

Protokoll
der 18. Sitzung der GMDS-Arbeitsgruppe
Datenschutz in Gesundheitsinformationssystemen
am 5. Dezember 2005 in Erlangen

Die Sitzung fand gemeinsam mit der 29. Beratung des GDD-Arbeitskreises "Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen" (AK GSW) im Fraunhofer-Institut für Integrierte Schaltungen IIS statt.

Sitzungszeit: Montag, 5. Dezember 2005, 10:00 Uhr bis 15:35 Uhr

Anwesend: Dr. Blobel, Dr. Brunner, Dobler, Engel, Holst, Dr. Hornung, Kaiser, Kalning, Krause, Dr. Leetz, Dr. Leis, Lolov, Müller, Dr. Münch, Prof. Dr. Nerlich, Pharrow, Prof. Dr. Pommerening, Ruf, Scheiter, Schnabel, Tietze, Dr. Wentz, Werner, Wichterich

Entschuldigt: Erdmann, Gump, Dr. Heidenreich, Dr. Herbst, Prof. Prokosch, Dr. Schug

Tagesordnung:

1. Begrüßung der Teilnehmer, Annahme der Tagesordnung, Protokoll der letzten Sitzung
2. Vorstellung des Fraunhofer IIS
3. Vorträge aus dem AK und der AG
 - a. Die ersten 100 Tage eines IT-Sicherheitsbeauftragten
 - b. Die Modellregion Ingolstadt und das Netzwerk GOIN
 - c. Aktuelle Themen aus der Sicht des Bayerischen Landesbeauftragten
 - d. Datenschutzaspekte bei e-pacs und Datenschutz-Rezertifizierung
4. Mitteilungen aus dem GDD-Arbeitskreis, Diskussion
 - a. Internet im Krankenhaus für Patienten
 - b. Der IT-Sicherheitsbeauftragte im GSW-Unternehmen
 - c. Aktuelle Themen
5. DAFTA 2005 und GMDS 2005
6. Aktuelle Probleme, Gesetze, Veranstaltungen
7. Sitzungstermine, Themen und Orte

TOP 1. Begrüßung der Teilnehmer, Annahme der Tagesordnung, Protokoll der letzten Sitzung

Herr Dr. Blobel begrüßte im Namen der Leitung des Arbeitskreises und des Vorstandes der GDD die Teilnehmer der 29. Beratung des AK GSW sowie die Teilnehmer der 18. Sitzung der AG DGI und dankte den Organisatoren. Anschließend stellten sich alle Teilnehmer kurz vor. Die Tagesordnung, das Protokoll der 28. Sitzung des GDD-AK vom 5. September 2005 in Volmarstein sowie das Protokoll der 17. Sitzung der GMDS-AG vom 15. September 2005 in Freiburg wurden angenommen.

TOP 2. Vorstellung des Fraunhofer IIS

Herr Dr. Blobel stellte in seiner Präsentation den Gastgeber, das Fraunhofer-Institut für Integrierte Schaltungen IIS in Erlangen, sowie die Projektgruppe Gesundheitstelematik vor. Die Präsentation ist auf den Webseiten der AK und der AG verfügbar.

TOP 3. Vorträge aus dem AK und der AG

Die Vorträge werden – soweit verfügbar – auf den Webseiten des GDD-AK und der GMDS-AG zum Download bereitgestellt.

1. Herr Kaiser berichtete über die ersten 100 Arbeitstage in seiner Funktion als IT-Sicherheitsbeauftragter im Klinikum in Erlangen. Stichworte seiner Präsentation waren das Ziel seiner Tätigkeit, die Wege dahin und die Probleme. Dabei stellte er heraus, dass seine Rolle vorerst mehr in der Informationssammlung und der Abgrenzung seines Funktionsrahmens gegenüber der EDV-Abteilung und dem Rechenzentrum besteht. Herr Kaiser ist bereit, zu gegebener Zeit wieder über den Stand seiner Tätigkeit zu berichten.

Herr Prof. Dr. Pommerening fragte nach, ob es bereits ein allgemein gültiges IT-Sicherheitskonzept für das Uniklinikum gibt. Solch ein Konzept hat Herr Kaiser erst einmal hintan gestellt, um aktuell anstehende Probleme Schritt für Schritt zu lösen. Es wird aber zukünftig ein Konzept erstellt werden.

Herr Dr. Hornung wollte wissen, ob es bei der Arbeit in den verschiedenen Abteilungen (Datenschutz/IT) nicht Überschneidungen gibt. Beim Datenschutz gibt es diese nicht – mehr Probleme gibt es mit der IT.

Herr Müller merkte an, dass eine Abgrenzung generell schwierig ist. Deshalb wurde in seinem Haus ein Team für diese Aufgaben gegründet. Dies trifft auch auf andere Häuser zu.

Herr Werner fragte, ob es einen expliziten Kontrollauftrag gibt. Im Auftrag des Klinikvorstandes darf Herr Kaiser alles kontrollieren. Begehungen gibt es nur, wenn polizeiliche Ermittlungen in Kraft getreten sind.

Herr Dr. Münch merkte dazu an, dass es den IT-Sicherheitsbeauftragten mit absoluter Sicherheit auch bald von der gesetzlichen Seite geben wird. Dann wird das Aufgabengebiet klar umgrenzt sein. Dabei wird es um mehr Risikomanagement und Strategie gehen.

Herr Kaiser meinte, dass das Grundschutzhandbuch (GSHB) des BSI für die Klinik keine besondere Relevanz hat. Herr Dr. Blobel bemerkte, dass die Delegation von Funktionen und Verantwortlichkeiten eine immer größer werdende Rolle spielen wird. Herr Dr. Münch wollte abschließend noch wissen, ob es am Klinikum eine ähnliche Einrichtung wie CERT gibt – Herr Kaiser verneinte dies.

2. Der Vortrag von Herrn Dr. Jedamzik musste leider ausfallen, da er nicht anwesend war. Herr Dr. Jedamzik war erkrankt.

3. Frau Scheiter berichtete in ihrer Präsentation über aktuelle Themen aus der Sicht des Bayerischen Landesbeauftragten für den Datenschutz. Dabei berührte sie sowohl das Thema eGK als auch das Thema Jobcard. Sie sprach dabei u.a. über die Ablage von digitalen Daten und die Frage von Archiven und Backup-Lösungen.

Herr Dr. Münch merkte an, dass sich die GDD an der Entwicklung des Konzeptes zur Jobcard beteiligt hat, und fragte, warum man nicht mit Pseudonymisierung arbeitet. Herr Ruf wollte weiterhin wissen, wo sich im Konzept der Jobcard die Selbständigen und Freiberuflern wieder finden. Herr Dr. Blobel wies darauf hin, dass es zukünftig auf jeden Fall zu einer vernetzten Gesellschaft kommen wird. Frau Scheiter erklärte, dass die Jobcard nicht irgendeine Signaturkarte ist, sondern eine Anwendung. Der unglücklich gewählte Name wird sich noch ändern.

Frau Scheiter gab die Anregung, sich zur Information den Tätigkeitsbericht von 2004 von der

Webseite des Bayerischen Landesbeauftragten für den Datenschutz herunter zu laden. Siehe hierzu (<http://www.datenschutz-bayern.de>).

4. Herr Dobler hielt einen Vortrag über externe Langzeit-Archivierung und die Arbeit mit dem Datenschutzgütesiegel des ULD. Er berichtete u.a. über sehr gute Resonanzen bei datenschutzkonformen Lösungen.

Herr Leetz fragte nach, was passiert, wenn die Datenbank defekt ist. Herr Dobler antwortete, dass Backups sowohl beim jeweiligen Kunden als auch beim archivierenden Unternehmen und an einem weiteren sicheren Ort existieren.

Von Seiten der Teilnehmer wurde außerdem danach gefragt, warum nicht der britische Standard (BS 7799) und dessen Zertifizierung benutzt werden. Datenschutz muss juristisch und technologisch gesehen werden, eine separate Betrachtung von Teilen macht wenig Sinn. Deshalb wurde das ULD-Gütesiegel angestrebt und nicht Zertifizierungen seitens des deutschen BSI oder des TÜV-IT. Herr Dr. Münch ergänzte, dass der britische Standard nicht produktbezogen ist.

Herr Dr. Hornung wollte wissen, welcher Schutz für die geheimen Schlüssel existiert. Es ist ein mehrfacher Schutz, da die Schlüssel mehrfach an unterschiedlichen Orten gespeichert und damit geschützt sind. Die Ablage von Bildinformationen in externen Archiven ist auch nicht von einer Zustimmung des Patienten abhängig, da die Daten verschlüsselt gespeichert sind. Es handelt sich also um Auftragsdatenverarbeitung. Das bayrische LKG sieht den Sachverhalt anders, aber der Begriff „Gewahrsam“ sollte hier rechtlich statt technisch interpretiert werden. Letztlich besteht bei einigen Gesetzen aber durchaus Reformbedarf.

Herr Kaiser fragte, was bei Insolvenz geschieht. Die Datenbestände werden nur treuhändisch geführt und im Insolvenzfall komplett an das Krankenhaus zurück gespielt. Herr Dr. Brunner ergänzte, dass wegen des Sachverhalts medizinischer Daten auch der Beschlagnahmeschutz gewährleistet ist. Der Schlüssel befindet sich ohnehin im Krankenhaus und damit in einer medizinischen Umgebung. Frau Scheiter verwies in diesem Zusammenhang auch auf den Tätigkeitsbericht 2004 des bayrischen Landesbeauftragten für den Datenschutz.

Herr Dr. Münch erwähnte die GDD-AK-Sitzung im Oktober 2004 in Zwickau, auf der beteiligte Ärzte ihre Akzeptanz gegenüber dem System deutlich zum Ausdruck gebracht haben (siehe Protokoll der 24. Sitzung). Die Sicht des Arztes ist in diesem Zusammenhang natürlich sehr interessant, da durch das Rückspeichern gewisse Zeitverzögerungen entstehen. Diese liegen im Bereich von einigen Minuten, bremsen nach Aussage der Ärzte die medizinischen Prozesse aber nicht, da beim Wissen um diese Verzögerung andere Tätigkeiten eingebaut werden können.

TOP 4. Mitteilungen aus dem GDD-Arbeitskreis, Diskussion

Herr Dr. Blobel gab eine Einführung zu TOP 4, und Herr Pharow gab anschließend einen Überblick zur Historie der GDD-Mitteilungen.

Zum TOP 4.1 informierte Herr Dr. Leis aus Regensburg die Teilnehmer über die Vorgehensweise am dortigen Uniklinikum. Ende 2003 wurde dort das „Internet am Krankenbett“ eingeführt. Das in Regensburg erstellte Policy-Dokument gleicht von der Struktur her der erarbeiteten GDD-Mitteilung. Für das Klinik- und das Wissenschaftsnetz ist eine Verlegung von zusätzlichen Kabeln nicht vorgesehen. Diese beiden separaten Netze werden abgeschottet vom Internet betrieben. Es schließt sich deshalb aus, das Klinik- oder das Wissenschaftsnetz als Patientennetz zu benutzen. Deshalb existiert ein eigenes Netz für Patienten mit einer DSL-Anschlussverlängerung, externem Provider, Router und Switch. Im Patientenzimmer gibt es einen Umsetzer mit lokalem Switch für das Notebook. Zusätzlich gibt es SurfTable, das nur ein Internet-Frontend darstellt und auf der Basis von embedded LINUX einen Internetbrowser zur Verfügung stellt. SurfTable läuft über das Telefonnetz, kostet pro Tag 4,95 EUR für die Anwendung (trägt sich von selber; kein Gewinn) bzw. 2,95 EUR nur für den Anschluss und bietet Filtermöglichkeiten für den Jugendschutz. Es dient z.B. der Selbst-Information des Patienten bei einer unvermittelt aufgetrete-

Patienten bei einer unvermittelt aufgetretenen Krankheitssituation und unterstützt damit auch die Arbeit des Klinikums. DSL-Provider ist die Firma Schlund & Partner.

Zum TOP 4.2 wurde zusätzlich zum vorliegenden Dokument nur die Anregung gegeben, dass das Zusammenspiel zwischen dem Datenschutz-Beauftragten und dem IT-Sicherheitsbeauftragten mit in das Dokument aufgenommen werden sollte. Dies ist bereits erfolgt, das Dokument wurde in den Dezember-Mitteilungen der GDD veröffentlicht.

Weitere Themen, die demnächst zur Ausarbeitung gelangen könnten, sind die Kooperation mit externen Partnern (Herr Dr. Brunner), Standardvertragsklauseln und Modellverträge sowie die Auswirkung des Antidiskriminierungsgesetzes auf die Prozesse im Gesundheits- und Sozialwesen (Herr Dr. Münch).

TOP 5. DAFTA 2005 und GMDS 2005

Dieser TOP wurde teilweise in den TOP 4 eingeschoben, da Herr Dr. Münch etwas eher zurück reisen musste.

Herr Dr. Münch gab einen Rückblick auf die 29. DAFTA, was auch 29 Jahre BDSG entspricht. Zeitlich bedingt gibt es noch keine Statements von der neuen Regierung. In der Koalitionsvereinbarung gibt es keine neuen Aussagen zum Datenschutz, deshalb wird die bisherige Strategie erst einmal fortgeführt. Auf der DAFTA selbst kam in vielen Beiträgen zum Ausdruck, dass man Spielball der technologischen Entwicklung sei. Nicht umsonst lautete das Leitthema 2005 „Datenschutz – ein Dispositionsfaktor“. Auch die Auftragsdatenverarbeitung spielte eine wesentliche Rolle im DAFTA-Programm 2005. Im Sinne einer datenschutzfreundlichen Technik hat das BSI neue Protection Profiles veröffentlicht. Gut angenommen wurde das Thema "Datenschutz im Hochschulwesen". Als ein neuer Begriff wurde auf der Tagung "Dynaxität" eingeführt, eine Wortschöpfung aus den Begriffen Dynamik und Komplexität.

Kontrovers wurde hingegen die geplante Novelle des BDSG im Hinblick auf die Erhöhung des „Schwellwertes“ für die Bestellung eines DSB von 5 auf 20 Personen gesehen. Dies würde u.a. für viele Einrichtungen im GSW bedeuten, dass die internen und externen DSB verschwinden würden – im Sinne von eGK und GMG sicher das falsche Zeichen. Außerdem würde Deutschland dann entgegen den Richtlinien der EU einen separaten Weg einschlagen.

Herr Dr. Blobel fand lobende Worte zum Spezialsymposium „Gesundheits- und Sozialdatenschutz“ und schätzte es als gelungene Veranstaltung ein. Er äußerte an die Adresse des GDD-Vorstandes zwei Bitten: das Symposium sollte zu einer besseren Zeit stattfinden (insbesondere wegen des in 2005 parallel stattfindenden Plenums), und es sollte über Rabatte für Mitarbeiter des GSW nachgedacht werden.

Herr Pharow berichtete über die GMDS-Jahrestagung 2005, zu der ein Workshop, ein Tutorium, eine Sitzung der GMDS-AG DGI sowie mehrere Beiträge stattfanden. Er erwähnte, dass es für die nächsten Veranstaltungen eine Verpflichtung für die Arbeitsgruppen ist, wieder Beiträge einzureichen und gestalterisch tätig zu werden.

TOP 6. Aktuelle Probleme, Gesetze, Veranstaltungen

Im Rahmen der Arbeit von GDD-AK und GMDS-AG spielen Veranstaltungen eine wesentliche Rolle. Deshalb soll in Zukunft auf den Webseiten von AK und AG regelmäßig über Veranstaltungen und zugehörige Einreichungsaufrufe (Call for Papers) informiert werden.

Veranstaltungen:

- 9. DVMD-Fachtagung zum Thema "Medizinische Dokumentation - wichtig oder nichtig?" am 30. und 31. März 2006 in Erlangen (gemeinsamer Workshop von AK und AG, weitere Programmbeiträge der AG)

- Öffentliche Veranstaltung "Datenschutz und Telematik im deutschen Gesundheitswesen" im Unfallkrankenhaus Berlin (UKB) am 30. Mai 2006 von 10 bis 17 Uhr (gemeinsames Programm von AK und AG)
- 11. Fachtagung "Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS)" vom 31. Mai bis 2. Juni 2006 in Frankfurt/Main (gemeinsamer Workshop von AG und AK)
- ICMCC vom 7. bis 9. Juni 2006 in Den Haag (Beteiligung ist noch zu definieren, geplant sind mehrere Workshops)
- MED-CAST 2006: Workshop in Darmstadt zu Fragen von Medizin und IT-Sicherheit (gestaltet unter Mitwirkung der AG)
- MIE 2006 vom 27. bis 30. August 2006 in Maastricht (mehrere Beiträge, Workshops und Tutorien unter Mitwirkung der AG)
- 51. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) vom 10. bis 14. September 2006 in Leipzig (seitens der AG geplant: Workshop, Tutorium, Beiträge, AG-Sitzung)

Herr Dr. Blobel gab anschließend einige Information zur aktuellen Entwicklung der Standardisierung. Er verwies auf neue ISO- und CEN-Standards (siehe Liste).

Standards:

- ISO 22857: Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information
- ISO 17799: Information technology - Security techniques - Code of practice for information security management Part 1
- ISO 27799: Health informatics - Security management in health using ISO 17799
- ISO 37799: Information technology - Security techniques - Code of practice for information security management Part 2
- ISO 22600: Health informatics - Privilege management and access control (3 Teile)
- ISO 17090: Health informatics - Public key infrastructure (wurde angenommen)
- ISO 21091: Health informatics - Directory services for security, communications and identification of professionals and patients
- ISO 21547: Health informatics - Security requirements for archiving and backup
- CEN ENV 13729: Health informatics - Secure user identification of healthcare - Strong authentication using microprocessor cards (wird neu geschrieben)

Herr Pharow fragte nach, welche Auswirkungen diese Standards für Deutschland haben. Es wird keine Übersetzung vorgesehen ist, das DIN wird jedoch trotzdem einige wesentliche Standards übersetzen wird. Für Deutschland ist nur CEN verbindlich – ISO-Standards können rechtlich nicht erzwungen werden.

Herr Prof. Dr. Pommerening berichtete zum Abschluss noch kurz über das TMF-Projekt Biomaterialbanken, in dessen Rahmen eine umfangreiche rechtliche Analyse durchgeführt wurde. Dabei kam zur Sprache, dass eine Weitergabe von Biomaterial ohne explizite Vereinbarung mit dem Probanden auch eine Unterschlagung ist. Das Thema wird im Moment stark diskutiert. Die GMDS-AG wird die Entwicklung verfolgen.

TOP 7. Sitzungstermine, Themen und Orte

Die nächste offizielle Sitzung des GDD-AK GSW findet am Montag, dem 6. März 2006, ab 10:00 Uhr in Köln statt. Herr Dr. Münch wird der Gastgeber sein.

Die nächste offizielle Sitzung der GMDS-AG DGI wird am 28. und 29. März 2006 in Erlangen stattfinden. Wir bitten Sie in beiden Fällen um rechtzeitige Anmeldung.

Protokoll: Kjeld Engel, 12.01.2006

E-Mail: kjeld.engel@iis.fraunhofer.de

Startseite der Arbeitsgruppe: <http://info.imsd.uni-mainz.de/AGDatenschutz>