

# Sitzung der GMDS-Arbeitsgruppe

## Datenschutz in Informationssystemen des Gesundheitswesens (DGI)

**Ort:** Fachhochschule Mannheim, Gebäude 1, 2. OG, Raum 210

**Datum:** 09.09.2010

**Protokoll:** Bernd Schütze

### Teilnehmer:

Name	Organisation / Institution	eMail	Teilnahme von - bis
Blobel, Bernd	eHCC, Uni Regensburg	bernd.blobel@klinik.uni- regensburg.de	09:00 - 13:00
Drepper, Johannes	TMF e.V.	johannes.drepper@tmf-ev.de	09:00 - 13:00
Hühnlein, Detlef	ecsec GmbH	detlef.huehnlein@ecsec.de	09:30 - 13:00
Isele, Christoph	Siemens	christoph.isele@siemens.com	09:00 - 13:00
Kaiser, Jochen	Uniklinik Erlangen	jochen.kaiser@uk-erlangen.de	09:00 - 11:00
Pommerening, Klaus	IMBEI, Unimedizin Mainz	klaus.pommerening@unimedizin- mainz.de	09:00 - 13:00
Schütze, Bernd	GKD Düsseldorf	schuetze@medizin-informatik.org	09:00 - 13:00
Vaske, Bernhard	MHH	vaske.bernhard@mh-hannover.de	09:00 - 13:00

### Tagesordnung

#### Begrüßung

Um 09:10 eröffnet Herr Pommerening die Sitzung mit einer kurzen Begrüßung. Es folgt eine kurze Vorstellungsrunde der Sitzungsteilnehmer.

#### 1. Formalia (Tagesordnung, Protokoll)

- Die Tagesordnung wird genehmigt.
- Über das Protokoll der letzten Sitzung wird nicht abgestimmt, da von den 5 Teilnehmern der letzten Sitzung nur 2 anwesend sind und die Richtigkeit des Protokolls daher nicht festgestellt werden kann.

#### 2. Empfehlungen der Arbeitsgruppe, insbesondere zur IT-Sicherheit in Krankenhäusern

- Herr Blobel gibt einen Hinweis auf die Arbeitsgemeinschaft der Landesdatenschutzbeauftragten, die sich mit der Abbildung der Datenschutzbestimmungen im KIS befassen und zu diesem Thema organisatorische und technische Gestaltungshinweise verfassen. Sobald diese Ausarbeitungen zur öffentlichen Kommentierung freigegeben sind, wird Herr Pommerening die Ausarbeitungen an die AG-DGI-Mitglieder verteilen, so dass die AG einen Konsens zur Kommentierung erzielen kann, den Herr Pommerening einreicht.
- Herr Blobel weist auf die diversen internationalen Normen hin, die sich mit dem Datenschutz beschäftigen.

- Herr Pommerening stellt die zuvor per E-Mail verteilte Ausarbeitung hinsichtlich der Probleme von vernetzten IT-Systemen vor. Die Präsentation entspricht der des Vortrages vom 12. DICOM-Treffen, d. h., der Vortrag steht unter [http://www.uni-mainz.de/FB/Medizin/Radiologie/agit/berichte/dicom2010/vortrag/IT-Sicherheitsprobleme\\_Vernetzung\\_von\\_Krankenhausern.pdf](http://www.uni-mainz.de/FB/Medizin/Radiologie/agit/berichte/dicom2010/vortrag/IT-Sicherheitsprobleme_Vernetzung_von_Krankenhausern.pdf) zum Download bereit. Einzelne in der Präsentation auftauchende Hinweise werden von der Gruppe diskutiert:
  - Es wird festgestellt, dass nicht alle Datenschutzanforderungen technisch gelöst werden können, sondern nur die Kombination von organisatorischen und technischen Möglichkeiten den Datenschutz gewährleistet. Herr Blobel erinnert an die existierenden Ausarbeitungen der GDD bzgl. Dienstanweisungen.
  - Herr Isele weist darauf hin, dass in Krankenhäusern schon ohne IT oftmals nicht bekannt ist, wer was wann darf. D. h., organisatorisch muss im Krankenhaus einiges geregelt werden, bevor Dienstanweisungen etwas nützen oder IT-Systeme die Umsetzung der Datenschutzvorgaben unterstützen können.
  - Der BSI-Grundschutz wird hinsichtlich seiner Eignung für Krankenhäuser diskutiert. Es herrscht Konsens, dass die Vorgaben für das Krankenhaus angepasst werden müssen. Ohne entsprechendes Management ist eine Sicherheitskultur im Krankenhaus kaum umzusetzen.
  - Es erfolgt ein Hinweis auf die Netzaufteilung entsprechend IEC 80001 in die 3 Schutzklassen.
  - Es wird darauf hingewiesen, dass heute Medizingeräte oftmals einen Zugang zum Internet benötigen, ohne dass dies vom Hersteller dokumentiert wird oder beschrieben wird, wie der Netzzugang aussehen muss.
  - Alle sind sich darüber einig, dass eine unverschlüsselte E-Mail keine Patientendaten beinhalten darf.
  - Eine Fernwartung ohne VPN sollte nicht unverschlüsselt erfolgen. Herr Kaiser weist darauf hin, dass NetViewer / Teamviewer über einen in der Klinik aufgestellten Server erfolgen kann. Die Kosten hierzu liegen unter 50.000 € für ein Universitätsklinikum.
- Herr Pommerening bittet die Arbeitsgruppe um Kommentierung der Ausarbeitung. Die Zielrichtung der Ausarbeitung ist die Praxisorientierung, d. h., es soll eher eine Praxishilfe in der Klinik darstellen als eine wissenschaftliche Abhandlung.
- Herr Drepper fragt bzgl. der vorgestellten Auftrennung der Kliniknetze an, wie der Single-Source-Ansatz bei Forschungsprojekten hier hineinpasst.
  - Dies ist im Konzept implizit enthalten, da die Aufteilung entsprechend der Sicherheitsanforderungen erfolgt, d. h., auf für die Forschung benötigte Daten kann zugegriffen werden.

### **3. Weiteres Arbeitsprogramm der Arbeitsgruppe**

- Aufteilung der anstehenden Arbeiten an die Mitglieder der Arbeitsgruppe
  - Praktisch alle von der AG angefertigten Dokumente, Empfehlungen usw. müssen überarbeitet oder von Grund auf neu geschrieben werden.
  - Bitte eine Mitteilung eines jeden Mitgliedes der AG DGI an Herrn Pommerening, die beinhaltet:
    - Welches Thema muss aus Sicht des jeweiligen AG-Mitgliedes von unserer AG dringend behandelt werden?
    - Zu welchem Thema bringt man eine Expertise mit?
- Webseiten
  - Auf der GMDS-Internetseite ([www.gmds.de](http://www.gmds.de)) wurde bis vor kurzem immer noch auf die Seiten hingewiesen, die seit 2008 nicht mehr aktualisiert wurden. Herr

Pommerening hat bei der GMDS einen neuen Internetauftritt der AG eingerichtet, der noch ausgebaut werden sollte. Die alten Webseiten bleiben bestehen, damit die Historie der AG-Arbeit verfolgt werden kann. Herr Blobel richtet auf der Startseite des alten Auftritts einen Link zur neuen Webseite ein.

- Mailverteiler
  - Herr Blobel überträgt Herrn Pommerening administrative Rechte für den Mailverteiler, so dass Herr Pommerening Aktualisierungen durchführen kann.
- Nächstes Treffen

Die nächste Sitzung soll im Frühjahr 2011 stattfinden. Zur Diskussion stehen folgende Möglichkeiten

  - Gemeinsames Treffen mit dem GDD-Arbeitskreis Gesundheitswesen im März
  - Tagung auf der conhIT. Herr Schütze wird auf Grund der auf der diesjährigen conhIT gesammelten Erfahrungen seitens seines Arbeitgebers nicht mehr die conhIT besuchen können und bittet darum, dann ein Treffen außerhalb des Messegeländes zu veranstalten. Herr Isele bietet ein Treffen in den Räumlichkeiten von Siemens in Berlin an.
  - Gemeinsames Treffen mit der TMF Arbeitsgruppe Datenschutz (AG DS)

#### **4. Berichte**

- Herr Blobel zeigt eine Präsentation bzgl. der Abbildung einer rollenbasierten Rechteverwaltung zur Abbildung der datenschutzrechtlichen Anforderungen, basierend auf ISO/TS 22600 und ISO/TS 21298.
  - Herr Drepper weist darauf hin, dass die in der von Herrn Blobel genutzten bzw. im Standard enthaltenen Begrifflichkeiten (funktionelle/strukturelle Rolle) auch seitens der Gematik genutzt und teilweise auch im SGB verwendet werden, allerdings in einer anderen Interpretation. D. h., bei der Verwendung dieser Begrifflichkeiten sollte immer eine kurze Erläuterung erfolgen, um Missverständnisse zu vermeiden.
  - Da Herr Blobel aus zeitlichen Gründen nur eine kurze Übersicht geben konnte, bietet er an, auf dem nächsten Treffen eine detailliertere Darstellung zu präsentieren, vorausgesetzt, ihm wird ein entsprechender Zeitrahmen eingeräumt.
  - Herr Blobel verschickt eine Kurzzusammenfassung bzw. eine Zusammenstellung der relevanten Folien seines Vortrages an die Mitglieder der AG.

#### **5. Verschiedenes**

Fiel aus zeitlichen Gründen aus.