PIPE: EIN SYSTEM ZUR PSEUDONYMISIERUNG VON GESUNDHEITSDATEN

Neubauer T[1], Mück T[2]

Kurzfassung

Der Einsatz des elektronischen Gesundheitsakts (ELGA) verspricht eine Verbesserung der Kommunikation zwischen Gesundheitsdiensteanbietern, wodurch nicht nur die Qualität der Behandlungen in bestimmten Bereichen weiter gesteigert, sondern auch die Behandlungskosten positiv beeinflusst werden können. Da diese streng vertraulichen Daten jedoch ein lohnendes Ziel für Angreifer darstellen, müssen zunächst wichtige Vorbedingungen erfüllt sein. Eine in diesem Zusammenhang gesellschaftspolitisch zentrale Forderung lautet, dass die Datenspeicherung auch und insbesondere so zu erfolgen hat, dass die Rechte der Patienten auf Vertraulichkeit und Datenschutz nicht untergraben werden. Dieser Artikel beschreibt ein neues System namens PIPE (Pseudonymization of Information for Privacy in e-Health) für die Pseudonymisierung von Gesundheitsdaten, das sich von bestehenden Systemen durch seine Eigenschaft abhebt, die primäre und sekundäre Verwendung von Gesundheitsdaten zu integrieren. PIPE reduziert die Schwachstellen bestehender Ansätze und kann somit als Basis für nationale e-Health Projekte oder als Erweiterung bestehender Applikationen und Forschungsdatenbanken eingesetzt werden.

1. Einleitung

Das derzeitige Gesundheitswesen befindet sich im Umbruch, da regionale demographische Entwicklungen, aber auch steigende Kosten der modernen Medizin zunehmenden Einfluss auf politische Entscheidungsprozesse ausüben. Die öffentlichen Gesundheitsausgaben betragen in der EU durchschnittlich 8% - 9% des Bruttoinlandsprodukts (BIP), manche Studien kommen zu dem Ergebnis, dass die Gesamtgesundheitsausgaben schneller als das BIP wachsen [10]. Die Aufrechterhaltung eines qualitativ hochwertigen Gesundheitssystems bei gleichzeitiger Reduktion oder zumindest Beibehaltung der Kosten ist eine der wesentlichen Herausforderungen im Gesundheitswesen, allfällige nachteilige Auswirkungen für Patientengruppen werden immer häufiger (und vor allem interessenspolitisch) in Diskussion gebracht. Durch den Einsatz des elektronischen Gesundheitsakts (ELGA), der die Digitalisierung, Speicherung und ständige Verfügbarkeit aller Daten und medizinischer Befunde des Patienten ermöglicht, werden eine Verbesserung der Kommunikation zwischen den Gesundheitsdiensteanbietern (GDA) und dadurch wesentliche Einsparungen in Aussicht gestellt [7]. Eine Studie aus den USA zeigt, dass eine flächendeckende Einführung des Gesundheitsaktes zu einer jährlichen Kostenreduktion von $81 Milliarden führen würde, sofern sich 90% der GDA an dieser Maßnahme beteiligen [3]. Derzeit führt das Auffinden von papierbasierten Akten oder die Mehrfacheingabe von Daten zu oftmals erheblichen Verzögerungen in der Behand-

[1] Secure Business Austria, Wien

[2] Sozialversicherungsanstalt der gewerblichen Wirtschaft, Wien

lung und somit zu zusätzlichen Kosten. Das Ziel des ELGA ist die Minimierung der Kosten für das Auffinden von medizinischen Informationen bei gleichzeitiger Maximierung der Nutzbarkeit dieser Informationen. Im heutigen Gesundheitssystem hat die Verfügbarkeit von fehlerfreier Information einen wesentlichen Einfluss auf die Behandlungsqualität des Patienten. In diesem Zusammenhang ermöglicht der ELGA eine Reduktion von unerwünschten Arzneimittelwirkungen, die in den USA nach Schätzungen zu jährlichen Kosten von $175 Mrd. und der hohen Anzahl von über 100.000 Todesfällen [3]führen, da Mediziner durch das System bei der Verordnung von Medikamenten unterstützt werden und auf diese Weise Wechsel- oder Nebenwirkungen automatisch berücksichtigt werden können. In Folge der verbesserten Dokumentation der Krankengeschichte sowie der gesteigerten Vernetzung zwischen den GDA kann die zusätzliche Qualitätssteigerung der medizinischen Behandlungsverfahren - insbesondere der Behandlungspfade - erzielt werden. Der elektronische Gesundheitsakt ermöglicht eine erweiterbare und besser kontrollierbare Sammlung von statistischen Daten für die medizinische Forschung. Auf diese Weise kann die Struktur klinischer Studien unter verschiedenen Gesichtspunkten optimiert werden (z.B. durch eine höhere Anzahl an Patienten und einer daraus resultierenden höheren statistischen Signifikanz).

Unter anderem Blickwinkel darf möglicher Missbrauch in den Auswertungsmöglichkeiten von zentral gespeicherten oder indizierten personenbezogenen Daten keinesfalls ausgeschlossen werden. Aus diesem Grund gleicht die Definition des erforderlichen Niveaus an Datenschutz einer Gratwanderung zwischen dem Recht des Patienten auf Schutz seiner sensiblen Daten und dem Bedarf der Gesellschaft nach gesteigerter Effizienz und reduzierten Ausgaben für das Gesundheitssystem. Durch die gesteigerte Interkonnektivität, die mit dem ELGA erzielt wird, kann die Offenlegung von vertraulichen Daten schwerwiegendere Folgen für den Patienten haben als bei papierbasierten Systemen [1]. Aufgrund dieser derzeit stark thematisierten Problematik in Bezug auf den Datenschutz, stehen einzelne Interessensgruppen der Umsetzung des ELGA in der geplanten Form skeptisch gegenüber. Die missbräuchliche Offenlegung vertraulicher Patientendaten hätte schwerwiegende Auswirkungen für Patienten und Familien. Versicherungen oder Arbeitgeber könnten diese Informationen dazu verwenden, um den Abschluss von Versicherungsverträgen oder eine Anstellung zu verweigern. Die Offenlegung von Daten beispielsweise über eine HIV-Infektion, früheren Drogenkonsum oder andere Interventionen (z.B. Schwangerschaftsabbruch) könnten zu Diskriminierung führen und sind für den Patienten generell unzumutbar. 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.

In den USA wurde mit dem Health Insurance Portability and Accountability Act (HIPAA) [19]eine Rechtsgrundlage geschaffen, die den Schutz von Patientendaten fordert, die über ihre ursprüngliche Datenquelle hinausgehend genutzt werden. In der Europäischen Union ist die Bearbeitung und Übertragung von Gesundheitsdaten durch die Direktive 95/46/EC [4]geregelt. Das Recht des Patienten auf Schutz seiner Daten ist darüber hinaus durch den Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten [2]sowie in nationalen Gesetzen (z.B. dem österreichischen Datenschutzgesetz [14]) festgelegt. Die Bedenken über den Missbrauch von Daten sowie die gesetzlichen Anforderungen haben zur Entwicklung einer Vielzahl von Methoden zur Sicherstellung des Datenschutzes geführt. Eine Möglichkeit besteht in der vollständigen bzw. teilweisen Verschlüsselung der medizinischen Daten. Da medizinische Daten tendenziell sehr groß sind wäre eine Verschlüsselung in der Praxis jedoch nicht zweckmäßig. Zusätzlich können verschlüsselte Daten nicht für Auswertungen im Rahmen der sekundären_Verwendung herangezogen werden. Als Folge dieser Einschränkungen empfehlen einige Autoren die Verwendung von Pseu-

donymen, um den Anforderungen des Datenschutzes gerecht zu werden. Das Konzept der Pseudonymisierung (vgl. [9][17]) erlaubt die Zusammenführung der Patientendaten mit den Gesundheitsdaten ausschließlich unter genau spezifizierten Umständen. Bestehende Ansätze (vgl. [8][18][6][11][12]) weisen jedoch einige Nachteile auf, wie zum Beispiel die Abhängigkeit von einer zentral gespeicherten Liste mit den Relationen zwischen Patient und Pseudonym oder der Geheimhaltung des verwendeten Algorithmus. Eine Kompromittierung dieser Liste würde konzeptbedingt alle Verbindungen zwischen den Identifikationsdaten und den medizinischen Daten des Patienten offenlegen.

Dieser Artikel präsentiert eine richtungsweisende Lösung für die Pseudonymisierung von Gesundheitsdaten mit der Bezeichnung PIPE (Pseudonymization of Information for Privacy in e-Health), die eine Integration von primärer und sekundärer Datenverwendung erlaubt. Primäre Datenverwendung umfasst alle Patientendaten, die ein GDA im Rahmen der Patientenbehandlung erstellt oder verwendet, während die sekundäre Datenverwendung die Verwendung der Daten im Rahmen von Analysen, Forschung oder der Qualitätssicherung beinhaltet.

PIPE löst die Probleme bestehender Verfahren indem der Verfügungsberechtigte der alleinige Geheimnisträger im System ist und ausschließlich auf Verschlüsselungsebene agiert. Das System ermöglicht dem Patienten jedoch die Autorisierung dritter Personen (z.B. GDA, Ehepartner), die auf seine Daten zugreifen dürfen. Zusätzlich wird ein Konzept vorgestellt, dass die Wiederherstellung der Schlüssel ermöglicht, falls der Patient seinen Zugangsschlüssel verliert. Das vorgestellte System kann als Basis für die Implementierung von sicheren ELGA Architekturen herangezogen werden oder als Erweiterung bestehender Applikationen und Forschungsdatenbanken dienen.

2. Hintergrund

Pseudonymisierung ist eine Methode bei der die Identifikationsdaten des Patienten durch ein Pseudonym ersetzt werden, dass ausschließlich bei Kenntnis eines bestimmten Geheimnisses mit den Identifikationsdaten assoziiert werden kann [17]. Da zur Gewährleistung des Datenschutzes der pseudonymisierte Datensatz keine Patienteninformationen enthalten darf, erfolgt die Trennung der Datenbank in zumindest zwei Tabellen. In einer Tabelle werden die Patientenstammdaten gespeichert, während die andere Tabelle die Pseudonyme sowie die pseudonymisierten Datensätze beinhaltet. Der Prozess der Identifikation und Trennung von Patientenstammdaten und pseudonymisierten Daten wird als Depersonalisierung bezeichnet (vgl. [13]). Nach der Depersonalisierung und anschließender Pseudonymisierung kann keine direkte Verbindung zwischen bestimmten Personen und deren Daten mehr hergestellt werden. Jene Algorithmen, die zur Erzeugung der Pseudonyme dienen, basieren üblicherweise auf Verschlüsselungs- oder Hashing-Methoden. Hashing-Methoden erfordern die Speicherung der Pseudonyme in einer Liste, um die Umkehrbarkeit des Vorgangs zur ermöglichen (vgl. [5][11][12]). Diese Vorgangsweise ist daher mit Sicherheitsrisiken verbunden, da ein Angreifer, der sich Zugriff auf diese Liste verschafft, eine Verbindung zwischen den Stamm- und den Anamnesedaten des Patienten herstellen kann. Thielscher et al. [18]schlagen ein Konzept vor, dass zwei Datenbanken für die separate Speicherung von Patientenidentifikationsdaten und medizinischen Daten verwendet und die Relation zwischen diesen beiden Elementen durch die Verwendung eines geheimen Schlüssels, der auf einer Smartcard gespeichert ist, absichert. Zusätzlich können GDA autorisiert werden auf bestimmte Datensätze zuzugreifen. Die Schwachstelle dieses Systems besteht in der Abhängigkeit von einer zentral gespeicherten Liste, die die Beziehung zwischen Patient und Pseudonym abbildet. Diese Liste wird als Backupmechanismus verwendet, falls der Patient seine Smartcard verliert, da ohne einen solchen Mechanismus der Zugriff auf die Daten unwiederbringlich verloren wäre. Thielscher et al. umgehen diese Sicherheitslücke

durch die lokale (offline) Bearbeitung der Liste. Diese Lösung bietet jedoch nur so lange einen höheren Grad an Sicherheit bis ein potentieller Angreifer physischen Zugriff auf den Computer erhält, wo sich die Liste befindet, wobei es sich hier insbesondere um Insider handeln kann. Pommerening et al. präsentieren zwei Ansätze [11][12]die beide Ähnlichkeiten mit der Lösung von Thielscher et al. aufweisen. Die vorgeschlagene Architektur kombiniert Hashing- und Verschlüsselungsmethoden und ist für die sekundäre Verwendung von medizinischen Daten in Forschungseinrichtungen konzipiert. Das Konzept basiert auf einem zentral gespeicherten geheimen Schlüssel, wodurch jedoch eine Sicherheitslücke erzeugt wird, da ein Angreifer, der diesen Schlüssel kennt, Zugriff auf die Daten aller Patienten erhält. Das Konzept von Peterson [8]basiert ebenfalls auf einer zentral gespeicherten Liste. Im Vergleich dazu bietet die Verschlüsselung einen höheren Grad an Sicherheit bei der Generierung von Pseudonymen. Gemäß dem Prinzip von Kerckhoff (vgl. [15]) müssen bei dieser Vorgangsweise nur die Schlüssel geheim gehalten werden, während die verwendeten Algorithmen frei verfügbar sind. Jedoch sollten die Schlüssel möglichst wenigen Personen - im Normalfall nur dem Benutzer selbst - bekannt sein. Zu diesem Zweck erfolgt heutzutage die Speicherung von Schlüsseln vorzugsweise auf Smartcards. Diese Karten sind mit Prozessoren ausgestattet, die für die Durchführung von kryptographischen Operationen verwendet werden, ohne dazu die Daten auf offene Clients (z.B. einen PC) übertragen zu müssen. Auf diese Weise können in Kombination mit einem zertifizierten Kartenlesegerät die Vertraulichkeit und Integrität der Daten während der Ver- und Entschlüsselung gewährleistet werden. Die Schlüssel sind auf dem Chip der Karte gespeichert und der Zugriff darauf wird mit einem PIN Code geschützt. Solange der PIN Code nur dem Karteninhaber bekannt ist, kann diese Methode als sicher bezeichnet werden. Dennoch können Smartcards verloren gehen, gestohlen, zerstört oder kompromittiert werden. Aus diesem Grund muss das System eine Möglichkeit zur Wiederherstellung der Schlüssel anbieten, um den Zugriff auf die damit geschützten Daten im Fall eines Verlusts der Karte zu ermöglichen. Ein Ansatz besteht in der zentralen Speicherung der Schlüssel in einem Keystore. Dabei können rollenbasierte Modelle (RBAC) verwendet werden, um den Zugriff auf den Keystore zu steuern. Da rollenbasierte Modelle kompromittiert werden können, muss der Keystore verschlüsselt werden, um den maximalen Grad an Sicherheit zu garantieren. Trotzdem muss für die Wartung des Systems bestimmten Personen der Zugang ermöglicht werden. Aus diesem Grund erweist sich dieser Ansatz als ungeeignet für den Zugriff auf hochsensible Gesundheitsdaten, da interne Angreifer das System kompromittieren bzw. Zugriff auf fremde Daten erlangen können. Eine Möglichkeit zur Verringerung dieser Schwachstelle ist die Verteilung der Zugangsschlüssel auf mehrere Administratoren (vgl. [16]). Dieses Konzept wird im Rahmen von PIPE aufgegriffen, um einen sicheren Backupmechanismus zu schaffen. Ein weiterer Schwachpunkt bestehender Systeme ist die Abhängigkeit des Patienten von einem einzelnen Pseudonym. Aufgrund dieser Einschränkung können nicht nur die medizinischen Daten eines bestimmten Pseudonyms zu dessen Krankengeschichte kombiniert werden, sondern bei Bekanntheit bestimmter Eigenschaften des Patienten auch dessen Identität ermittelt werden (z.B. unter Verwendung von Data Mining). Zusätzlich wird durch die Article 29 Working Party der Europäischen Union definiert, dass die Verwendung eines einzelnen Pseudonyms eine eindeutige Identifikation des Patienten ermöglicht und daher zu vermeiden ist. Aus diesen Gründen besteht eine wichtige Anforderung an eine zeitgemäße Pseudonymisierungslösung in der Verwendung von disjunkten Pseudonymen.

3. Systemüberblick

Das System (vgl. *Abbildung 1*) besteht aus der Menge von Benutzern, die in die Rollen Patient, Verwandter, GDA und Operator unterteilt werden. Der Patient (A) hat als Dateninhaber die vollständige Kontrolle über seine Daten. Er kann jedoch anderen Benutzern das Recht erteilen auf seine Daten zuzugreifen. Der Patient kann beispielsweise einem Verwandten (B) den Vollzugriff auf seine

medizinischen Daten ermöglichen oder einen GDA (C) autorisieren bestimmte Daten zu lesen und neue Daten zu erstellen. Als Operator (O) bezeichnen wir die administrative Rolle, die herangezogen wird, um Teile des Schlüssels des Patienten zu halten und somit einen Backupmechanismus zu bieten, falls der Patient seine Smartcard verliert oder diese kompromittiert wird.

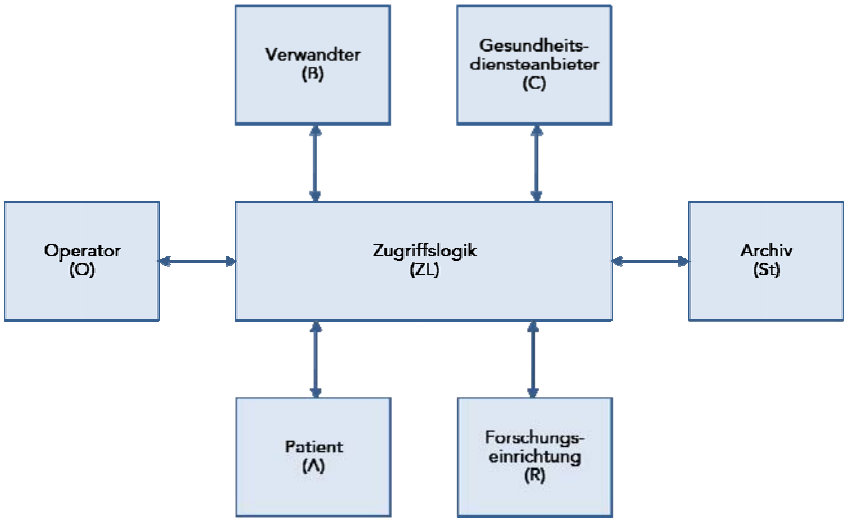

Abbildung 1: Architektur von PIPE

Alle Daten werden in einem Archiv (St) persistiert, das aus einer Datenbank und einem Keystore besteht. In Kombination mit der Zugriffslogik (ZL) muss das Archiv eine vertrauenswürdige Instanz darstellen, da dort das Smartcard Management erfolgt (vgl. *Abbildung 1*). *Abbildung 2* zeigt die neuartige Hüllenarchitektur, die dem System PIPE zugrunde liegt und den Kern des erhöhten Sicherheitsniveaus darstellt. Dabei beinhaltet jede Hülle eines oder mehrere Geheimnisse (z.B. verschlüsselte Schlüssel oder versteckte Relationen), auf die nur durch Kenntnis des Geheimnisses der nächstäußeren Hülle zugegriffen werden kann. Beispielsweise ist der innere private Schlüssel des Patienten (e‘A) der inneren Hülle mit dem äußeren öffentlichen Schlüssel (dA) verschlüsselt, der sich auf der Smartcard des Patienten und somit in der äußeren Hülle befindet. Der innere private Schlüssel wird dazu verwendet, um Zugriff auf den inneren symmetrischen Schlüssel (KA) zu erhalten, der verschlüsselt mit dem inneren öffentlichen Schlüssel (d‘A) in der innersten Hülle des Systems liegt. Jeder Datensatz (CD) wird mit einer Liste von *j* Pseudonymen identifiziert. Auf diesen Datensatz kann nur mit Kenntnis des Pseudonyms (PSN_j) zugegriffen werden, dass mit dem inneren symmetrischen Key verschlüsselt wurde. Möchte der Patient Zugriff auf seine Daten erhalten, muss er den inneren privaten Schlüssel entschlüsseln, der sich im System befindet und mit dem äußeren öffentlichen Schlüssel von der Smartcard verschlüsselt wurde. Danach kann der Patient den inneren privaten Schlüssel verwenden, um den inneren symmetrischen Schlüssel zu entschlüsseln. Dieser ermöglicht nun den Zugriff auf die Pseudonyme und somit auf die medizinischen Daten.

Das System ist darauf ausgerichtet den Austausch von Geheimnissen zu unterstützen, um dem Patienten zu ermöglichen andere Benutzer zu autorisieren auf bestimmte Daten zuzugreifen. Beispielweise kann der Patient einem Verwandten den vollständigen Zugriff auf seine Daten erlauben. Zu diesem Zweck wird der innere private Schlüssel des Patienten mit dem inneren symmetrischen Schlüssel des Verwandten verschlüsselt. Der Verwandte kann solange auf die Daten des Patienten zugreifen bis der innere private Schlüssel des Patienten geändert wird. Des Weiteren kann mit einer ähnlichen Vorgangsweise ein GDA autorisiert werden auf bestimmte medizinische Datensätze des Patienten zuzugreifen. Zu diesem Zweck existiert für jeden Datensatz ein Root Pseudonym (PSN_0)

mit dem die Relation zwischen dem Patienten und dem medizinischen Datensatz definiert wird. Zusätzlich gibt es für jede Relation zwischen dem Patienten und einem autorisierten Benutzer (z.B. einem GDA) ein eigenes Pseudonym. Sind beispielsweise zwei GDA berechtigt auf einen bestimmten Datensatz des Patienten zuzugreifen, werden zusätzlich zum Root-Pseudonym zwei weitere Pseudonyme (PSN_1, PSN_2) zwischen dem Patienten und jeweils einem GDA angelegt. Der Patient hat die vollständige Kontrolle über seine Daten und kann als einziger Systemteilnehmer alle Relation zu seinen Datensätzen uneingeschränkt kontrollieren, d.h. sowohl anlegen als auch wiederum löschen.

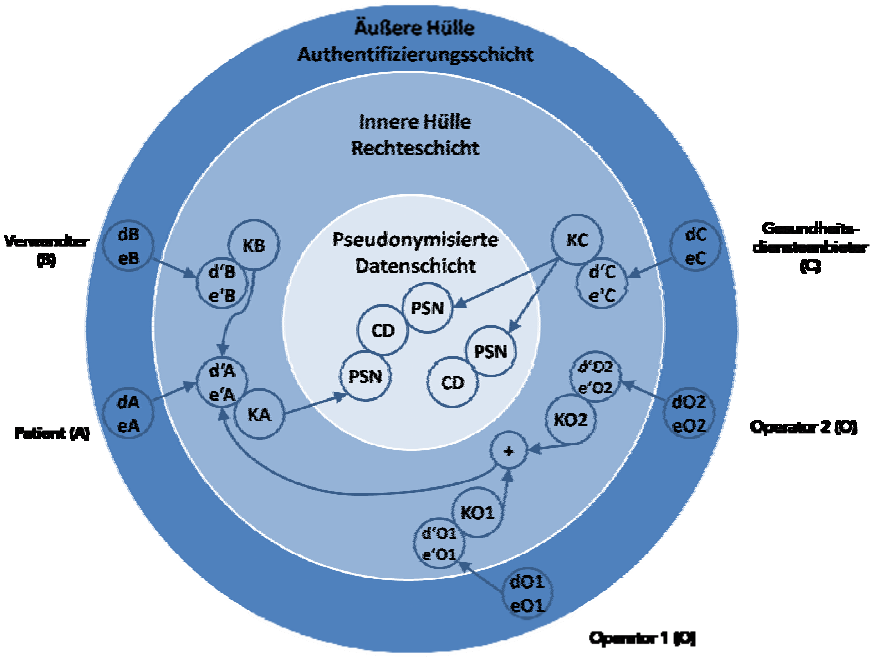

Abbildung 2: Die Hüllen Architektur von PIPE

4. Zusammenfassung

Der Einsatz des elektronischen Gesundheitsakts verspricht in bestimmten Fällen bzw. Konstellationen nicht nur eine weiter gesteigerte Behandlungsqualität für den Patienten sondern auch eine Optimierung der Ausgaben im Gesundheitssystem (z.B. durch die Vermeidung von Mehrfachuntersuchungen, effizientere Behandlungspfade, etc.). Da derartige Systeme hochsensible Daten speichern, die elektronisch verarbeitet und ausgewertet werden können, muss der Datenschutz für den Patienten uneingeschränkt gewährleistet sein, um Missbrauch der Daten auszuschließen. Entsprechend der bestehenden gesetzlichen Vorgaben, die insbesondere im deutschsprachigen Raum sehr ausgeprägt sind, darf die Einführung des ELGA nicht als Argument für die Aushöhlung dieser Rechte missbraucht werden. Obwohl in der Vergangenheit einige Ansätze zur Absicherung von medizinischen Daten präsentiert wurden, weisen diese Methoden oftmals Schwachstellen auf, die eine Verwendung für die Speicherung medizinischer Daten stark einschränken. In diesem Artikel diskutierten wir bestehende Systeme und deren Einschränkungen in Bezug auf die Sicherheit. Basierend auf diesen Schwachstellen präsentierten wir eine neue Architektur für die sichere und effiziente Speicherung von medizinischen Daten mit dem Namen PIPE. Dieses System integriert die primäre und sekundäre Datenverwendung und gewährleistet, dass der Patient die vollständige Kontrolle über seine Daten hat während die Verwundung disjunkter Pseudonyme eine eindeutige Abgrenzung zwischen einzelnen Behandlungsfällen ermöglicht. Der Patient kann zu jedem Zeitpunkt bestimmen,

welchen Personen er diese Daten zur Verfügung stellt. Zusätzlich beinhaltet das System einen Mechanismus für das sichere Backup von Zugangsschlüsseln für den Fall, dass ein Benutzer des Systems seine Zugangskarte verliert.

5. Danksagungen

Diese Arbeit wurde im Rahmen des Kompetenzzentrums Secure Business Austria durchgeführt, das vom Bundesministerium für Wirtschaft und Arbeit (BMWA) sowie der Stadt Wien gefördert wird.

6. Literatur

[1] BARROWS, R. C., & CLAYTON, P. D. (1996). Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association, 13, pp. 139-148.

[2] Council of Europe. European convention on human rights.

[3] ERNST, F. R., & GRIZZLE, A. J. (2001). Drug-related morbidity and mortality: Updating the cost-of-illness model. Journal of the American Pharmaceutical Association, 41(2), pp.192-199.

[4] European Union. (1995). Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, L 281, pp. 31-50.

[5] FLEGEL, U. (2002). Pseudonymizing unix log files. In Proceedings of the international conference on infrastructure security (pp. 162-179). London, UK: Springer-Verlag. Gulcher, J., Kristjansson, K., Gudbjartsson, H., K., & Stefanson. (2000). Protection of privacy by third-party encryption in genetic research. European journal of human genetics, 8, pp.739-742.

[6] LYSYANSKAYA, A., RIVEST, R. L., SAHAI, A., & WOLF, S. Pseudonym systems. In Proceedings of the sixth annual workshop on selected areas in cryptography (SAC'99).

[7] MAERKLE, S., KOECHY, K., TSCHIRLEY, R., & LEMKE, H. U. (2001). The PREPaRe system {Patient Oriented Access to the Personal Electronic Medical Record. In: Proceedings of CARS 2001 Computer Assisted Radiology and Surgery, 2001, pp. 849-854.

[8] PETERSON, R. L. (2003). Patent: Encryption system for allowing immediate universal access to medical records while maintaining complete patient control over privacy. US Patent US 2003/0074564 A1.

[9] PFITZMANN, A., & KOEHNTOPP., M. (2005). Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management A Consolidated Proposal for Terminology. In Lecture Notes in Computer Science. Springer Berlin / Heidelberg.

[10] PICHLER, EVA (2005): Public Health Expenditures and Social Security Expenditures in Austria. Official Statistics and Lacking Cost Transparency. AGI Working Paper Series, No. 4.

[11] POMMERENING, K. (1994). Medical Requirements for Data Protection. In Proceedings of IFIP Congress, Vol. 2, pp. 533-540.

[12] POMMERENING, K., & RENG, M. (2004). Medical and care compunetics 1. In L. Bos, S. Laxminarayan, & A. Marsh (Eds.), pp. 441-446. IOS Press.

[13] RECTOR, A., ROGERS, J., TAWEEL, A., INGRAM, D., KALRA, D., MILAN, J., et al. (2003). Clef - joining up healthcare with clinical and post-genomic research. In Proceedings of UK e-science all hands meeting, pp. 203-211.

[14] Republik Österreich. (1999). Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999.

[15] SCHNEIER, B. (1995). Applied cryptography: Protocols, algorithms, and source code in Wiley; 2 edition.

[16] SHAMIR, A. (1979). How to share a secret. Commun. ACM, 22 (11), pp. 612-613.

[17] TAIPALE, K. (2004). Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd. International Journal of Communications Law & Policy, 9.

[18] THIELSCHER, C., GOTTFRIED, M., UMBREIT, S., BOEGNER, F., HAACK, J., & SCHROEDERS, N. (2005). Patent: Data processing system for patient data. Int. Patent, WO 03/034294 A2.

[19] United States Department of Health & Human Service. (2006). Hipaa administrative simplification: Enforcement; final rule. Federal Register / Rules and Regulations, Vol. 71, No. 32.