

# Sitzung der GMDS-Arbeitsgruppe

## Datenschutz in Informationssystemen des Gesundheitswesens (DGI)

**Ort:** Veranstaltungsräume der TMF, Georgenstraße 22, 10117 Berlin

**Datum:** 27. 3. 2011, 13:00 – 18:00 Uhr

**Protokoll:** J. Drepper, B. Schütze, K. Pommerening

**Webseite:** <http://www.imbei.uni-mainz.de/AGDatenschutz/>

### Teilnehmer:

Name	Organisation / Institution	eMail
Birkle, Markus	Uni Heidelberg	markus.birkle@med.uni-heidelberg.de
Blobel, Bernd	eHCC, Uni Regensburg	bernd.blobel@klinik.uni-regensburg.de
Brunner, Manfred	UK Erlangen	manfred.brunner@uk-erlangen.de
Christoph, Jan	UK Erlangen	jan.christoph@uk-erlangen.de
Drepper, Johannes	TMF e.V.	johannes.drepper@tmf-ev.de
Ganslandt, Thomas	UK Erlangen	thomas.ganslandt@uk-erlangen.de
Isele, Christoph	Siemens	christoph.isele@siemens.com
Pommerening, Klaus	IMBEI, Uniklinik Mainz	pommeren@uni-mainz.de
Schütze, Bernd	GKD Düsseldorf	schuetze@medizin-informatik.org
Vaske, Bernhard	MH Hannover	vaske.bernhard@mh-hannover.de

### Tagesordnung

#### I. Gemeinsamer Sitzungsblock der AG DGI mit der AG DS der TMF

1. Bericht zum TMF-Projekt V039-03: Fortschreibung der generischen Datenschutzkonzepte der TMF
2. Softwaregestütztes Einwilligungsmanagement
3. Rechtliche Rahmenbedingungen für die Forschung mit Patientendaten in Krankenhäusern in den Bundesländern
4. Eckpunktepapier der Datenschützer zu technischen Anforderungen an KIS

#### II. Sitzung der AG DGI

1. Formalia (Tagesordnung, Protokoll)
2. Empfehlungen der Arbeitsgruppe
3. Veranstaltungen
4. Rollenbasierte Rechteverwaltung
5. Verschiedenes

### Teil I. Gemeinsamer Sitzungsblock der AG DGI mit der AG DS der TMF

Herr Pommerening begrüßt die zum gemeinsamen Sitzungsteil hinzugekommenen Teilnehmer der GMDS-AG „Datenschutz in Gesundheitsinformationssystemen“ (AG DGI) und stellt die geplante Agenda vor.

## **TOP 1. Bericht zum TMF-Projekt V039-03: Fortschreibung der generischen Datenschutzkonzepte der TMF**

Herr Pommerening erläutert die Motivation für die Überarbeitung der generischen Datenschutzkonzepte der TMF und stellt den aktuellen Stand des hierzu schon länger laufenden Projekts vor. Das Projekt sei deutlich in Verzug, nun stehe aber das Konzept und es stünden im Wesentlichen noch redaktionelle Arbeiten und die Abstimmung mit den Datenschützern aus (Folien auf Webseite).

## **TOP 2. Softwaregestütztes Einwilligungsmanagement**

Herr Birkle dankt für die Einladung und die Gelegenheit, hier die konzeptuellen und technischen Lösungen aus Heidelberg zum Einwilligungsmanagement vorstellen zu können. Hintergrund dieser Entwicklung sei u. a. auch die in Heidelberg entwickelte Persönliche einrichtungsübergreifende elektronische Patientenakte (PEPA) gewesen. Man habe jedoch unterschiedliche Anwendungsfälle und infrastrukturelle Rahmenbedingungen adressieren wollen, weshalb sowohl Lösungen für einen zentralen wie auch einen dezentralen Ansatz zum Einwilligungsmanagement entwickelt worden seien (Folien auf Webseite).

Herr Semler fragt nach den bisherigen Erfahrungen, insbesondere mit der zentralen Lösung und der hier offensichtlich voreingestellten „Nulleinstellung“, die ja zu einem sehr aufwändigen Dokumentationsprozess führen könne, da vermutlich häufig viele Optionen der Einwilligung einzeln aktiviert werden müssten. Herr Birkle weist zunächst darauf hin, dass bisher nur die dezentrale Variante des Einwilligungsmanagements in Heidelberg umgesetzt sei. Die Nulleinstellung gehe auf die Diskussion mit den Datenschützern zurück. Hierzu fehle noch die Erfahrung, er könne die Skepsis jedoch nachvollziehen. Bei der aktuell umgesetzten dezentralen Lösung reiche häufig das Setzen eines Häkchens für die Dokumentation, die Akzeptanz sei entsprechend hoch.

Herr Semler führt aus, dass man gerade im Kontext der Nutzung von Biobanken für die Forschung die Erfahrung mache, dass immer häufiger extrem differenzierte Einwilligungen von Ethikern und Datenschützern gefordert würden. So sollten Probanden detailliert angeben können, für welche Forschungsfragestellungen ihre Proben verwendet werden dürften und für welche nicht. Es sei jedoch aus seiner Sicht illusorisch anzunehmen, dass so differenzierte Antwortmöglichkeiten immer auch zu einem differenzierten Entscheidungsprozess führten. Vielmehr werde die Gefahr größer, dass in der Menge der weniger wichtigen Optionen die eigentlich entscheidenden Fragen für die Patienten untergingen.

Herr Birkle teilt die Sorge, dass man mit einer Vielzahl maximal differenzierter Policies den Patienten im Regelfall wohl nicht gerecht werde. Allerdings könne man heute, z. B. auf Basis von XACML, technisch jede noch so differenzierte Lösung umsetzen. Daher müssen man die Diskussion um patientengerechte Lösungen nicht auf technischer, sondern allein auf inhaltlicher und ethischer Ebene führen. Herr Harnischmacher stimmt dem zu, man dürfe Patienten nicht überfordern. Eventuell müssten Ärzte den Einwilligungsprozess auch im Sinne der Patienten stärker steuern, was jedoch wiederum eine Reihe ethischer Fragen aufwerfe. Es gebe hierfür wohl keine einfachen Lösungen. Herr Brunner erinnert in diesem Zusammenhang daran, dass Ärzte im Regelfall nicht über die für einen immer differenzierteren Aufklärungs- und Einwilligungsprozess nötige Zeit verfügten.

Herr Blobel sieht allerdings auch eine große Chance in den neuen Möglichkeiten. Es sei zwar aufwändig, aber man sei nun gezwungen, sich mit Policies auseinanderzusetzen und die Standardisierung voran zu bringen. Allerdings gebe es auch schon eine Reihe von Vorarbeiten, wie z. B. den Standard ISO 22600 „Privilege management and access control“. Bei internationaler Betrachtung des Themas zeige sich auch ein starker kultureller Einfluss auf die jeweils favorisierten Lösungen. In vielen Ländern würde z. B. das Opt-Out-Prinzip bevorzugt, was aber in Deutschland offenbar wenig Akzeptanz bei Ethikern und Datenschützern finde.

Zur technischen Umsetzung fragt Herr Blobel, ob die Consent Communication auf Basis einfacher binärer Flags der Differenziertheit der Fragen angemessen sei. Hierfür gebe es auf Basis von CDA und HL7 Version 3 weiterführende Lösungen. Vor dem Hintergrund frage er sich auch, warum man sich auf die Möglichkeiten HL7 Version 2 beschränke. Herr Birkle antwortet, dass die Unterstützung von Version 3 in den Primärsystemen noch zu selten sei. Selbst CDA würde nicht von allen Systemen der relevanten Partner in den verschiedenen Projekten im Raum Heidelberg unterstützt. Herr Blobel verweist auf die Möglichkeit, Adapter zu entwickeln und einzusetzen. Bezüglich der Umsetzung auf Basis von CDA sei auch der HL7-Standard „Patient Consent Directive“ von Interesse. Hier passiere derzeit auf internationaler Ebene sehr viel.

Herr Drepper fragt nach der Abbildung des Rückzugs einer Einwilligung, insbesondere bei Verwendung des dezentralen Ansatzes. Herr Birkle räumt ein, dass dies beim dezentralen Ansatz noch manuelles Eingreifen erfordere. Dies lasse sich in einer zentralen Lösung deutlich besser abbilden. Herr Drepper fragt zudem, ob bei einer zentralen Lösung die Speicherung der abgelehnten Optionen in einer Einwilligung oder des Widerrufs möglicherweise ein Problem darstellen könnte. Herr Birkle antwortet, dass hierfür verschiedene Lösungen möglich wären.

Herr Lablans spricht ebenfalls den Umstand an, dass bei einer zentralen Lösung sensible Informationen an einer zentralen Stelle gesammelt werden. Ein solcher Server sei als Single Point of Failure (SPF) anzusehen und das Beispiel des jüngst gehackten Servers der Firma Comodo, die u. a. SSL-Zertifikate herausgebe, zeige, dass kein Rechner vollständig abgesichert werden könne. Herr Birkle antwortet, dass ein solcher Server auch als Cluster und ggf. auch verteilt auf mehrere Standorte implementiert werden könne. Zudem könne der Zugang und die Kommunikation über elektronische Signaturen oder wenn verfügbar auch über Hardware-Token abgesichert werden. Dies sei immer eine Frage der Verhältnismäßigkeit. Herr Blobel weist darauf hin, dass man international eher zu dezentralen Strukturen tendiere. Zentral würde nur noch ein Policy Enforcement Point vorgesehen, alle weiteren Informationen würden dezentral gespeichert.

### **TOP 3. Rechtliche Rahmenbedingungen für die Forschung mit Patientendaten in Krankenhäusern in den Bundesländern**

Herr Schütze stellt seine Rechercheergebnisse zu den Nutzungsmöglichkeiten medizinischer Daten für Forschung und Qualitätssicherung vor. Insbesondere geht er dabei auf die unterschiedlichen Landeskrankengesetze und deren Regelungen zur internen und externen Nutzung von Patientendaten ein (Folien auf Webseite).

Herr Drepper zeigt sich verwundert, dass an einigen Stellen nicht zwischen Pseudonymisierung und Anonymisierung unterschieden werde. Herr Schütze stimmt dem zu, diese Begriffe würden in den unterschiedlichen Gesetzen z. T. uneinheitlich verwendet. Auf die Nachfrage von Herrn Brunner, ob eine interne Nutzung auch bei Klinikkonzernen immer auf das einzelne Krankenhaus bezogen bleibe, bestätigt Herr Schütze dies, es gebe kein Konzernprivileg.

Herr Semler dankt für den guten Überblick, dies seien auch für die TMF spannende Ergebnisse, insbesondere auch für eine Reihe von Projekten an der Schnittstelle zwischen Versorgung und Forschung. Herr Brunner ergänzt, dass gerade für retrospektive Forschungsfragestellungen oft keine andere Möglichkeit als die dezentrale Auswertung in den einzelnen beteiligten Häusern existiere, da keine weiterreichenden Einwilligungen der Patienten vorlägen. Hierfür sei die Kenntnis der einschlägigen Gesetze jedoch wichtig. Herr Schütze merkt an, dass solche Fragen auch Auslöser für seine Recherche gewesen seien. Zudem seien seiner Erfahrung nach auch die Regelungen zum Outsourcing hoch relevant, da dies oftmals aus finanziellen Gründen für Krankenhäuser attraktiv sein könne. Allerdings sei es nicht überall erlaubt.

## **TOP 4. Eckpunktepapier der Datenschützer zu technischen Anforderungen an KIS**

Herr Pommerening schlägt aus Zeitgründen vor, diesen TOP auszulassen, aber die Folien als Protokollanhang auf die Webseite zu stellen (s. Webseite). Herr Isele weist darauf hin, dass das Papier mittlerweile veröffentlicht und auch im Web öffentlich zugreifbar sei (<http://www.datenschutz-bayern.de/technik/orient/oh-kis.pdf>). Es wird festgestellt, dass das Papier direkt nicht rechtlich bindend sei, man müsse aber davon ausgehen, dass es den State of the Art prägen werde.

Herr Pommerening dankt allen Teilnehmern für die vielen Beiträge und die rege Diskussion und schließt den gemeinsamen Sitzungsteil der beiden AGs.

## **Teil II. Sitzung der AG DGI**

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

- Die Tagesordnung wird genehmigt.
- Das Protokoll der letzten Sitzung wird angenommen.

### **TOP 2. Empfehlungen der Arbeitsgruppe**

#### **a) zur IT-Sicherheit in Krankenhäusern**

Zu dieser Empfehlung, die bereits auf der vorigen AG-Sitzung diskutiert wurde, gibt es keine neuen Gesichtspunkte. Sie soll auf den Web-Seiten der AG veröffentlicht werden. Ein Hinweis darauf soll in den GMDS-Mitteilungen erscheinen.

#### **b) zu dem Eckpunktepapier „Orientierungshilfe 'Krankenhaus-Informationssysteme (KIS) datenschutzgerecht gestalten und betreiben'“ der Arbeitskreise Technische Grundsatzfragen sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.**

Herr Pommerening erhielt verschiedene Kommentare, die er zu einer Stellungnahme der AG zusammengefasst hat. Diese wurde an die Arbeitskreise Technische Grundsatzfragen sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weitergereicht.

Die Stellungnahme wird auf der GMDS-Webseite der AG veröffentlicht mit Hinweis in den GMDS-Mitteilungen. Herr Blobel fragt nach, was mit den Webseiten der AG in Regensburg geschehen soll. Es wird beschlossen, die Arbeitsgruppenergebnisse der früheren Jahre in Regensburg zu belassen und von der aktuellen GMDS-Webseite zu verlinken, Nach der offiziellen Veröffentlichung der Orientierungshilfe können weitere Stellungnahmen abgegeben werden. Im Beschluss der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (16./17. März 2011 in Würzburg) steht „Die Konferenz nimmt die Orientierungshilfe zustimmend zur Kenntnis.“ Links dazu:

- [http://www.sachsen-anhalt.de/fileadmin/Elementbibliothek/Bibliothek\\_Politik\\_und\\_Verwaltung/Bibliothek\\_LFD/PDF/binary/Service/orientierungshilfen/OH\\_KIS/DSK\\_81-KIS.pdf](http://www.sachsen-anhalt.de/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_LFD/PDF/binary/Service/orientierungshilfen/OH_KIS/DSK_81-KIS.pdf)
- <http://www.lfd.m-v.de/dschutz/beschlue/entsch81.html#nr6>
- [http://www.lda.brandenburg.de/sixcms/detail.php?gsid=bb1.c.245455.de&template=aktuelle\\_d1](http://www.lda.brandenburg.de/sixcms/detail.php?gsid=bb1.c.245455.de&template=aktuelle_d1)

Derzeit ist die Orientierungshilfen zugänglich unter

- Bayern  
<http://www.datenschutz-bayern.de/technik/orient/patdatkh.html>
- Brandenburg  
[http://www.lda.brandenburg.de/sixcms/detail.php?template=lda\\_info\\_d](http://www.lda.brandenburg.de/sixcms/detail.php?template=lda_info_d)

- Hessen  
[http://www.datenschutz.hessen.de/download.php?download\\_ID=229&download\\_now=1](http://www.datenschutz.hessen.de/download.php?download_ID=229&download_now=1)
- NRW  
[https://www.ldi.nrw.de/mainmenu\\_Datenschutz/submenu\\_Technik/Inhalt/TechnikundOrganisation/Inhalt/Krankenhausinformationssysteme/Orientierungshilfe\\_KIS.pdf](https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Krankenhausinformationssysteme/Orientierungshilfe_KIS.pdf)
- Rheinland-Pfalz  
[http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=081\\_kis](http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=081_kis)
- Sachsen-Anhalt  
<http://www.sachsen-anhalt.de/index.php?id=48464>

### **TOP 3. Veranstaltungen**

- Die Deadline zur Beitragseinreichung für die GMDS-Jahrestagung läuft noch bis zum 15. April 2011. Es wird begrüßt, wenn die Mitglieder der AG noch Beiträge zu unserem Fachgebiet einreichen. Weitere Informationen unter:  
<http://www.mainz2011.de/>.
- Auf der GMDS-Tagung sind zwei Datenschutz-Tutorien geplant:
  - Datenschutz in der medizinischen Forschung (Pommerening)
  - Datenschutz und Datensicherheit in verteilten Netzen (Blobel)
- Herr Pommerening berichtet, dass der Call for Paper für die Tagung „perspektive - Sichere Informationstechnologie für das Gesundheitswesen von morgen“ erfolgt ist.
  - Deadline ist der 08.05.2011
  - Die AG ist Mitveranstalter; daher wäre eine Einreichung eines AG-Mitglieds wünschenswert

### **TOP 4. Rollenbasierte Rechteverwaltung**

Herr Blobel berichtet über die Möglichkeiten der rollenbasierten Rechteverwaltung entsprechend ISO 22600 und ISO 21298. Die Folien der Präsentation werden nachgereicht.

### **TOP 5. Verschiedenes**

Die nächste Sitzung der AG soll auf der GMDS-Jahrestagung 2011 in Mainz stattfinden.