

## Tutorium

### Datenschutz und Datensicherheit in Gesundheitsanwendungen

Peter Pharow<sup>1</sup>, Dr. Manfred Brunner<sup>2</sup>, Prof. Klaus Pommerening<sup>3</sup>

<sup>1</sup> eHealth Competence Center, Regensburg

<sup>2</sup> Universitätsklinikum, Erlangen

<sup>3</sup> Johannes-Gutenberg-Universität, Mainz

#### Einführung:

Die Veränderung der demographischen Struktur und des Anspruchdenkens der Bevölkerung sowie der Paradigmenwechsel im Gesundheitssystem hin zum Erhalten und Steigern der Lebensqualität führen zu einem wachsenden Druck auf das Gesundheitswesen, die Qualität und Effizienz der Prozesse zu verbessern und gleichzeitig die Kosten zu beherrschen. Der exakte Personenbezug und das Management digitaler Identitäten spielen dabei eine wichtige Rolle. Das bedeutet u.a. die Gewährleistung von Datenschutz (Protection), Sicherheit (Safety) und IT-Sicherheit (Security) sowie die Wahrung der Privatsphäre der Betroffenen (Privacy). Im Zuge der Umsetzung der genannten Bedingungen entstehen neue Anforderungen für zukünftige Gesundheitsinformationssysteme und Netzwerke. Dabei spielen die elektronische Gesundheitsakte, die elektronische Gesundheitskarte und der Heilberufsausweis sowohl in der Theorie als auch in der Praxis eine zunehmend wichtige Rolle. Der Datenschutzbeauftragte im Krankenhaus sieht die neuen Anforderungen, die in diesem Zusammenhang auf ihn zukommen werden, mit großer Skepsis. Die schwierigen Aufgaben in der täglichen Praxis, die unübersichtliche und komplizierte rechtliche Lage, der reale Betrieb des Krankenhausinformationssystems mit handhabbaren Zugriffsrechten sowie der Widerstand von ärztlichem und pflegerischem Personal gegen Beschränkungen sind handfeste Probleme, mit denen sich der Datenschutzbeauftragte täglich auseinandersetzen muss. Für die sekundäre Verwendung von Patientendaten für Gesundheitsberichterstattung, Qualitätssicherung, Versorgungsforschung und epidemiologische Forschung ist hingegen kein Personenbezug notwendig. Datenschutzgerechte Lösungen lassen sich in diesem Fall auf Pseudonymisierungstechniken aufbauen. Hierfür wurden in der TMF, ausgehend vom Bedarf medizinischer Forschungsnetze und Biomaterialbanken, Modelle entwickelt und in konkrete Verfahren umgesetzt.

#### Zielsetzung:

Das Tutorium hat das Ziel, eine Informations- und Diskussionsgrundlage für verschiedene rechtliche, soziale, technische, organisatorische, gesellschafts- und gesundheitspolitische sowie Verhaltensaspekte für die Dienste der Gesundheitstelematik zu offerieren. Insbesondere kommen Anforderungen und Lösungen für sichere, verlässliche und vertrauenswürdige Gesundheitsinformationssysteme und Gesundheitsnetze zur Sprache. Alle Aspekte werden durch handhabbare praktische Erläuterungen und Handlungshilfen unteretzt. Die grundlegenden Verfahren zur Pseudonymisierung werden vorgestellt und die Möglichkeiten zur Umsetzung unter konkreten organisatorischen Rahmenbedingungen diskutiert; hierbei wird auch über die bisher schon in Forschungsnetzen gemachten Erfahrungen berichtet. Das Tutorium hat das Ziel, handhabbare Lösungen für die tägliche Arbeit im Krankenhaus aufzuzeigen. Die juristisch eindeutig erscheinenden Anforderungen werden dabei in praxisnahe Handlungshilfen umgesetzt. Die Möglichkeiten, Berechtigungskonzepte, rechtlich zulässige, sichere und effektive Fernwartungszugänge sowie die Vernetzung von Krankenhäusern, Arztpraxen oder auch Ge-



## Tutorium

sundheitsnetzwerken zu realisieren, werden erläutert. Das Tutorium bietet den Teilnehmern einen umfassenden Überblick über Sicherheitsbedrohungen, Risiken und Lösungen in modernen verteilten Gesundheitsinformationssystemen und Netzwerken und versetzt sie in die Lage, die vermittelten Informationen in ihrem eigenen Umfeld einzusetzen, wobei die präsentierten Erfahrungen auf der langjährigen aktiven Mitarbeit der Tutoren in Projekten, Initiativen und Gremien basieren.

### Zielgruppe:

Das Tutorium richtet sich vorrangig an Datenschutzbeauftragte in Krankenhäusern und anderen Einrichtungen, Medizininformatiker, Mediziner und Techniker, die sich bereits aktiv mit den Aspekten von Datenschutz, Datensicherheit und IT-Sicherheit von Gesundheitsinformationssystemen befassen oder künftig befassen wollen. Die inhaltlichen Schwerpunkte betreffen neben dem Datenschutz und der Datensicherheit die Gesundheitskarten und die Sicherheitsinfrastruktur. Die Ergebnisse erfolgreicher Projekte und Initiativen werden aus der Sicht des Gesundheitswesens präsentiert.

### Voraussetzungen:

Die Teilnehmer sollten über eigene Erfahrungen mit Gesundheitsanwendungen verfügen sowie die wesentlichen Grundbegriffe von Datenschutz und Datensicherheit, wie Identifikation, Authentifizierung, Integrität, Vertraulichkeit, elektronische Signatur, Verschlüsselung und Zertifizierung kennen.

### Termin

Der genaue Termin und die Uhrzeiten werden noch abgestimmt und bekannt gegeben.

### Programm:

10 Minuten	Begrüßung, Vorstellungsrunde, Erwartungen, Erfahrungen
10 Minuten	Bedrohungen und Risiken in Gesundheitsinformationssystemen
15 Minuten	Sicherheitsdienste und Sicherheitsmechanismen in Gesundheitsanwendungen
15 Minuten	Spezifikation einer Sicherheitsinfrastruktur nach nationalen und europäischen Regeln
15 Minuten	Chipkarten (eGK und HBA) im Gesundheits- und Sozialwesen
30 Minuten	Pause
10 Minuten	Grundlagen von Anonymisierung und Pseudonymisierung (Datenschutzrecht, Begriffe)
20 Minuten	Methoden des Anonymisierung und Pseudonymisierung
20 Minuten	Die Pseudonymisierungsmodelle der TMF für Forschungsnetze und Biomaterialbanken
30 Minuten	Praktischer Datenschutz: Anforderungen und Konzepte
20 Minuten	Praktischer Datenschutz: Beispiele und gelebte Praxis
15 Minuten	Zusammenfassung, Ergebnisse, Chancen, Ausblick, Diskussion

Dauer des Tutoriums: insgesamt 3,5 Stunden (210 Minuten).

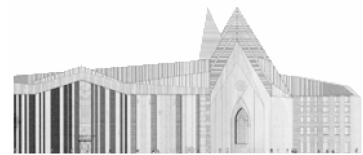


[www.gmDS2006.de](http://www.gmDS2006.de)

Telefon: +49 (0) 341-9 71 62 83 Fax: +49 (0) 341-9 71 62 99 E-mail: [information@gmDS2006.de](mailto:information@gmDS2006.de)

Bankverbindung: Deutsche Apotheker- und Ärztebank e.G. Köln BLZ: 370 606 15 KTO: 030 160 18 22

IBAN : DE35 3006 0601 0301 6018 22 BIC (Swift Code) : DAAEDED



## Tutorium

### Weitere Leistungen:

Pausengetränke und Unterlagen.

### Referent(en):

Die Tutoren arbeiten seit vielen Jahren aktiv als Partner bzw. Gutachter und Berater in nationalen Forschungsaktivitäten und europäischen Projekten. Sie sind aktiv in verschiedene Arbeitsgruppen und Task Forces für Sicherheit und Architektur, Datenschutz, Datensicherheit, Pseudonymisierung usw. involviert. Peter Pharow leitet seit April 2005 die GMDS-AG „Datenschutz in Gesundheitsinformationssystemen“ und bearbeitet Fragestellungen von PKI und TTP sowie Chipkarten. Klaus Pommerening stand der gleichen AG bis März 2005 vor und leitet die Entwicklung von Datenschutzrichtlinien und Pseudonymisierungsstrategien für die TMF. Manfred Brunner ist stellvertretender Leiter der AG und praktizierender Datenschutzbeauftragter des Universitätsklinikums in Erlangen.

### Teilnehmerzahl:

Das Tutorium findet statt, wenn sich mindestens 10 Teilnehmer anmelden. Die maximale Teilnehmerzahl beträgt 35. Haben sich bis zum 30. August 2006 weniger als 10 Teilnehmer angemeldet, wird das Tutorium abgesagt und bereits bezahlte Gebühren zu 100% erstattet.

### Anmeldung:

Die Anmeldung erfolgt im Rahmen der GMDS-Jahrestagung 2006 online über die Tagungswebseiten: <http://registry.gmds-online.de>. Beachten Sie bitte, dass für den Besuch eines Tutoriums auch eine gültige Tagungskarte erforderlich ist. Sie können Tagungskarten und Tutorien unabhängig voneinander online buchen. Für die Tutorien gelten die Allgemeinen Geschäftsbedingungen ([AGB](#)) der Tagung.