GMDS - Deutsche Gesellschaft für Medizinische Informatik,
Biometrie und Epidemiologie e.V.
Industriestraße 154
D-50996 Köln

Tel.: +49 (2236) 3319958
Fax: +49 (2236) 3319959
Email: info@gmds.de
http://www.gmds.de

Vereinsregister: VR 16225 Amtsgericht Köln

Umsatzsteuer-Identifikationsnummer:
27.07.02 DE 182645846

# GMDS-AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“

## Protokoll für die Sitzung vom 19. November 2014

Protokoll erstellt durch: B. Schütze

## Teilnehmerliste

| Name | Anwesend | Abgesagt | Keine Rückmeldung |
|---|---|---|---|
| Alkemade, Jan | | | X |
| Bahls, Thomas | | | X |
| Blobel, Bernd | | | X |
| Brenner, Hubert | | | X |
| Brunner, Manfred | | | X |
| Bürger, Norman | X | | |
| Drepper, Johannes | X | | |
| Isele, Christoph | X | | |
| Lautenbacher, Heinrich | | X | |
| Pommerening, Klaus | X | | |
| Sax, Ulrich (Pate AG) | | | X |
| Schütze, Bernd | Y | | |
| Schwanke, Jens | | X | |
| Stahmann, Alexander | | | X |
| Wichterich, Eric | | | X |
| Wunschel, Stefan | X | | |

## Top 1: Biobank der Protein Research Unit Ruhr within Europe (PURE)

- PURE = Biometerialdatenbank für epidemiologische Fortschung
- Gespeichert wird Biomaterial und medizinische Daten
- Das PURE-Datenschutzkonzept beinhaltet
    - Rechtekonzept
    - Pseudonumisierungsverfahren (symmetrisch für Rückverfolgbarkeit)

## Top 2: Sekundärdatennutzung am Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS)

- Projekt beinhaltet die Sekundärnutzung von Krankenkassendaten
- Abrechnungsdaten von 4 gesetzlichen Krankenversicherungen werden genutzt, dies beinhaltet die Daten von etwa 20% der gesetzlich Versicherten
- Forschungsschwerpunkt ist die Arzneimittelforschung
- Einmal jährlich erfolgt eine Datenextraktion der Krankenkassen, wobei die Daten in einer gemeinsamen Forschungsdatenbank gespeichert werden
    - Daten stehen für alle Forschungen zur Verfügung, d.h. die Daten werden zunächst ohne einen spezifischen Forschungszweck gesammelt; zu Datensammlung dient eine „universelle“ Zweckbestimmung:
      „Untersuchung von Einsatz, Sicherheit und Wirksamkeit von Arzneimittel und Impfstoffen in der Routineanwendungin einer Krankenversorgung“
    - Für ein spezifisches Forschungsvorhaben wird ein Antrag gestellt und nach erfolgter Genehmigung des Projektes aus BIPS die zur Beantwortung der Forschungsfrage notwendigen Daten extrahiert und an die Forscher übergeben
- Mittelfristig soll §75 SGB X geändert werden; ein Vorschlag wurde vom BIPS-Team 2011 in Abstimmung mit dem Bremer Datenschutzbeauftragten erarbeitet und wurde 2014 an die Länder verteilt → Ziel ist eine Bundesratinitiative zur Änderung des §75 SGB X

## Top 3: Biomaterialbank für Bronchialkarzinome am Klinikum Kassel

- Verbindung medizinischer Daten aus dem onkologischen Informationssystem GTDS mit den Daten einer Biomaterialdatenbank über einen Datentreuhänder

## Top 4: Register der Deutschen Gesellschaft für Allgemein- und Viszeralchirurgie (DGAV)

- Vorstellung der Qualitätsinitiative der DGAV insbesondere des StuDoQ-Registers (http://www.dgav.de/studoq.html)
- Aktuell soll Datenschutzkonzept überarbeitet werden mit dem Ziel, einer „Abnahme“ durch die TMF

## Top 5: DZHK: Translational Registry for Cardiomyopathies (Torch)

- Modular aufgebaute Patienten-Aufklärung
- Treuhand und Datenhaltung ist getrennt
- Monolithische SecuTrial-Anwendung (http://www.secutrial.com/) als Client-/Server-Lösung im Einsatz

## Top 6: Aktualisiertes Konzept des Mukoviszidose Registers

- Überarbeitung des vorhandenen Projektes mit Hinblick auf Klarstellung von
    - Vorgaben bei Datenweitergabe
    - Umgang mit Widerruf
    - Klarstellung der Unabhängigkeit des Treuhänders
    - Usw.

## Top 7: Bericht aus der TMF

Herr Semmler berichtet über die datenschutzrelevanten Aktivitäten der TMF aus dem Jahr 2014 und weist auf einzelne für 2015 geplante TMF-Veranstaltungen hin.

## Top 8: Auftragsdatenverarbeitung

### *8.1 Stellungnahme zur Auftragsdatenverarbeitung mit Gesundheitsdaten (beteiligt: BvD, bvitg, GDD, GMDS)*

- Gemeinsames Projekt bvitg, BvD, GDD und unsere AG
- Stand
    - Initialtreffen am 10. Juli 2014, Ergebnisse

a) Alle Verbände sind der Meinung, dass die Erarbeitung eines Muster-ADV-Vertrages sinnvoll ist
    - Grundlage soll der bitkom-Vertrag sein
b) BvD, GDD und GMDS sind sicher, dass eine Stellungnahme bzgl. §203 StGB erforderlich ist, bvitg muss hierzu Mitglieder befragen
    - Evtl. Änderungsvorschlag zu §203 StGB erarbeiten

- 1. Workshop am 12. August 2014
    a) Gemeinsame Überarbeitung des bitkom-Muster-ADV-Vertrages im Hinblick auf notwendige Änderungen und Ergänzungen
    b) Vorschläge bzgl. der identifizierten Änderungen und Ergänzungen werden von den AG Mitgliedern erarbeitet und bilden Grundlage für den 2. Workshop
- 2. Workshop am 26. September 2014
    a) Zwischen 12.08. und 26.09. wurde Überarbeitung durch die Arbeitsgruppe durchgeführt und Ergebnisse an den bvitg zwecks „Einsammlung“ gemailt
    b) Beim Treffen Abstimmung der Ergebnisse und Abgleich auf ein gemeinsames Dokument
- Kommentierungsphase endete am 31. Oktober 2014, zur Kommentierung wurde angefragt
    a) Arbeitsgemeinschaft Kommunaler Großkrankenhäuser (akg)
    b) Arbeitskreis der Leiter der Klinischen Rechenzentren der Universitätskliniken Deutschland (ALKRZ)
    c) Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Arbeitskreis Medizin
    d) Bundesverband der Krankenhaus IT-Leiterinnen / Leiter e. V. (KH-IT)
    e) Bundesverband Gesundheits-IT e.V. (bvitg)
    f) Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
    g) Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS), Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)
    h) Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“
    i) Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF)
- Viel Zustimmung und positives Feedback ohne schriftliche Kommentierung (BvD, GDD), insgesamt 76 zu bearbeitende Kommentierungen
- 3. Workshop am 25. November 2014 in Berlin
    - Überarbeitung Kommentare
    - Finalisierung angestrebt

### *8.2 Aktuelle Aktivitäten bzgl. der Fortentwicklung des von BvD und GDD entwickelten Datenschutzstandards DS-BvD-GDD-01 hinsichtlich der „Anforderungen an Auftragnehmer nach § 11 BDSG“*

- Von BvD und GDD entwickelter Datenschutzstandards zur Prüfung von Auftragsdatenbearbeitern
- DIN EN ISO 19011:2011-12 „Leitfaden zur Auditierung von Managementsystemen“ wurde bei Entwicklung nicht berücksichtigt
- Entwicklung initiiert von Aufsichtsbehörde NRW, Ergebnis vom LDI NRW „befürwortet“
- URL: http://www.dsz-audit.de/
  Download des Standards: http://www.dsz-audit.de/datenschutzstandard/
- 9 Kernmodule, darunter
    - Leistungsbeschreibung
    - Input- und Output-Management
    - Auftragsmanagement
    - Datenschutzkonzept
- 2 ergänzende Module
    - Vertragsbewertung
    - Beendigung der Leistungsbeziehung
- Kosten für Auftragnehmer: ~ 10.000 bis 20.000 €
    - Kosten für Zertifikaterteilung (Erstzertifizierung): 5.100 €
    - Zu erbringende Dienstleistung bei Auditierung: 64 Stunden (Preis Verhandlungssache)

- Aktuell Weiterentwicklung
  - Ausschreibung September 2014
  - Zielsetzung
    - Anpassung des Datenschutzstandards DS-BvD-GDD-01 an technische oder rechtliche Änderungen
    - Ergänzung von Best-Practice-Beispielen
    - Schaffung von bereichsspezifischen Modulen
    - Entwicklung neuer Datenschutzstandards
    - Mitarbeit bei anderen Zertifizierungsprojekten
  - Bereichsspezifische Module: z.B. **Medizin**, Personal, Steuern, Kunden

## Top 9: Stellungnahme der GMDS zum Referentenentwurf ITSiG sowie Abstimmung weiteres Vorgehen bzgl. IT-Sicherheitsgesetz

- 18.08.2014: Überarbeitung Entwurf vorgestellt (http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html)
- Geschäftsstelle prüft derzeit, wie unsere Kommentierung am besten plaziert wird
- Entwurf enthält viele Unklarheiten
  - Für wen gilt das Gesetz? Wer betreibt eine „kritische Infrastruktur“?
  - Unklare Begriffsbestimmungen wie bspw. „Stand der Technik“
  - Pflicht zur Selbstanzeige, aber keine Befreiung bzgl. StGB, OWG oder stopp wie sie im §42a BDSG („Informationspflicht“ vorhanden ist
  - Unklarer Verwendungszweck der bei den geforderten Meldungen von Sicherheitsvorfällen angefallenen Daten
  - Einführung einer „Vorratsdatenspeicherung“:
    - §100 Abs. 1 TKG erlaubt Speicherung von Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer
    - §15 Abs. 8 TMG erlaubt die Erhebung und Verwendung von Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen
  - BKA kann bei Antragsdelikten §§ 202a, 202b, 202c StGB direkt ermitteln, d.h. Antrag muss nicht vorliegen (Für uns relevant?)
- KRITIS: Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
  http://www.kritis.bund.de/
- KRITIS veröffentlichte im Juni 2014 Aufruf zur Fortschreibung des UP KRITIS
  (UP KRITIS = UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen -Grundlagen und Ziele)
- Eine bei KRITIS genannte „kritische Infrastruktur“ ist das Gesundheitswesen
- Mitgliedschaft KRITIS
  - Aufnahme bei UP KRITIS erfolgt zunächst als Teilnehmer
  - Bei Wunsch zur aktiveren Mitarbeit kann eine Organisation dann Partner im UP KRITIS werden
  - Zusammenarbeit im UP KRITIS = zwei Formen
    - operativ-technischen Zusammenarbeit zwischen allen Teilnehmern des UP KRITIS
    - strategisch-konzeptionellen Zusammenarbeit in den eingerichteten Gremien
- Frage: sollen wir (also GMDS in Form unserer AG) uns an UP KRITIS beteiligen?
  - Wenn ja: wer beteiligt sich aktiv an der Arbeit = Entwicklung eines branchenspezifischen Sicherheitsstandards für das Gesundheitswesen

→ Zeitnah wird per Mail in der AG nachgefragt, wer aus der AG Interesse an der Mitarbeit bei der Entweicklung eines brancheninternen IT-Sicherheitsstandards für das Gesundheitswesen hat.

## Top 10: Abstimmung weiterer Aktivitäten der beiden AGs

### *10.1 Entwicklung einer Empfehlung zum Einsatz von mobilen Geräten im Krankenhaus? Umgang mit Apps? Evtl. gemeinsamer Workshop mit der GDD?*

- Hintergrund: Workshop auf der GMDS-Jahrestagung zeigte Verunsicherung bzgl. Umgang mit dem Thema

- Von Seiten der Mitglieder der GMDS-AG besteht momentan kein Interesse an der Ausarbeitung einer derartigen Empfehlung.

### *10.2 Workshop Pseudonymisierung?*

- Hintergrund: Mehrfache Nachfargen auf GMDS-Jahrestagung bzgl. des Umgangs mit der Pseudonymisierung – das Vorgehen selbst, also die technische Umsetzung, ist dabei allen klar, vielmehr geht es um die Identifizierung der Daten, die behandelt werden müssen
- Vorstand des KKS-Netzwerks (http://www.kks-netzwerk.de) findet Thema wichtig und würde Workshop unterstützen
- Grundidee:
    - Session bzgl. Grundlagen
        - Was ist ein Pseudonym, was ist Anonym? (aus Sicht der Aufsichtsbehörden)
        - Wann darf ich pseudonymisieren/anonymisieren?
          D.h. brauche ich für die Verarbeitung eine rechtliche Grundlage?
    - Anforderungen der Datenverarbeiter
        - Umgang mit Daten, die aus Sicht des Datenverarbeiters nicht pseudonymisiert werden dürfen (da ansonsten der Verarbeitungszweck nicht erreichbar ist)
        - Umgang mit besonderen Arten von Daten (DICOM-Dateien, Biomaterialien, …), die in sich das Potential zu Identifizierung beinhalten
    - Mögliche Vorgehensweisen
        - Open Source Tool zur Pseudonymisierung des epi. Krebsregister NRW
        - TNM-Pseudonymisierungskonzept
        - Cloud-basierte Anonymisierunglösung von Aircloak
- Rahmenbedingungen
    - Beteiligung aller Gruppen inkl. Datenschutzaufsichtsbehörde
    - Dauer: ca. 7-8 Stunden
    - Ergebnis: Veröffentlichung über MIBE und Webseite
- Die GMDS wird einen entsprechenden Workshop organisieren. Dabei erfolgt eine enge Absprache mit Herrn Drepper (TMF) und Herrn isele (bvitg).

## Top 11: Sonstiges

### *11.1 Datenschutz bei Patientenportalen*

- Hintergrund: Portale werden für Krankenhäuser immer wichtiger, einzelne Aufsichtsbehörden fangen an sich mit dem Thema zu beschäftigen (z.B. Bayern, Hessen)
- Wahrscheinlich werden sich GDD und/oder BvD mit den datenschutzrechtlichen Anforderungen von Patientenportalen beschäftigen. Hier könnte eine Zusammenarbeit mit unserer AG erfolgen, in welcher unsere AG (ggfs. in Zusammenarbeit mit dem bvitg) technische Lösungsmöglichkeiten zu den von BvD/GDD erarbeiteten datenschutzrechtlichen Anforderungen erarbeitet.

### *11.2 „Selbstdatenschutz“*

- Darstellung, wie man selbst Maßnahmen treffen kann, z.B. bei der Browsernutzung, im Chat, bei Suchmaschinen, Facebook usw., ist in unsere Wiki integriert. Alle GMDS-Mitglieder sind aufgerufen, sich heir zu beteiligen.
- Herr Drepper weist darauf hin, dass derzeit das BMBF hierzu Fördermittel ausgeschrieben hat (http://www.bmbf.de/foerderungen/25038.php).
    - Antragstellung muss bis 16.1.2015 erfolgen, wobei der 16.1. nicht als Ausschlußfrist gilt. Die Förderdauer ist auf 2-3 Jahre begrenzt
    - Die einzureichende Projektskizze soll inklusive Anhang maximal 15 Seiten betragen
    - Am 27. November gibt es in Berlin zur Ausschreibung selbst eine Informationsveranstaltung (http://www.vdivde-it.de/KIS/bekanntmachungen/bm-selbstbestimmung), für Teilnehmer an der Info-Veranstaltung ist eine Anmeldung bis zum 24.11. gewünscht

## Top 12: Formalia

### *12.1 Protokoll letzte Sitzung*

Wird einstimmig von den anwesenden AG-Mitgliedern angenommen

### *12.2 MIBE*

MIBE als GMDS-Organ zur Veröffentlichung von Ergebnissen der AG

### *12.3 Termine für AG-Treffen 2015*

1) conhIT 2015
   Donnerstag, 16. April 2015 von 11.00 – 14.00 Uhr
   Raum Lindau 4 (conhIT, Anreiseinformationen unter http://www.conhit.de/HotelUndAnreise)
2) Gemeinsame Sitzung mit der TMF
   November 2015