

# Datenschutz und Datensicherheit im Gesundheitsanwendungen

P Pharow, M Brunner, K Pommerening

Keywords: Datenschutz, Datensicherheit, Gesundheitskarte, Pseudonymisierung, Sicherheit

## Einleitung

Die Veränderungen in der demographischen Struktur und im Anspruchdenken der Bevölkerung sowie der Paradigmenwechsel im Gesundheitssystem hin zur Steigerung der Lebensqualität jedes Bürgers (personal Health) führen zu einem wachsenden Druck auf das Gesundheitswesen. Es muss die Qualität und Effizienz der Prozesse verbessern und gleichzeitig Kosten senken. Der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte sowie die Verantwortlichen im Krankenhaus sehen die neuen Anforderungen, die auf sie zukommen, mit Skepsis. Die Aufgaben in der täglichen Praxis, die oft unübersichtliche rechtliche Lage, der reale Betrieb des Krankenhausinformationssystems mit handhabbaren Zugriffsrechten sowie der sanfte Widerstand von ärztlichem und pflegerischem Personal gegen Einschränkungen sind Probleme, mit denen die Verantwortlichen konfrontiert sind. Anwendbare Handlungshilfen sind gefragt [1].

## Material und Methoden

Personenbezug und das Management digitaler Identitäten spielen eine zunehmende Rolle hinsichtlich der Gewährleistung von Interoperabilität, Datenschutz, Datensicherheit, persönlicher Unversehrtheit und IT-Sicherheit sowie der Wahrung der Privatsphäre der Betroffenen. Dabei entstehen neue Anforderungen an die Gesundheitsinformationssysteme einschließlich Gesundheitsakte, Gesundheitskarte und Heilberufsausweis. Einführend werden diese Systeme vorgestellt und bewertet. Bei sekundärer Verwendung von Daten für Gesundheitsberichterstattung, Qualitätssicherung, Versorgungsforschung und epidemiologische Forschungen ist hingegen kein Personenbezug notwendig. Datenschutzgerechte Lösungen lassen sich auf der Pseudonymisierung aufbauen. Ausgehend vom Bedarf medizinischer Forschungsnetze und Biomaterialbanken wurden Modelle entwickelt und in konkrete Verfahren umgesetzt. 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 [2], [3].

## Erwartete Ergebnisse

Das Tutorium *Datenschutz und Datensicherheit in Gesundheitsanwendungen* hat sich zum Ziel gestellt, eine breite Grundlage zur Diskussionen verschiedener rechtlicher, sozialer, technischer, organisatorischer, gesellschafts- und gesundheitspolitischer sowie Verhaltensaspekte für die Dienste der Gesundheitstelematik anzubieten. Anforderungen und Lösungen für sichere, verlässliche und

vertrauenswürdige Gesundheitsinformationssysteme und Gesundheitsnetze sowie Gesundheitskarten kommen ebenso zur Sprache wie Anonymisierungs- und Pseudonymisierungsszenarien und Algorithmen. Alle Aspekte werden durch handhabbare praktische Erläuterungen und Handlungshilfen untersetzt. Die Referenten sind erfahren in Theorie und Praxis.

- [1] B.Blobel, K.Engel, P.Pharrow: Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, Teil II: Datensicherheit. In: C.Bake, B.Blobel, P.Münch (Hrsg.): Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, 2. aktualisierte und überarbeitete Auflage. DATAKONTEXT-FACHVERLAG GmbH, Frechen 2003.
- [2] Pommerening K et al. Ein generisches Datenschutzkonzept für Biomaterialbanken. München: MWV; 2007
- [3] Reng CM, Debold P, Specker C, Pommerening K. Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin. München: MWV; 2006

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)  
Schedestrasse 9, D-53113 Bonn