. Deutscher IT-Sicherheitskongress des BSI am 8.-11.Mai in Bonn-Bad Godesberg.

- IMIA WG 4 Security Working Conference `Communicating Health Information' in Helsinki vom 30. September bis 3. Oktober.
- HEALTH CARDS '95 am 23.-26. Oktober in Frankfurt am Main.
- Seminar "Datenschutz in verteilten und offenen Systemen" an der Akademie Medizinische Informatik, Heidelberg, am 29. November unter der Leitung von Herrn Pommerening.

TOP 2. Benutzung von PGP in der Arbeitsgruppe

Herr Hortmann führt die Benutzung des Verschlüsselungsprogramms PGP vor. Nach Möglichkeit sollen die Arbeitsgruppenmitglieder das Programm bei sich installieren und für sich Schlüssel erzeugen. Um Erfahrungen mit dem Schlüsselmanagement zu gewinnen, sollten die Schlüssel ausgetauscht und wechselseitig oder vom Vorsitzenden unterschrieben werden.

Herr Blobel weist darauf hin, dass die elektronische Unterschrift bisher keine gesicherte rechtliche Relevanz hat. In Magdeburg sei die Verwendung im Pilotprojekt mit dem Datenschutzbeauftragten abgesprochen. Herr Hortmann weist auf folgendes Problem hin: Woher weiß ein Anwender, welches Dokument er wirklich unterschreibt? Bei Mehrbenutzer-Anlagen (z. B. unter UNIX) gibt es Probleme mit dem Systemverwalter, der Programme und Daten manipulieren könnte.

TOP 3. Folgerungen des GSG für die Datenübermittlung

Herr Blobel erläutert die nach dem GSG notwendigen Verfahren zur Datenübermittlung und deren Umfang. Dieser übertrifft das, was nach dem Grundsatzpapier der Arbeitsgruppe (und dem Buch von Seelos) klinikintern an Datenaustausch erlaubt ist. Die Daten müssen maschinenlesbar übermittelt werden; bevorzugtes Medium ist die Diskette im Brief. Die Durchführungsbestimmungen lassen z. T. nicht einmal Versand per Einschreiben zu, erst recht ist keine Rede von kryptographischer Verschlüsselung. Es ist also keine erwähnenswerte Transportsicherung im Sinne der Datenschutzgesetze möglich. Ein weiteres Problem ist, dass es für die Verarbeitung der Daten von verschiedenen Patiententypen (z. B. privat Versicherte) unterschiedliche rechtliche Grundlagen gibt, die streng genommen keine einheitliche Verarbeitung und Speicherung, etwa in derselben Datenbank, zulassen würden. Ferner bringt die beabsichtigte Steuerung der Kostenentwicklung im Gesundheitswesen die Gefahr mit sich, dass eine medizinisch notwendige Behandlung wegen fehlender Kostenübernahme durch die zuständige Krankenkasse unterlassen werden könnte.

Als Vorschläge zur Verbesserung der datenschutzrechtlichen Defizite des GSG werden genannt:

- Verschlüsselung der Datenübermittlung mit einem verfügbaren Programm, z. B. PGP.
- Einführung von Pseudonymen für die Kassenabrechnung.

Herr Pommerening wird das für die Verwendung von Pseudonymen nötige Verfahren bis zur nächsten Sitzung ausarbeiten. Als Musterbeispiele dienen das elektronische Rezept nach Struif und das elektronische Geld nach Chaum.

TOP 4. Stand der Realisierung von Schutzmaßnahmen im Magdeburger KIS

Herr Blobel berichtet über den weiteren Ausbau der Schutzmaßnahmen und die Weiterentwicklung des Sicherheitskonzepts. Der Einsatz des Systems MACS ist erweitert und die

Vorbereitung von NACS intensiviert worden. Im Sicherheitskonzept werden das Organisations-, das Funktions- und das Datenmodell abgebildet. Es wird unterschieden zwischen statischen Zugriffsrechten (die an die Person oder Organisation gebunden sind) und dynamischen Zugriffsrechten (die an die Rolle gebunden sind). Die vorhandenen Hierarchieebenen werden berücksichtigt, z. B. Chefarzt (der alle Patienten seiner Abteilung sieht), Oberarzt, Stationsarzt (der nur seine Patienten sieht). Die Notfallproblematik wird gesondert behandelt. Geplant ist die Einführung eines Dienstplansystems zur Zugriffsteuerung sowie der digitalen Signatur in der Kommunikation zwischen Leistungsstellen und Stationen und die Realisierung der verschlüsselten Kommunikation und Speicherung von Daten. Ein weiteres Ziel ist die Einführung der Professional Card zur Absicherung der Zugriffsregelungen und des Routings.

TOP 5. Bedrohungsanalyse für KIS

Die Arbeitsgruppe diskutiert, welche Bedrohungen in einem Sicherheitskonzept zu berücksichtigen sind. Reale Vorfälle im Gesundheitssystem sind kaum bekannt und sind dann kaum nachvollziehbar dokumentiert. So wurde aus den USA von einem Erpressungsfall und der Ausspähung eines Politikers berichtet. Bekannt wurde im Frühjahr der Fall eines Hackers in England, der Behandlungsdaten verfälscht hatte. Häufig wurden Computer-Viren in Kliniken angetroffen. Von Bedeutung, wenn auch nicht nachweislich im Gesundheitssystem aufgetreten, ist auch der Fall "Vobis-Festplatten", wo die Firma Vobis in Computer gebrauchte Festplatten einbaute, auf denen noch alte Daten des Vorbesitzers zu erkennen waren. Insgesamt muss man bei Datenschutz- und Sicherheitsverstößen von einer hohen Dunkelziffer ausgehen, über die man nur spekulieren kann.

Prinzipiell zu beachtende Bedrohungen sind:

- Dateneinsicht durch Klinikbesucher oder nichtmedizinisches Personal,
- unberechtigte Datenübermittlung innerhalb der Klinik,
- unberechtigter Datenexport,
- Forschung mit nicht anonymisierten Daten,
- auswärtige Hacker über das Internet,
- Computer- und Netzwartung,
- Personalprobleme,
- kriminelle Aktionen,
- Journalisten.

Das technische Grundproblem ist die ungesicherte Speicherung von Daten auf Arbeitsplätzen und Servern sowie die ungesicherte Datenübertragung im lokalen Netz, auch die Übertragung von Authentikationsdaten (z. B. Passwörtern). Probleme entstehen auch durch das `Outsourcing' der Verarbeitung von Patientendaten und durch die Langfristspeicherung. Herr Blobel weist darauf hin, dass die oft geforderte Wartung eines Software-Systems mit Testdaten in vielen Fällen nicht realistisch ist, da Probleme möglicherweise nur mit realen Daten auftreten.

Ein kurzer Abschnitt dieses Inhalts soll in das zu entwerfende Musterkonzept eingebaut werden.

TOP 6. Zugriffsrechte im KIS

Aus dem Grundsatzpapier der Arbeitsgruppe leitet sich als Vorgabe her, daß die Daten primär bei der erhebenden Abteilung gespeichert werden und vor den anderen Abteilungen zu schützen sind. Nötig ist eine klare Definition des Nutzerkreises und der Zugriffsrechte. Eine sinnvolle Aufgliederung der Zugriffsrechte umfasst die Rechte `create', `use (read)', `modify', `add', `copy', `access control', wobei letzteres gemäß dem "Prinzip der logischen Überweisung" (Blobel) zu handhaben ist. Besonders zu berücksichtigen ist das Notfallzugriffsrecht, das eine besondere Supervivion erfordert. Die von Herrn Seelos erarbeitete Zugriffsmatrix kann als Ansatzpunkt dienen, ist aber entsprechend zu modifizieren. Die Schutzstufen aus dem Katalog der technischen und organisatorischen Maßnahmen zum Datenschutz des staatlichen Koordinierungsausschusses Datenverarbeitung (Bayern) sollten nur implizit berücksichtigt werden, da ohnehin das `need to know'-Prinzip strikt anzuwenden ist. Für die Definition von Rollen und zugehörigen Zugriffsrechten ist das von Herrn Hortmann im TANIT-Projekt entwickelte Modell als Grundlage geeignet. Herr Blobel erklärt sich bereit, aufgrund der Vorarbeiten in Magdeburg einen entsprechenden Teil des Sicherheitskonzepts zu verfassen.

TOP 7. Sicherheitstechnik für KIS (Erarbeitung von Empfehlungen)

Herr Pommerening führt bisherige Überlegungen zum Thema aus. Sicherheitstechnik soll dafür sorgen, dass Zugangs- und Zugriffsrechte gewährt, kontrolliert, abgesichert und protokolliert werden. Als Vorgaben aus der Grundsatzerklärung der Arbeitsgruppe sind zu beachten:

- möglichst wenig Belästigung der Benutzer,
- keine Beeinträchtigung der Verfügbarkeit der Daten.

Wegen der großen Unterschiede zwischen Krankenhausinformationssystemen ist darauf zu achten, dass vor allem systemunabhängige oder anpassbare Vorschläge gemacht werden. Der "Flaschenhals" bei der Anwendung von Sicherheitsprodukten, egal, ob kommerziell oder frei verfügbar, ist der Einbau in bestehende Anwendungen.

Mögliche allgemeingültige Empfehlungen für Sicherheitsmaßnahmen sind:

- grundsätzlich verschlüsselte Datenspeicherung,
- grundsätzlich verschlüsselte Kommunikation (Datenübermittlung),
- überprüfbare Zugriffskontrolle (mandatory) aufgrund einer systemweit definierten Zugriffsmatrix,
- elektronische Unterschrift von Verordnungen, Leistungsanforderungen, Kommunikation, Dokumentation,
- zentrales Schlüsselverzeichnis (mit zentraler Zertifikationsinstanz),
- Chipkarten als persönlicher Ausweis und Schlüsselablage (Professional Card),
- Firewall- und andere Netzsicherheitstechniken,
- Einsatz von PC-Sicherheitssystemen,
- organisatorisch: Verpflichtung, Schulungen, ...

Ob sichere oder schwache Verschlüsselungsverfahren eingesetzt werden, macht für den Implementierungs- und Organisationsaufwand keinen Unterschied, es gibt also keinen Grund, schwache Verfahren zu verwenden.

Als Techniken zur Gewährleistung der Sicherheit auf Arbeitsplatzsystemen und Servern sind geeignet:

- Kryptographische Filesysteme -
  - SFS, SecureDrive u. a. für MS-DOS,
  - CFS für UNIX,
- PC-Sicherheitssysteme, z. B. von den Firmen CEInfosys oder uti-maco,
- Chipkarten als Zugangsschutz.

Zur Erhöhung der Netzsicherheit einsetzbare Produkte sind:

- Kerberos als Authentikationsservice,
- DCE zum Einbau der Kerberos-Dienste in Anwendungen,
- SESAME als europäische Variante der Kerberos-Dienste,
- TCP-Wrapper zur Kontrolle der TCP/IP-Dienste,
- PGP für e-Mail

und viele andere. Dazu kommt noch die gesamte Sammlung der Produkte, die man zur Einrichtung einer Firewall braucht. An der Uniklinik Mainz wird gerade mit der Einrichtung einer Firewall begonnen; Herr Pommerening wird der Arbeitsgruppe auf der nächsten Sitzung darüber berichten.

Bezugsquellen für die genannten Produkte werden in einer Liste "Literatur und Internet-Ressourcen für die GMDS-Arbeitsgruppe ..." genannt, die diesem Protokoll beigefügt ist.

TOP 8. Festlegung der weiteren Arbeit

Herr Pommerening wird gebeten, rechtzeitig vor der nächsten Sitzung einen ersten Entwurf für ein Mustersicherheitskonzept zu erstellen und den Mitgliedern der Arbeitsgruppe zuzusenden.

Die nächste Sitzung ist für den 18./19. Mai 1995 in Bremen geplant.

TOP 9. Verschiedenes

Auf der Interhosptial-Messe in Hannover im April ist ein Beitrag der Universitätsklinik Magdeburg geplant.

Protokoll: (Prof. Dr. K. Pommerening)

email: Pommerening@imsd.uni-mainz.de

PGP public key fingerprint = F5 03 CE E7 70 C2 8C 74 BA ED EC 60 83 3B 7C 89