# Protokoll
# der 13. Sitzung der GMDS-Arbeitsgruppe
# *Datenschutz in Gesundheitsinformationssystemen*
# am 19./20. Dezember 2000 in Frankfurt

Die Sitzung fand im Zentrum der Medizinischen Informatik des Klinikums der Johann Wolfgang Goethe-Universität in Frankfurt am Main statt.

**Sitzungszeit:** Dienstag, 19. 12. 2000, 14.00 bis 18.15 Uhr,
Mittwoch, 20. 12. 2000, 9.05 bis 12.10 Uhr.

**Anwesend:** Dr. B. Blobel (Magdeburg)
J. Erdmann (Berlin)
G. Exenberger (Erlangen)
Dr. W. Kirsten (Frankfurt)
Dr. W. Leetz (Erlangen)
Prof. Dr. K. Pommerening (Mainz)
M. Schnabel (München)
M. Sergl (Mainz)

**Entschuldigt:** Dr. B. Hornung (Marburg)
Dr. M. Hortmann (München)
Dr. Z. Kardasiadou (Thessaloniki)
Prof. Dr. H.-U. Prokosch (Münster)
J. Walther (Essen)
B. Wirlitsch (Nürnberg)

**Tagesordnung:**
1. Begrüßung und Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. Status der bisherigen Empfehlungen der AG
5. Die Situation des Datenschutzes am Universitätsklinikum Frankfurt
6. Von der Ausschreibung zum Verfahrensverzeichnis - Datenschutz gemäß EU-Richtlinie in Marburg
7. IT-Sicherheit an klinischen Arbeitsplätzen
8. Administrator-Verpflichtung
9. Fernwartung und Wartung vor Ort
10. Externe Befundserver
11. Datenschutz-FAQ
12. Telearbeit
13. Verschiedenes

## TOP 1. Begrüßung und Festlegung der Tagesordnung

Herr Pommerening begrüßt die Teilnehmer und dankt Herrn Kirsten für die Organisation der Sitzung. Da neue Teilnehmer anwesend sind, stellen sich alle kurz vor. Die Tagesordnung wird in der mit der Einladung verschickten Form angenommen. Da Herr Hornung kurzfristig absagen musste, wird der Tagesordnungspunkt 6 auf die nächste Sitzung verschoben.

**TOP 2. Protokoll der vorigen Sitzung**

Das Protokoll der 12. Sitzung wird in der vorliegenden Form angenommen.

**TOP 3. Mitteilungen und Berichte**

- Der Jahresbericht der AG für die GMDS wurde von Herrn Pommerening verfasst.

- Herr Pommerening berichtet aus der Arbeitsgruppe »Datenschutz und Datensicherheit« der TMF (Telematik-Plattform für die medizinischen Forschungsnetze des BMBF). Als Forderungen für kartenbasierte PKI wurden aufgestellt:
    - Aufwärtskompatibilität zur HPC (Health Professional Card),
    - Unterstützung von offenen Protokollen, vor allem Interoperabilität mit dem http-Protokoll, insbesondere mit vorhandenen Browsern,
    - keine Installation von umfangreicher proprietärer Software,
    - Nutzerwerkzeuge zur Schlüsselerzeugung,
    - Verwendbarkeit zur Zugriffskontrolle bei RDE.

  Die vorhandenen Angebote erfüllen maximal 3 dieser 5 Forderungen.

  Herr Blobel berichtet, dass das KKS Düsseldorf eine in Magdeburg zur Einbindung in das Onconet entwickelte PKI-Infrastruktur übernehmen will.

  Ein weiteres zentrales Thema der TMF-AG ist der Pseudonymisierungsdienst. Hier wurden verschiedene Modelle zur Pseudonymisierung in medizinischen Forschungsnetzen entwickelt, die im nächsten Jahr in Pilotprojekten umgesetzt werden sollen.

- Die Stellungnahme der GMDS-Präsidiumskommission zu Netzdiensten im Gesundheitswesen wurde bisher nicht veröffentlicht. Die Vorschläge der AG sind zum großen Teil in den Entwurf eingeflossen, aber z.T. abgeschwächt. Herr Erdmann weist darauf hin, dass die Stellungnahme bereits öfter zitiert wird. Die AG ist der Meinung, dass sie ihre eigene E-Mail-Empfehlung ausarbeiten und im WWW bereitstellen sollte.

- Aktuelle Themen der ATG (Aktionsforum Telematik im Gesundheitswesen) sind:
    - internationale Dimension der Gesundheitstelematik,
    - elektronisches Rezept,
    - elektronischer Arztbrief,
    - Sicherheitsinfrastruktur.

- Bei der Gesundheitsreform ist endlich eine Pseudonymisierung des Abrechnungsverfahrens vorgesehen, wie von der AG schon vor einigen Jahren gefordert. Die AG weist darauf hin, dass Anonymisierung und Pseudonymisierung

keinen absoluten Schutz bedeuten; die Gefahr eines Datenabgleichs besteht trotzdem. Daher müssen auch anonymisierte oder pseudonymisierte Daten zugriffsgeschützt sein.

- In letzter Zeit wurden viele Angriffe auf WWW-Server von Sicherheitsfirmen bekannt, z. B. NAI und McAfee. Es scheint sich um ein Outsourcing-Problem zu handeln. Bekannt wurden aber auch Angriffe auf Krankenhausserver in den USA, siehe Risks-21.14.

  Herr Pommerening erwähnt, dass das ISHTAR Incident Reporting Scheme auf dem ISHTAR-Server zwar erwähnt wird, aber nicht zu finden ist.

  Herr Blobel berichtet, dass auf das Magdeburger Netz (Server) viele Hackerangriffe registriert wurden; die meisten von innen.

  Nach den CERT-Summaries sind die aktuell häufigsten Bedrohungen:
  - Ausnutzung von Sicherheitslücken in TCP/IP-Software, insbesondere von Servern, zunehmend von Windows-Servern, darunter sehr viele Denial-of-Service-Attacken.
  - Mail-Viren und andere, per Mail übertragene Schadprogramme, hier fast ausschließlich unter Nutzung von Windows-Technologie - z. B. ActiveX, File Sharing, Object-Linking und »Features« von Outlook und Outlook Express - sowie von Browser-Fehlern.

  In der Diskussion wird noch einmal ein Vergleich zwischen LINUX und Windows gezogen. Allgemein wird darauf hingewiesen, dass Interoperabilität Angriffsmöglichkeiten schafft.

- Die Datenschutzbeauftragten des Bundes und der Länder haben ihre WWW-Präsenz weiter ausgebaut. Zu erwähnen ist zunächst das virtuelle Datenschutzbüro im Web unter www.datenschutz.de:
  - Deutsche Sektion,
  - Schweizer Sektion,
  - internationale Sektion,
  - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

  Ferner findet man Orientierungshilfen, Arbeitspapiere und Musterverträge, u.a.:

  - Orientierungshilfe Internet
  - Datenschutzrechtliche Vorgaben für die Verarbeitung personenbezogener Patientendaten im Rahmen des neuen Hausarztmodells und in Praxisnetzen
  - Mustervereinbarung zur Hardwarewartung
  - Checkliste zur Vorabkontrolle nach § 7 HDSG
  - Mustervertrag zur Auftragsdatenverarbeitung
  - Orientierungshilfe Fernwartung / Text, Erläuterung
  - Orientierungshilfe Protokollierung
  - Arbeitspapier zur Sicherheit bei Client-Server-Systemen
  - Arbeitspapier zu Dienstanweisungen für den Datenschutz
  - Telefax und Datenschutz / Arbeitspapier, Erläuterung
  - Arbeitspapier Kommunikation im Krankenhaus
  - Arbeitspapier Epidemiologie und Datenschutz

und die oft zitierten Broschüren des LfD Rheinland-Pfalz:

  - Heft 3 - Datenschutzrechtliche Anforderungen an wissenschaftliche Forschungsvorhaben
  - Heft 4 - Datenschutz im Krankenhaus

Besonders erwähnenswert ist die Volltextsuche im WWW-Angebot der Datenschutzbeauftragten.

- Herr Blobel weist darauf hin, dass der Arbeitskreis der Datenschutzbeauftragten in der GDD zurzeit ein Handbuch zum Datenschutz erarbeitet, das für die Mitglieder der GDD erhältlich sein wird.

- Von der KVB Bayern gibt es eine Empfehlung »Ärztliche Schweigepflicht, Datenschutz in der Arztpraxis, Sicherheit der Praxis-EDV«.

- Herr Blobel berichtet, dass von der CEN TC 251 AG 2 eine Empfehlung zur Durchführung von Audits in Vorbereitung ist. Außer Zugreifendem und Zeitpunkt sollen u. a. auch die genaue Funktion und die betroffenen Daten bis auf Itemebene erfasst werden.

- Weitere neue Verweise ins WWW:
  - Seite des Bundestagsunterausschusses »Neue Medien« zur BDSG-Novellierung. Herr Erdmann schlägt vor, zu überprüfen welche Veränderungen mit dem neuen BDSG auf uns zukommen. (Grundsätzlich Öffnung für die elektronische Welt, Präventionsgedanke, Protokollierung, externe Datenschutzbeauftragte)
  - Die neue Telekommunikations-Datenschutzverordnung wurde am 22.11.2000 vom Kabinett beschlossen; Volltext im WWW. Sie sieht eine längere und umfangreichere Speicherung von Verbindungsdaten vor und bestärkt somit das Argument, dass von elektronischer Kommunikation zwischen Arzt und Patienten abzuraten ist.
  - Die BMWI-Initiative Sicherheit im Internet behandelt u. a. die Themen: E-Mail-Sicherheit, Förderung von GnuPG, Sicherheit beim Browsen, Förderung von Open-Source-Software.
  - Health Privacy Bibliography (Robert Gellman, EPIC) (Electronic Privacy Information Center)

- Herr Pommerening weist hin auf die Veranstaltungen
  - KIS 2001, 28. - 30. März 2001 in der Westfalenhalle Dortmund,
  - VIS2001, 11. - 14. September 2001 in Kiel.

- Herr Blobel berichtet über die Aktivitäten der Standardisierungsgremien:
  - GMDS AG Standards für Kommunikation und Interoperabilität.
  - DIN NAMed FB G Medizinische Informatik - AA G 4 Sicherheit: Keine eigenen Aufgaben, sondern Weiterleitung an europäische und internationale Gremien.

- CEN TC 251 Health Informatics - WG III Security, Safety, Quality - mit folgenden Ergebnissen:
  - SEC-COM/FR Framework for Security Protection of Health Care, eine Navigationshilfe für Sicherheit,
  - SEC-COM: Security for Health Care, Protokolle für Kommunikationssicherheit,
  - SEC-ID/PASS Secure User Identification for Healthcare: Authentisierung mit Passwort,
  - SEC-ID/CARDS Standard für Authentisierungen mit Smartcards.

  Ferner befasst sich die WG mit u. a. den Themen Qualitätsstandards für Schutz und Sicherheit, Health Security Policies, Data Protection Contract Guide, Access Control Policy Bridging, Anonymisierung, Risk Assessment Procedures.

- ISO TC 215. Hier wird eine PKI for Health entwickelt; ein Final Draft soll im März fertig sein. Weitere Themen sind: ein Thesaurus für Security, Security Framework for Health (global), Secure Access for Electronic Health Care Records.

- Herr Blobel berichtet über das Onconet Sachsen-Anhalt. Es setzt Ergebnisse aus sechs europäischen Projekten um. Es hat die Aufgaben: Aus-, Weiterbildung, Qualitätssicherung, -management, Unterstützung klinischer Studien, Patienteninformierung, virtuelles Gesundheitsnetz. Es beruht auf dem Datenpool des Krebsregisters Sachsen-Anhalt. An Anwendungs- und Kommunikationssicherheit sind implementiert:
  - die HPC mit 3 Schlüsselpaaren zu 1024 Bit (wobei die Schlüssellänge zu Perfomanzeinbußen führt - 4 Sekunden pro Operation, Flaschenhals ist die Schnittstelle zwischen Karte und Leser),
  - Attributzertifikate mit Rolle und Rechten,
  - VPN-Architektur im Internet,
  - sichere Kommunikation über einen Kommunikationsserver (Abholen der Informationen).

  Verwendet wird das GTDS (Gießener Tumor-Dokumentationssystem). Übertragen werden Arztbriefe, freie SQL-Statements, Teile der elektronischen Krankenakte, beliebige Files, zertifizierte Dokumente an Mitarbeiter, Einrichtungen und Patienten. Das Onconet ist deutsches Pilotprojekt des europäischen RESHEN-Projekts (REgional Secure HEalthcare Networks).

- Herr Blobel berichtet ferner über das HARP-Projekt (Harmonization for the security of web technologies and applications). Hier geht es um die sichere Kooperation verteilter Web-Komponenten. Die Sicherheit beruht auf drei Ansätzen:
  - VPN,
  - Benutzerzentrierung: herunterladen einer sicheren Clientkomponente und zertifizierter Dokumente,
  - Serverzentrierung: Sicherheitsumgebung beim Benutzer, sichere Kommunikation mit dem Server; die Funktionalität bleibt auf dem Server.

Maßnahmen zur Realisierung der Sicherheit sind:

- Adressierung von Rechner und Port,
- keine zwei Kommunikationsverbindungen zur gleichen Zeit,
- sorgfältige Administration,
- Rechnerhygiene.

**TOP 4. Status der bisherigen Empfehlungen der AG**

Die AG stimmt überein, dass die Empfehlung zum Internet-Anschluss von Krankenhäusern überarbeitungsbedürftig ist; sie soll zukünftig auch Ärztenetze berücksichtigen. Die im einzelnen diskutierten Änderungs- und Ergänzungsvorschläge werden von Herrn Pommerening eingearbeitet; der Text wird dann zunächst im zugangsgeschützten Bereich »Entwürfe« des AG-Servers abgelegt.

Die Empfehlungen für NT-Netze behalten ihre Gültigkeit im Wesentlichen auch für Windows 2000. Notwendige kleine Änderungen werden bis zur nächsten Sitzung eingearbeitet. Die AG ist der Meinung, dass auch Linux-Server ausführlicher behandelt werden sollten.

Als nächstes Ziel sieht die AG eine Empfehlung zur Handhabung von E-Mail im Gesundheitswesen für wünschenswert an. Sie soll auf der in der vorigen Sitzung diskutierten Stellungnahme für die Präsidiumskommission beruhen; weitere Gesichtspunkte werden gesammelt. Herr Pommerening wird daraus bis zur nächsten Sitzung ein beschlussfähiges Papier zusammenstellen.

**TOP 5. Die Situation des Datenschutzes am Universitätsklinikum Frankfurt**

Herr Kirsten berichtet aus seiner Tätigkeit. Aktuelle Themen sind insbesondere die Verpflichtung des Datenschutzbeauftragten nach dem hessischen Datenschutzgesetz, Schulungen abzuhalten, sowie die Beschlagnahmeproblematik im Zusammenhang mit der Archivierung, aber auch mit dem »Mobile Computing«.

**TOP 6. Von der Ausschreibung zum Verfahrensverzeichnis - Datenschutz gemäß EU-Richtlinie in Marburg**

Verschoben auf die nächste Sitzung.

**TOP 7. IT-Sicherheit an klinischen Arbeitsplätzen**

Verschoben auf die nächste Sitzung.

**TOP 8. Administrator-Verpflichtung**

Verschoben auf die nächste Sitzung.

**TOP 9. Fernwartung und Wartung vor Ort**

Herr Exenberger berichtet über die Konzepte des Technischen Dienstes, Siemens Medizinische Technik, für die Fernwartung. Die AG diskutiert vor diesem Hintergrund die Formulierungshilfen für einen Fernwartungsvertrag aus der Sicht des Datenschutzes, ohne zu

einem übereinstimmenden Meinungsbild zu kommen. Es werden folgende Gesichtspunkte genannt:

- Die Forderung nach festen Listen berechtigter Mitarbeiter ist unflexibel; insbesondere ist die besondere Verpflichtung der Mitarbeiter der »Firma« nicht praktikabel - Anwendung des §5 BDSG (Datengeheimnis) sollte ausreichen.

- Dagegen: Es handelt sich weniger um ein Problem des Datenschutzgesetzes, sondern um ein Problem der ärztlichen Schweigepflicht. Hier wären eine Entlastung des Arztes und eine Mitverantwortung durch Dienstleister im Gesundheitswesen anzustreben. Hierfür sind zurzeit die rechtlichen Grundlagen aber nicht gegeben. Eine Regelung analog der Produkthaftung wäre denkbar.

- Die Fernwartung impliziert eine umfassende Systemkontrolle. Auch für einen halbwegs sachkundigen Mitarbeiter der Klinik wird ein solcher Vorgang von hoher Komplexität im Allgemeinen nicht durchschaubar sein, so dass ein großes Maß an Vertrauen in die fernwartende Firma nötig ist.

- Eine umfangreiche Fernwartung nach dem vorgestellten Konzept bedeutet ein Outsourcing von wesentlichen Administrationsaufgaben. Ein Systemadministrator hat aber eine zentrale Vertrauensstelle innerhalb einer Klinik.

- Der Bayerische Landesdatenschutzbeauftragte schlägt vor, durch einen Passus im Behandlungsvertrag vom Patienten eine Entbindung von der Schweigepflicht als Legitimation für die Fernwartung einzuholen.

- Fernwartung unterscheidet sich von der Wartung vor Ort dadurch, dass Daten den Bereich und somit die Kontrolle der Klinik verlassen und dabei auch nicht mehr vor Beschlagnahme geschützt sind.

- Die bisherigen Regelungen sind in Hinblick auf den rasanten Technologie-Wandel kaum noch durchzuhalten. An Stelle von festgeschriebenen Regelungen sind Policies/Richtlinien nötig, die Vertragsbestandteil werden müssten und deren Einhaltung kontrollierbar sein muss.

- Die »Formulierungshilfen« der AG entsprechen der gegenwärtigen Rechtslage und können daher nicht kurzfristig in ihrer Grundkonzeption geändert werden.

Die AG ist der Meinung, dass zum Thema Fernwartung wie auch allgemeiner zum Outsourcing von technischen Dienstleistungen im Gesundheitswesen grundsätzlicher Diskussionsbedarf auf politischer und standespolitischer Ebene besteht und wird das Thema auch weiterhin behandeln.

**TOP 10. Externe Befundserver**

Verschoben auf die nächste Sitzung.

**TOP 11. Datenschutz-FAQ**

Verschoben auf die nächste Sitzung.

**TOP 12. Telearbeit**

Verschoben auf die nächste Sitzung.

**TOP 13. Verschiedenes**

Die nächste Sitzung soll am 17. und 18. Mai 2001 in Virchow-Klinikum in Berlin stattfinden; Sitzungszeiten 14 - 18 bzw. 9 - 13 Uhr.

---

Protokoll: Prof. Dr. K. Pommerening, 7. 5. 2001, letzte Änderung: 7. 5. 2001
E-Mail: Pommerening@imsd.uni-mainz.de