

Protokoll
der 12. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Gesundheitsinformationssystemen
am 23./24. November 1999 in Marburg

Die Sitzung fand in der Institutsbibliothek des Institut für Medizinische Informatik der Philipps-Universität in Marburg statt.

Sitzungszeit: Dienstag, 23.11.1999, 15.15 bis 19.30 Uhr,
Mittwoch, 24.11.1999, 9.10 bis 12.00 Uhr.

Anwesend: H. Baumann (Erlangen)
Dr. B. Blobel (Magdeburg)
J. Erdmann (Berlin)
Dr. B. Hornung (Marburg)
Dr. W. Kirsten (Frankfurt)
Prof. Dr. K. Pommerening (Mainz)
M. Schnabel (München)
M. Sergl (Mainz)
A. Teschler (Münster)
J. Walther (Krefeld)
S. Wolf (Kiel)

Entschuldigt: S. Hinze (Bonn)

Tagesordnung: 1. Begrüßung und Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Status der bisherigen Empfehlungen der AG
5. Nutzung von E-Mail in der Medizin
6. Datenschutz und Datensicherheit in medizinischen Forschungsnetzen
7. Die Situation des Datenschutzes am Universitätsklinikum Marburg
8. Outsourcing von Sicherheitsdienstleistungen
9. IT-Sicherheit an klinischen Arbeitsplätzen
10. Datenschutz-FAQ
11. Verschiedenes

TOP 1. Begrüßung und Festlegung der Tagesordnung

Herr Kuhn als Leiter des Instituts begrüßt die Arbeitsgruppe in Marburg. Herr Pommerening begrüßt die Teilnehmer und dankt Herrn Hornung für die Organisation der Sitzung. Die Tagesordnung wird in der mit der Einladung verschickten Form angenommen.

TOP 2. Protokoll der vorigen Sitzung

Das Protokoll der 11. Sitzung wird in der vorliegenden Form angenommen.

TOP 3. Mitteilungen und Berichte

- Die WWW-Adresse der GMDS hat sich geändert: www.gmds.de.
- Verschiedene Stellungnahmen zur Gesundheitsreform 2000 sind im WWW zu finden:
 - GMDS: www.gmds.de/texte/onlinedocs/stellungn_gesundheitsreform_2000.html.
 - DVD (Deutsche Vereinigung für Datenschutz e. V.): www.aktiv.org/DVD/texte/gvk2000.html.
 - LfD Schleswig-Holstein: <http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/gesund/gesref.htm>.
 - Entschließung der Datenschutzbeauftragten des Bundes und der Länder: <http://www.datenschutz-bayern.de/dsbk-ent/gesref00.htm>.

Eine Stellungnahme Dr. M. Walz (Mannheim) wurde den AG-Mitgliedern per E-Mail zugesendet. In diesem Zusammenhang ist auch von Interesse der Vorschlag:

- Patientenschutz durch Pseudonymisierung: <http://www.datenschutz-bayern.de/dsbk-ent/patpse58.htm>.

Die AG ist der Meinung, dass sie keine weitere Stellungnahme verfassen sollte.

- Weitere neue Verweise ins WWW:
 - Denley/Smith: Privacy in clinical information systems in secondary care, BMJ.
 - Ethical issues of IT in Healthcare.
 - Health Care Professionals' Protocol (HCP), ein gemeinsames Pilotprojekt der Kassenärztlichen Vereinigung Bayerns und der Bayerischen Landesärztekammer.
 - Eckpunkte der deutschen Kryptopolitik (Pressemitteilung des BMWi) [Link existiert nicht mehr].
 - BSI warnt vor dem Einsatz von JavaScript.
 - Aktionsforum Telematik im Gesundheitswesen (ATG). Die GMDS und der BVMi sind durch Benennung von Experten beteiligt.
- Weitere Stellungnahmen von Landesdatenschutzbeauftragten:
 - Epidemiologie und Datenschutz.
 - Zugriff auf Behandlungsunterlagen von Patienten durch pensionierte Ärzte einer Klinik für Forschungszwecke.
 - Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet (erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder).
 - Datensicherheit bei der Installation und beim Betrieb von Windows NT.

Stellungnahmen zum Outsourcing siehe unter TOP 8, zur Arbeitsplatzsicherheit unter TOP 9.

- Das im WWW zur Verfügung gestellte Vorlesungsmanuskript »Datenschutz und Datensicherheit« von Herrn Pommerening wurde erheblich erweitert.

- Eine neue Arbeit von Arjen Lenstra und Eric Verheul, »Selecting cryptographic key sizes«, diskutiert den aktuellen Stand der Wissenschaft bei der Wahl von Schlüssellängen; Fazit: für Sicherheit bis ca. 2020 sollte man mindestens 90-Bit-Schlüssel für die gängigen symmetrischen Verfahren, 2048-Bit-Schlüssel für RSA/DH und 190-Bit-Schlüssel für Elliptische-Kurven-Verfahren verwenden.
- Bei dem von der DFG geförderten Projekt des Instituts für Medizinische Biometrie und Informatik der Universität Heidelberg, einen Anforderungskatalog für die Informationsverarbeitung im Krankenhaus zu erstellen, ist Herr Pommerening als Experte beteiligt.
- Durch die Presse ging unlängst ein Vorfall, bei dem mehrere hundert Patienten-Blätter frei im Internet zugänglich waren. In diesem Zusammenhang weist Herr Blobel darauf hin, dass im ISHTAR-Projekt ein Schema für Incidence Reports zur Verfügung gestellt wird, die dort als PGP-verschlüsselte Mail eingesendet werden können und vertraulich behandelt werden.
- Herr Wolf berichtet, dass der Datenschutzbeauftragte des Universitätsklinikums Kiel zurzeit ein Datenschutz-Handbuch vorbereitet, das evtl. im WWW zur Verfügung gestellt werden soll.
- Die IMIA Working Group 4 veranstaltet vom 21. bis 24. Juni 2000 in Victoria, B. C., Canada, eine Arbeitstagung zum Thema »Security of the Distributed Electronic Patient Record«.
- Herr Blobel berichtet, dass der Ausschuss DIN C-7 zu einer Arbeitsgruppe wird. Zusammenarbeit besteht mit der CEN TC-251, WG3 (Security, Safety and Quality), und der ISO TC-215, WG 4 (Security). Er gibt einen Überblick über Security Proposals, Security Policy und rechtliche Grundlagen; eine Zusammenstellung wird er für die AG zur Verfügung stellen.
- Das Onkonet Sachsen/Anhalt verwendet eine Sicherheitsinfrastruktur auf Internetbasis. Verwendet wird ein Kommunikationsserver, der mit SecuDE sichere Kommunikation, Filetransfer und sichere Abfragen ermöglicht.

TOP 4. Status der bisherigen Empfehlungen der AG

Auf Wunsch des Präsidiums soll die AG regelmäßig die herausgegebenen Empfehlungen auf Aktualität überprüfen. Aus Sicht der AG sind zurzeit keine wesentlichen Änderungen nötig.

Die Empfehlungen zu Modem-Verbindungen, zum Zugriff auf Patientendaten und die Formulierungshilfen für einen Fernwartungsvertrag bleiben unverändert. Den Sicherheitsempfehlungen zu Windows-NT-Netzen werden am Ende einige neue Links hinzugefügt:

- Datensicherheit bei der Installation und beim Betrieb von Windows NT (LfD Bayern)
- Kostenlose und geprüfte Software - Empfehlungen für Sicherheitsbeauftragte (Uni Tübingen)
- Windows 2000 Security
- Die Sicherheit von Windows 2000

Die Empfehlungen zum Internet-Anschluss erscheinen leicht überarbeitungsbedürftig; es soll deutlicher betont werden, welche Sicherheit durch eine Firewall-Lösung nicht gewährleistet wird. Ferner sind Verweise ins Internet angebracht zu:

- BSI warnt vor dem Einsatz von Javascript.
- Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet (erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder).

TOP 5. Nutzung von E-Mail in der Medizin

In letzter Zeit mehren sich Empfehlungen zum Einsatz von E-Mail im Gesundheitswesen; auch enthält Praxissoftware inzwischen oft ein integriertes E-Mail-Programm. Es liegen vor:

- Hodge, Gostin, Jacobson: Legal issues concerning electronic health information - Privacy, quality, and reliability. JAMA 282 (1999) 1466 - 1471.
- KV Bayern: Leitlinien für den E-Mail-Versand im Gesundheitswesen.
- Regeln für die sichere digitale Kommunikation. Deutsches Ärzteblatt 96/38, 24. September 1999, B-1905 - 1907.
- Empfehlung der AG Internet: Klinische Nutzung von E-Mail.
- Ein Entwurf der GMDS-Präsidiumskommission "Netzdienste im Gesundheitswesen".

In der Diskussion werden folgende Gesichtspunkte aufgeführt:

- Sicherheit in der IT ist ein komplexes Thema, auch für Experten. Sicherheitsmaßnahmen sind oft trügerisch und nur mit großer Sorgfalt stabil zu erhalten. Wer das Medium nicht sicher beherrscht, sollte die Finger davon lassen!
- Für den Internet-Anschluss von niedergelassenen Ärzten sollte der Dienst eines geschlossenen Ärztenetzes in Anspruch genommen werden; ist das nicht möglich, ist bis auf weiteres für die Informationsbeschaffung und Kommunikation ein separater, nicht ans lokale Netz angeschlossener Rechner zu verwenden, wobei ein Billigrechner völlig ausreicht.
- Ärztenetze sollten Schutzmaßnahmen nach dem Stand der Technik anbieten, insbesondere:
 - einen gesicherten Übergang ins Internet (Firewall-Technik),
 - eine kryptografische Infrastruktur,
 - Hilfe für eine sichere Grundkonfiguration,
 - explizite Qualitätssicherung auch im Bereich der IT-Sicherheit.

Die patientenbezogene Kommunikation muss grundsätzlich verschlüsselt ablaufen, wobei für symmetrische Verschlüsselung 128-Bit-Schlüssel, für die gängigen asymmetrischen Verschlüsselung 2048-Bit-Schlüssel als Minimum nach dem Stand der Technik anzusehen sind. Zu beachten ist, dass diese beiden Verfahrensklassen meist kombiniert eingesetzt werden (»hybride Verschlüsselung«) -- es müssen *beide* Schlüssellängen stimmen.

- Universitätskliniken und große Krankenhäuser sind dazu angehalten, für gründliche Fortbildung ihres IT-Personals in Sicherheitsfragen zu sorgen; insbesondere sollten sie einen IT-Sicherheitsbeauftragten beschäftigen.

- Private und dienstliche E-Mail sind strikt zu trennen.
- Eine in Praxis- oder Krankenhaussoftware integrierte E-Mail-Funktion sollte nur dann verwendet werden, wenn sie die im Ärztenetz oder der Telematik-Plattform vorgesehene kryptografische Infrastruktur verwenden kann.
- Durch Multimedia-Mail werden statt reiner Texte zunehmend Dokumente verschickt, die mit Standard-Software (z. B. Textverarbeitung) erstellt wurden. Gegen das Risiko, dass hier Schadprogramme (Viren und Trojanische Pferde) sowie verdeckte Informationen mit versendet werden, hilft auch keine Verschlüsselung. Solche Dateien sollten so lange nicht verschickt werden, wie die Anbieter dieser Software nicht Vorkehrungen für einen sicheren Dokumentenaustausch vorsehen.
- Weitergehende Netzdienste wie Telekonferenzen, Terminal-Services u.a. werden sicherheitstechnisch noch überhaupt nicht beherrscht. Ihre Verwendung sollte daher bis auf Weiteres sorgfältig kontrollierten Pilotprojekten vorbehalten bleiben.
- Von der elektronischen Kommunikation mit Patienten ist grundsätzlich abzuraten aus Gründen der Fürsorgepflicht und des Vertrauensschutzes:
 - Der Arzt kann nicht davon ausgehen, dass der Patient sich der vielfältigen Risiken der elektronischen Kommunikation bewusst ist und die notwendigen Kenntnisse zu einer sicheren Gestaltung hat.
 - Eine Terminvereinbarung per E-Mail ist genauso wenig zulässig wie eine Terminvereinbarung per Postkarte.
 - Auch bei verschlüsselter Kommunikation kann der Netzbetreiber Patientenlisten für jeden angeschlossenen Arzt erzeugen.
 - Insofern ist auch eine Einwilligung des Patienten in die elektronische Kommunikation keine Rechtfertigung.

Herr Pommerening wird eine entsprechende Stellungnahme für die Präsidiumskommission »Netzdienste im Gesundheitswesen« abfassen.

TOP 6. Datenschutz und Datensicherheit in medizinischen Forschungsnetzen

Herr Pommerening berichtet über die Telematik-Plattform für die medizinischen Forschungsnetze (TMF), in deren AG »Datenschutz und Datensicherheit« er mitwirkt. Sie soll den Kommunikationsbedarf in Forschergruppen und insbesondere multizentrische Studien unterstützen; vertreten sind in ihr z. Z. 23 Verbände der Gesundheitsforschung, die vom BMBF gefördert werden. Hauptziel ist, eine Kommunikationsinfrastruktur mit den nötigen Sicherheitsmaßnahmen aufzubauen. Es gibt zur Zeit noch erhebliche Probleme mit der Auswahl einer chipkartengestützten PKI (Public Key Infrastructure) mit den Anforderungen:

- Umsetzung offener Standards,
- Aufwärtskompatibilität zur Health Professional Card,
- Unterstützung vorhandener Anwendungen, insbesondere Mail und WWW-Browser,
- Verwendbarkeit für Zugriffskontrolle und kryptografisch geschützte Kommunikation bei Remote-Data-Entry.

Von den angebotenen kommerziellen Lösungen erfüllt keine mehr als zwei dieser Anforderungen.

TOP 7. Die Situation des Datenschutzes am Universitätsklinikum Marburg

Herr Hornung berichtet über die Organisation des Datenschutzes am Universitätsklinikum Marburg sowie über Vorab-Begutachtung und Technikfolgenabschätzung am Beispiel des ABDA-Telematik-Projekts. Hier wird ein systematischer Ansatz zur Evaluierung von IT-Systemen des Gesundheitswesens in Anlehnung an das EUROCARDS-Projekt verfolgt. Die technischen Vorarbeiten sind abgeschlossen, z.Z. werden Pilotregionen gesucht. Eine systematische Evaluation ist vorgesehen.

TOP 8. Outsourcing von Sicherheitsdienstleistungen

Hier liegen einige neuere Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder vor:

- Outsourcing von Schreibarbeiten bei Krankenhäusern.
- Rechtliche Grenzen bei der externen Archivierung von Behandlungsunterlagen aus Krankenhäusern (Outsourcing der Krankenblattarchivierung).
- Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen (Entschließung der Datenschutzkonferenz vom 17./18.04.1997).

Die AG beschließt, zunächst von einer weiteren Stellungnahme anzusehen und statt dessen auf die genannten zu verweisen.

TOP 9. IT-Sicherheit an klinischen Arbeitsplätzen

Auch hier liegen Empfehlungen der Datenschutzbeauftragten vor, die angesichts des sehr umfangreichen Problembereichs natürlich nur unvollständig sein können:

- Sicherheitsbelehrung für die Benutzung von Personal Computern.
- Prüfansätze des PC-Einsatzes.

Die Arbeitsgruppe diskutiert den Inhalt einer möglichen eigenen Empfehlung. Dabei werden folgende Gesichtspunkte genannt:

- Grundeinstellungen von Arbeitsplatzrechnern:
 - Bootvorgang,
 - Zugriffskontrolle,
 - Kontrolle von Laufwerken und Schnittstellen.
- Persönliche Verhaltensregeln:
 - Umgang mit Datenträgern,
 - Passwörter oder andere Authentisierungsmethoden,
 - Bildschirmschoner.

- Umgang mit Standard-Software:
 - Umgang mit Makros, Virengefahr,
 - Verwendung von Versandformaten, z. B. bei Arztbriefen.
- Umgang mit Netz-Software:
 - WWW-Browser und Sicherheitseinstellungen,
 - Gefahren durch aktive Inhalte,
 - E-Mail und Mail-Attachments,
 - Bedeutung und Einsatz von Virenschutz-Programmen,
 - Bedeutung von Sicherheitslücken des Arbeitsplatzes für das Kliniknetz.
- Hinweise auf Verschlüsselungsmöglichkeiten und deren Einsatz:
 - verschlüsselte Speicherung mit Produkten wie PGP-Disk oder Scramdisk,
 - verschlüsselte Datenübertragung mit PGP oder S/MIME.

Herr Hornung will hierzu auch die entsprechenden Teile des Marburger Datenschutzkonzeptes zur Verfügung stellen.

TOP 10. Datenschutz-FAQ

Der Tagesordnungspunkt wird aus Zeitmangel auf die nächste Sitzung verschoben. Ein Entwurf ist auf dem zugangsbeschränkten Teil des WWW-Servers der AG zu finden. Die Herren Erdmann, Hornung, Kirsten und Schnabel erklären sich bereit, ihn bis zur nächsten Sitzung zu überarbeiten.

TOP 11. Verschiedenes

Die Linksammlung zu medizinischen Themen in den Tätigkeitsberichten der Landesdatenschutzbeauftragten soll überarbeitet und auf den neuesten Stand gebracht werden. Herr Wolf erklärt sich dazu bereit.

Die nächste Sitzung soll Anfang April 2000 in Frankfurt stattfinden. Der Termin wird noch festgelegt. Die AG ist einhellig der Meinung, dass die zweitägige Sitzungsdauer -- ein Nachmittag und der folgende Vormittag -- beibehalten werden soll, nach Möglichkeit am Dienstag und Mittwoch.

Protokoll: Prof. Dr. K. Pommerening, 5.12.2000, letzte Änderung: 5.12.2000

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