Pseudonymisierung zur sicheren Umsetzung des elektronischen Gesundheitsakts

Dipl.-Ing. Mag. Dr. Thomas Neubauer,
Dipl.-Ing. Mag. Mag. Bernhard Riedl, Mag. Dr. Thomas Mück

Der elektronische Gesundheitsakt (ELGA) bietet hohes Potential zur Steigerung der Effizienz im Gesundheitswesen und somit der Behandlungsqualität der Patienten. Es sind jedoch sicherheitstechnische Maßnahmen wie die Pseudonymisierung erforderlich, um zu gewährleisten, dass der Verfügungsberechtigte die absolute Hoheit über seine Daten behält und die Erfordernisse des Datenschutzes mit den gewohnt hohen Standards erfüllt werden.

Aufgrund von demographischen Entwicklungen sowie den steigenden Kosten der modernen Medizin befindet sich das derzeitige Gesundheitswesen im Umbruch. Die Aufrechterhaltung eines qualitativ hochwertigen Gesundheitssystems bei gleichzeitiger Reduktion oder zumindest Beibehaltung der Kosten gleicht einer Gratwanderung, bei der es nur eine Frage der Zeit ist, bis der Patient nachteilige Auswirkungen zu erwarten hat. Die öffentlichen Gesundheitsausgaben betragen in Österreich 8 % - 9 % des BIP und steigen jährlich um ca. 5 % schneller als das BIP[1,2,3]. In der Machbarkeitsstudie ELGA werden wesentliche Einsparungen durch die Digitalisierung, Speicherung und ständige Verfügbarkeit aller Daten und medizinischer Befunde des Patienten in Aussicht gestellt. Das Ziel des ELGA ist die Minimierung der Kosten für das Auffinden von medizinischen Informationen bei gleichzeitiger Maximierung der Verfügbarkeit dieser Informationen. Durch die verbesserte Dokumentation der Krankengeschichte sowie die gesteigerte Vernetzung zwischen den Gesundheitsdiensteanbietern (GDA) könnte darüber hinaus eine zusätzliche Qualitätssteigerung der medizinischen Behandlungsverfahren, insbesondere der Qualität der Behandlungspfade, erzielt werden. Der Gesundheitsakt ermöglicht die Reduktion fehlerhafter Medikation, die nicht nur zu hohen Kosten, sondern auch zu mehreren tausend Todesfällen pro Jahr führt, da Mediziner durch das System bei der Verordnung von Medikamenten unterstützt werden und auf diese Weise Wechsel- oder Nebenwirkungen bei der Behandlung automatisch berücksichtigt werden können. Darüber hinaus würde der elektronische Gesundheitsakt eine erweiterbare und besser kontrollierbare Sammlung von statistischen Daten für die medizinische Forschung hervorbringen, wodurch die Struktur klinischer Studien unter verschiedenen Gesichtspunkten optimiert werden könnte.

Unter anderem Blickwinkel darf möglicher Missbrauch in den Auswertungsmöglichkeiten von zentral gespeicherten oder indizierten personenbezogenen Daten keinesfalls ausgeschlossen werden. Aufgrund dieser stark thematisierten Problematik in Bezug auf den Datenschutz stehen einzelne Interessensgruppen der Umsetzung des ELGA in der derzeit geplanten Form skeptisch gegenüber. Die missbräuchliche Offenlegung vertraulicher Patientendaten hätte schwerwiegende Auswirkungen für Patienten und Familien, da Versicherungen oder Arbeitgeber diese Informationen dazu verwenden könnten, um den Abschluss von Versicherungsverträgen oder eine Anstellung zu verweigern. Datenschutz erfüllt hier die wichtige Funktion einer Sicherheitsinstanz, die die Bedürfnisse des Patienten nach korrekter - im Sinne der vom Patienten intendierten - Verwendung seiner Daten und die Anforderungen der Gesellschaft nach einem qualitativ hochwertigen Gesundheitssystem, das weiterhin allen Bürgern gleichermaßen zugänglich ist, harmonisieren muss. Die oftmals bemühte Argumentation, dass eine elektronische Speicherung zu einer Verbesserung des Datenschutzes beiträgt, kann ausschließlich bei Schaffung der entsprechenden Rahmenbedingungen als gegeben bezeichnet werden. Diese Bedenken steigern den Bedarf nach einer Lösung, die Datensicherheit und Datenschutz garantieren und den Zugriff auf Gesundheitsdaten unter der strikten Kontrolle einer entsprechenden Instanz (z. B. des Patienten) halten kann. In diesem Zusammenhang wird das Konzept der Pseudonymisierung zunehmend diskutiert. Dieses in der Informationsverarbeitung wohl bekannte Konzept sieht vor, dass bestimmte Identifikationsmerkmale durch ein Kennzeichen ersetzt werden, um auf diese Weise die Identifikation des Betroffenen auszuschließen oder wesentlich zu erschweren. Es stellt daher einen Ansatz dar, der im E-Health-Bereich eine „vollständige Anonymität" ermöglicht, jedoch trotzdem eine Zuordnung von personenbezogenen Patientendaten zu den medizinischen Daten des Patienten ausschließlich unter kontrollierten Umständen ermöglicht.

Das Kompetenzzentrum Secure Business Austria hat in enger Kooperation mit Partnerfirmen eine richtungsweisende Lösung für die Pseudonymisierung von Gesundheitsdaten mit der Bezeichnung PIPE (Pseudonymization of Information for Privacy in e-Health) entwickelt und patentiert. Im Vergleich zu bestehenden Lösungen basiert dieses Konzept nicht auf der Anonymisierung oder einer zentralen Patientenliste, die einen wesentlichen sicherheitstechnischen Schwachpunkt darstellt. Eine Kompromittierung dieser Liste würde konzeptbedingt alle Verbindungen zwischen den Identifikationsdaten und dem Pseudonym des Patienten offenlegen. PIPE löst die Probleme bestehender Verfahren, indem der Verfügungsberechtigte der alleinige Geheimnisträger im System ist und ausschließlich auf Verschlüsselungsebene agiert, woraus auch

[1] *OECD Health Data 2006, http://www.oecd.org.*
[2] *Hofmarcher, M., Riedel, M., Röhrling, G.: Gesundheitsausgaben in der EU: Annäherung durch Erweiterung? Health System Watch I/2004.*
[3] *Pichler, Eva: Public Health Expenditures and Social Security Expenditures in Austria. Official Statistics and Lacking Cost Transparency. AGI Working Paper Series, No. 4, 2005.*

ein höherer Grad an Sicherheit bei der Autorisierung resultiert. Da der Verfügungsberechtigte - gemäß dem mehrstufigen Hüllenmodell (vgl. Abb. 1.) - als einziger Zugriff auf seine Daten hat, wäre der Zugang zu diesen Daten nach dem Verlust oder einem Defekt der Smartcard für niemanden mehr möglich. Ein Backup-Mechanismus in PIPE erlaubt jedoch die Wiederherstellung des Zugriffs auf die Gesundheitsdaten, falls beispielsweise die Smartcard verloren wird. PIPE bietet weiters die Möglichkeit, die Gesundheitsdaten für die medizinische Forschung zu verwenden, ohne dass eine Verbindung zwischen dem Patienten und den Daten hergestellt werden kann. Es ist trotzdem möglich, bestimmte Patienten bzw. dessen behandelnden Arzt über Ergebnisse einer Studie, die beispielsweise unmittelbare Auswirkungen auf seine weitere Behandlung haben, zu informieren, wobei gewährleistet ist, dass die Person, die diese Verständigung durchführt, keine Kenntnis über die Identität des betroffenen Patienten hat. Bei bestehenden Systemen können theoretisch aus bestimmten Daten Rückschlüsse auf den Patienten getroffen werden. Dies ist insbesondere bei sehr seltenen Krankheiten oder bestimmten Kombinationen von Krankheiten der Fall. Dieses „Profiling“ wird bei PIPE wesentlich reduziert, indem für jeden Befund bzw. eine bestimmte Gruppe von Befunden des Patienten ein eigenes Pseudonym verwendet werden kann. Der vorgestellte Ansatz bildet die Basis für eine sichere Umsetzung von E-Health-Diensten und gewährleistet auf diese Weise die Wahrung der Privatsphäre des Patienten. ■

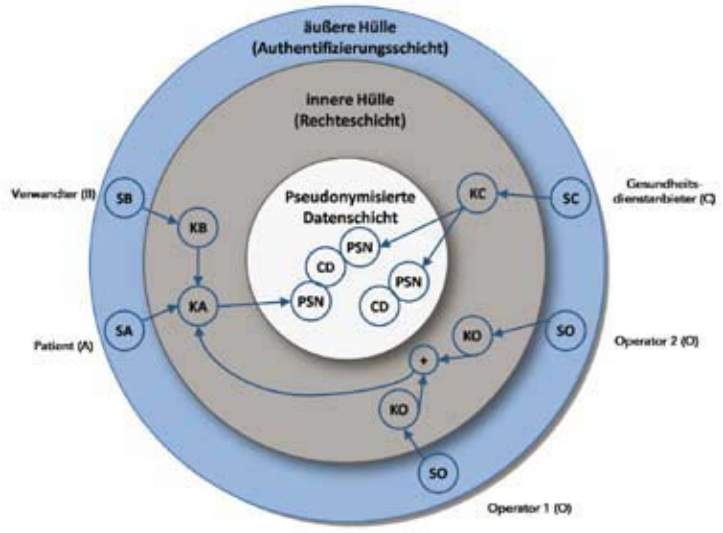

Abb. 1.: Das Hüllenmodell (S=Smartcard, K=Key, PSN=Pseudonym, CD=Daten)

Informationssicherheit muss stärker ins Bewusstsein gerückt werden

Staatssekretärin Silhavy präsentiert neues Informationssicherheits-Handbuch

Die Staatssekretärin im Bundeskanzleramt, Heidrun Silhavy, stellte Ende Oktober gemeinsam mit Expertinnen und Experten des Bundeskanzleramtes das neue „Österreichische Informationssicherheits-Handbuch“ vor. Dieser Leitfaden beschreibt Strategien und Maßnahmen, wie Informationssicherheit effektiv in Verwaltung und Wirtschaft realisiert werden kann.

„In unserer Gesellschaft ist das wirtschaftliche und gesellschaftliche Leben zunehmend digitalisiert. Durch die wachsende Komplexität in der Informationstechnologie steigt auch das Potenzial an Bedrohungen. Täglich erfordert es mehr Wissen, diesen Gefahren wirksam zu begegnen. Das stellt eine gewaltige Herausforderung für die öffentliche Verwaltung und die Wirtschaft dar. Das vorliegende Handbuch soll daher ein praktikables Hilfsmittel sein, um die Informationssicherheit in Österreich weiter zu verbessern“, sagte Silhavy.

Die Ausgangsversion des Nachschlagewerks aus dem Jahr 1998 wurde aufgrund der aktuellen internationalen Entwicklung neu überarbeitet. Damit soll auf das gestiegene Bedrohungspotenzial reagiert werden: „Die Sicherheitslücken in der Standardsoftware sind beispielsweise im Jahr 2006 um 40 Prozent gegenüber dem Vorjahr gestiegen. Daher ist es wesentlich, das Sicherheitsbewusstsein zu erhöhen. Dies gilt auch besonders für die industrielle Sicherheit“, so Katharina Fritze und Gerald Trost vom Informationssicherheitsbüro im Bundeskanzleramt.

Das Handbuch ist in zwei Teile gegliedert: Der Teil „Informationsmanagement“ beschreibt den grundlegenden Vorgang, Informationssicherheit in einer Organisation zu etablieren. Der zweite Teil mit dem Titel „Informationssicherheitsmaßnahmen“ geht auf die konkreten Einzelmaßnahmen auf organisatorischer, personeller und technischer Ebene ein. Dabei wird besonders auf die spezifisch österreichischen Rahmenbedingungen und Regelungen geachtet. Das Nachschlagewerk wird auch als Online-Version auf der Homepage des Bundeskanzleramtes, der „Plattform digitales Österreich“, zur Verfügung stehen.

„Es ist mir ein Anliegen, das Bewusstsein für Informationssicherheit in Österreich voranzutreiben. Dieses Handbuch ist ein wesentlicher Beitrag dazu. Wir sehen es als ein Service für die Bürgerinnen und Bürgern sowie die österreichischen Wirtschaftsunternehmen, um die Vertraulichkeit und Integrität von Informationen sicherzustellen“, meinte Silhavy abschließend. ■

Bestellung
Tel.: 01/512 02 35
Fax: 01/512 02 35-9
gabriel@ocg.at
www.ocg.at/bookshop