EIN SICHERES PATIENTENZENTRIERTES KONZEPT FÜR PERSONAL HEALTH RECORDS

Slamanig D[1], Stingl C[1]

Kurzfassung

Neben nationalen Ansätzen zur Einführung von Elektronischen Gesundheitsakten (EHRs), gibt es im angloamerikanischen Raum auch den Ansatz des so genannten Personal Health Records (PHR), z.B. von Google oder Microsoft. Diese Systeme integrieren verschiedene regionale EHRs in ein Gesamtsystem und zeichnen sich dadurch aus, dass sie vom Patienten verwaltet werden. Obwohl PHRs, aufgrund der verbesserten Behandlungsqualität bei gleichzeitig niedrigeren Kosten, viele Vorteile mit sich bringen, muss aktuell die Akzeptanz hinsichtlich der Teilnahme in der Bevölkerung unserer Meinung nach als eher gering eingestuft werden. Dies liegt einerseits an Horrorszenarien hinsichtlich der Verletzung der Privatsphäre, die durch Medien transportiert werden, und andererseits an konkreten Bedrohungsszenarien, die von Betreibern weitestgehend ignoriert werden bzw. diesen teilweise nicht bekannt oder bewusst sind. In dieser Arbeit werden diese Szenarien diskutiert und eine effiziente Möglichkeit für den Aufbau eines PHRs vorgestellt.

1. Einleitung

In vielen Bereichen des Gesundheitswesens werden derzeit Anwendungen entwickelt, die auf der Basis von Informations- und Kommunikationstechnologien Prozesse effizient abbilden und nachhaltig optimieren sollen. Durch die hohe Verfügbarkeit des Internets können, neben den klassischen Akteuren im Gesundheitswesen, zunehmend auch Patienten integriert werden. Dies trägt einerseits dazu bei, dass die Qualität der Behandlung gesteigert werden kann, aber andererseits bringt die zeit- und ortsunabhängige Verfügbarkeit der medizinischen Daten zusätzliche Gefahrenpotentiale mit sich. In vielen Projekten wird letzterer Aspekt als sekundär betrachtet, da sich der Fokus auf die Etablierung der medizinischen Prozesse richtet. Eine zentrale Anwendung in diesem Kontext ist der so genannte Personal Health Record (PHR). Betrachtet man die Einführung eines PHR, so ist die informationelle Selbstbestimmung der Patienten ein elementares Grundprinzip [3]. Konkret bedeutet dies, dass Personen selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten bestimmen können. Dabei muss jedoch erwähnt werden, dass die Moderation nicht explizit vom Patienten durchgeführt werden muss, sondern an eine Person des Vertrauens, z.B. Verwandte, Ärzte, delegiert bzw. in Zusammenarbeit mit dieser Person durchgeführt werden kann. Neben dieser letztgenannten Forderung spielt aus Sicht der Patienten der Schutz der medizinischen Daten und folglich ihrer Privatsphäre die zentrale Rolle [2,5].

[1] Healthcare IT & Information Security Group, Fachbereich für Medizinische Informationstechnik, Fachhochschule Kärnten, 9020 Klagenfurt

2. Bedrohungsszenarien

Da aus Sicht der Patienten der Datenschutz einen wesentlichen Faktor darstellt [2], muss folglich dieser Aspekt als erfolgskritischer Faktor für einen PHR angesehen werden. Bei Bedrohungsszenarien im Kontext von PHRs ist die ausschließliche Betrachtung klassischer Angriffe gegen Systemkomponenten, z.B. Hacking, nicht ausreichend. Darüber hinaus müssen auch „Angriffe“ durch Systeminsider [4], sowie aus dem Bereich des Social Engineerings betrachtet werden. Unter Insiderangriffen versteht man den unautorisierten Zugriff auf medizinische Daten unter Ausnutzung von Berechtigungen, die grundsätzlich für die Administration des Systems benötigt werden. Bei Angriffen im Bereich des Social Engineerings wird versucht über zwischenmenschliche Beeinflussungen Zugriff auf die medizinischen Daten zu erlangen. Beispielsweise können Informationen für die Authentifikation am System, z.B. Benutzername und Passwort, durch den Patienten „freiwillig“ weiter gegeben werden. Ein zusätzlicher Aspekt ist das Erlangen von Informationen durch Nötigung von anderen Personen [8].

Auf Basis von Angriffen gegen den Client, den Kommunikationskanal und das PHR Systems, die beispielsweise in [6] behandelt werden, können nun die folgenden sicherheitsrelevanten Primärziele für die Konzeption eines PHR identifiziert werden:

- Situationsabhängige Darstellung von Ausschnitten des PHR, z.B. bei Nötigung werden nur nicht-kompromittierende Informationen preisgegeben bzw. einem Facharzt werden nur behandlungsrelevante Informationen zur Verfügung gestellt.
- Gewährleistung der Vertraulichkeit (Geheimhaltung) von Inhaltsdaten medizinischer Dokumente.
- Gewährleistung der Vertraulichkeit (Geheimhaltung) von Metadaten zur Unterbindung statistischer Analysen, z.B. eine Verbindung zwischen Arzt und Patient ist nicht eruierbar.
- Unterbinden von Insider-Angriffen bezüglich Inhalts- und Metadaten.
- Patientenindividuelle Strukturierung des PHR.

3. Strukturierung eines PHR

In diesem Kapitel werden grundlegende Begriffe für das PHR Konzept erläutert. Dafür wird angenommen, dass die Struktur des PHR für jede Person individuell gestaltet werden kann. Zur Verwaltung können eindimensionale bzw. mehrdimensionale Ordnerstrukturen eingesetzt werden. Diesen Ordnern werden die relevanten medizinischen Dokumente zugeordnet, wobei diese Zuordnung sich entweder auf einen oder auf mehrere Ordner beziehen kann.

3. 1. Topographie der Ordnerstruktur

Die Topographie der Ordnerstruktur beschreibt die unterschiedlichen Möglichkeiten zum Aufbau eines patientenindividuellen PHR. Dazu werden die folgenden drei Darstellungsformen unterschieden:

- Eindimensionale Ordnerstruktur: Es können beliebig viele Ordner linear angeordnet werden.
- Hierarchische Ordnerstruktur: In diesem Ansatz können Ordner in Form einer Baumstruktur (hierarchisch) angeordnet werden.
- Netzwerk-Ordnerstruktur: Dabei kann im Gegensatz zur hierarchischen Ordnerstruktur jeder Ordner beliebig vielen anderen Ordnern, in Form eines Unterordners, zugeordnet werden.

3. 2. Zuordnung der Dokumente

Die Zuordnung der Dokumente beschreibt den Zusammenhang zwischen Dokumenten und Ordnern. Dazu werden folgende Formen der Zuordnung unterschieden:

- Eindeutige Zuordnung: Jedes medizinische Dokument des PHR wird eindeutig einem Ordner der jeweiligen Ordnerstruktur zugeordnet.
- Mehrfache Zuordnung: Dabei können medizinische Dokumente gleichzeitig einem oder mehreren Ordnern der jeweiligen Orderstruktur zugeordnet werden. Dies wird mittels Referenzen realisiert, da Kopien Inkonsistenzen mit sich bringen.

3. 3. Inhaltliche Ausprägungen der Ordner

Die inhaltliche Strukturierung der Gesundheitsdaten in einem PHR ist einerseits entscheidend für eine effiziente und effektive Verwaltung der Dokumente und andererseits ein Baustein für die Lösung der situationsabhängigen Darstellung von Ausschnitten des PHR. In weiterer Folge dient dies auch zur komfortablen und benutzerspezifischen Vergabe von Berechtigungen. In diesem Kontext werden folgende ein- bzw. mehrdimensionale Ansätze vorgestellt:

- Eindimensionaler Ansatz: Dabei wird jeweils ein wesentliches Kriterium zur Gliederung der medizinischen Inhaltsdaten herangezogen.
    - Zeitbezogener Ansatz: In diesem Ansatz werden medizinische Dokumente anhand des Entstehungsdatums in zeitliche Perioden eingeordnet. Eine einfache Möglichkeit wäre beispielsweise die Klassifizierung nach „aktuellen“ und „nicht aktuellen“ Dokumenten.
    - Fallbezogener Ansatz: Dabei werden die medizinischen Dokumente, die im Rahmen der Behandlung einer Erkrankung entstehen, zusammengefasst. Im Regelfall wird diese Strukturierung auch in Krankenhausinformationssystemen herangezogen.
    - Fachspezifischer Ansatz: Im fachspezifischen Ansatz werden die medizinischen Dokumente primär in Abhängigkeit vom medizinischen Fach- bzw. Anwendungsbereich strukturiert. Ein illustratives, aber nicht vollständiges, Beispiel ist die Einteilung in Allgemeinmedizin, Notfall, Zahnheilkunde und Innere Medizin.
- Mehrdimensionaler Ansatz: Dieser Ansatz kombiniert mehrere eindimensionalen Ansätze gleichzeitig in einem PHR, um die jeweiligen Vorteile vereinen zu können. Es muss jedoch erwähnt werden, dass der Verwaltungsaufwand linear mit der Anzahl der Dimensionen steigt.

Ein wesentliches Merkmal für die Ausprägungen der Ordner ist, dass diese Strukturierung eine virtuelle eindimensionale Ordnerstruktur aufweist, wobei für jeden Ordner eine beliebige Topographie gewählt werden kann. Beispielsweise bedeutet dies, dass im fachspezifischen Ansatz eine virtuelle Liste Allgemeinmedizin-Notfall-Zahnheilkunde-Innere Medizin existiert, wobei jedes Listenelement für sich entweder eine eindimensionale, hierarchische oder Netzwerk-Ordernstrukturen beinhalten kann. Diese Liste wird als virtuell bezeichnet, da sie schlussendlich im PHR in dieser Form nicht abgebildet wird, sondern nur deren Elemente als Bausteine für den Aufbau von so genannten Identitäten dienen.

4. Methoden

Nachfolgend werden Methoden diskutiert, die auf die zuvor diskutierte Struktur angewendet werden können um Bedrohungsszenarien entgegenwirken zu können.

4. 1. Identitäten

Identitäten spielen die entscheidende Rolle bei der Konzeption des hier vorstellten PHR. Diese werden durch die nachfolgenden Eigenschaften charakterisiert:

- Jede Identität kann beliebig viele Elemente der virtuellen Liste beinhalten.
- Die Inhalte von verschiedenen Identitäten müssen nicht disjunkt sein.
- Jede Identität definiert einen potentiellen Einstiegspunkt in den PHR. Dazu ist jedoch eine separate und unabhängige Authentifikation pro Einstiegspunkt notwendig.
- Jede Identität kann beliebig viele so genannte Sub-Identitäten beinhalten. Damit können Identitäten anderen Identitäten untergeordnet werden und somit können beim Öffnen einer Identität alle Sub-Identitäten ohne zusätzliche Authentifikation eingesehen und verwaltet werden.
- Jeder Benutzer kann eine so genannte Super-Identität definieren, die alle relevanten Identitäten beinhaltet und zur einfachen und effizienten Verwaltung dieser dient.
- Von einer Identität kann auf keine weitere Identität geschlossen werden, außer diese ist zuvor als Sub-Identität integriert worden.
- Jede Identität kann anderen Benutzern oder Benutzergruppen freigegeben werden.

Dieser Sachverhalt soll nun anhand eines konkreten Beispiels dargestellt werden. Es sei darauf hingewiesen, dass die verwendete Strukturierung grundsätzlich ein reales Szenario darstellt, jedoch dieses primär zur Illustration des Konzepts der Identitäten dienen soll. In diesem Beispiel wird der fachspezifische Ansatz zur Erstellung der virtuellen Liste herangezogen. Dabei werden folgende Fach- bzw. Anwendungsbereiche betrachtet:

- Allgemeinmedizin (AM): Allgemeine medizinische Daten, die generell relevant sind.
- Notfall (NF): Notfallrelevante medizinische Daten.
- Zahnheilkunde (ZH): Medizinische Daten aus dem Bereich Zahnheilkunde.
- Innere Medizin (IM): Medizinische Daten aus dem Bereich Innere Medizin.
- Nicht-kompromittierender Bereich (NK): Medizinische Daten, die kaum kompromittierende Aussagen über eine Person zulassen.

Auf Basis dieser Elemente wird eine hierarchische Struktur erstellt (siehe *Abbildung 1*). Diese Abhängigkeiten könnten jedoch auch allgemeiner mittels eines Netzwerks dargestellt werden.

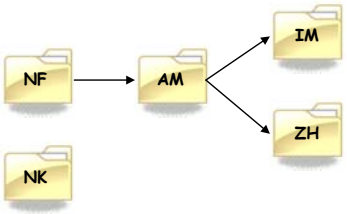

Abbildung 1: Hierarchische Strukturierung der Fach- und Anwendungsbereiche

Für die Struktur in *Abbildung 1* wurde folgende Regel zugrunde gelegt:

- Wenn man auf allgemeinmedizinische Daten zugreift, dann müssen auch Notfalldaten eingesehen werden können.
- Wenn man auf medizinische Daten aus den Bereichen Interne Medizin bzw. Zahnheilkunde zugreift, dann müssen allgemeinmedizinische Daten eingesehen werden können.
- Wenn auf nicht-kompromittierende Daten zugegriffen wird, dann sollen keine weiteren Daten eingesehen werden können.

Auf Grundlage von *Abbildung 1* werden nun die Identitäten des Systems definiert. Dazu wird grundsätzlich für jedes Element aus *Abbildung 1* eine Identität erzeugt, die alle unmittelbaren Kindelemente als Sub-Identitäten integriert. Darüber hinaus wird eine künstliche Super-Identität kreiert, die alle Identitäten der obersten Ebene der Hierarchie (IM, ZH, NK) beinhaltet. Ein Ausschnitt der daraus resultierenden Identitäten wird in *Abbildung 2* dargestellt. Wie bereits oben erwähnt, stellt jede Identität prinzipiell einen Einstiegspunkt in den PHR dar. In diesem Beispiel werden nun jedoch nur die folgenden Identitäten als Einstiegspunkte gewählt. Zusätzlich wird noch ein Anwendungsfall für jede dieser Identitäten angegeben.

- Super-Identität: Dient zur einfachen und effizienten Verwaltung aller relevanten Identitäten.
- Identität „IM“: Dient zur Darstellung aller Informationen, die bei einer konkreten Behandlung durch einen Internisten von Interesse sein könnten.
- Identität „ZH“: Dient zur Darstellung aller Informationen, die bei einer konkreten zahnärztlichen Behandlung von Interesse sein könnten.
- Identität „NK“: Diese Identität dient zur Darstellung der Informationen bei einer erzwungenen Offenlegung, z.B. im Rahmen eines Vorstellungsgespräches.

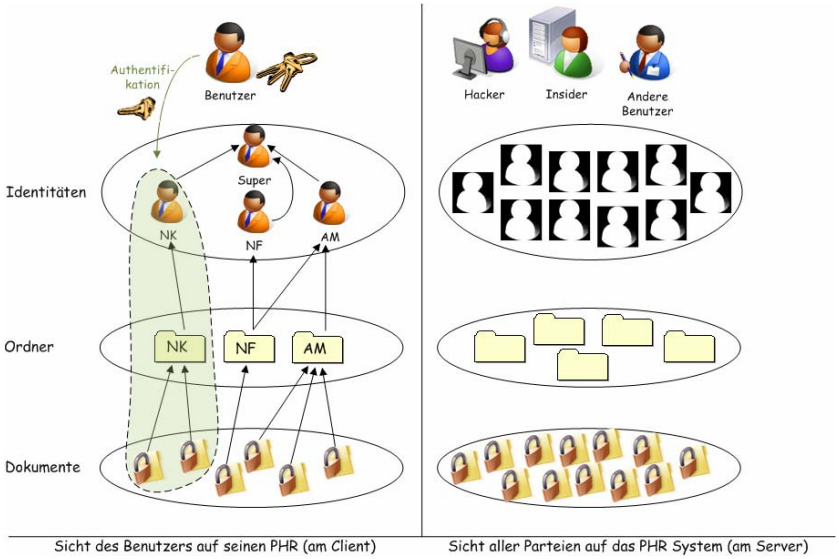

Abbildung 2: Eine Authentifikation gegenüber der Super-Identität bietet dem Benutzer Zugriff auf alle Informationen. Authentifiziert sich der Benutzer gegenüber der Nicht-kompromittierenden Identität (NK), sind nur die Informationen im hinterlegten Bereich einsehbar. Alle Daten eines Benutzers (Identitäten, Ordner, etc.) sind auch für Insider nicht ermittelbar.

Als Zugriffspunkt bei einer Behandlung durch einen Allgemeinmediziner könnte in Abhängigkeit vom Vertrauensverhältnis die Super-Identität bzw. die Identität „AM“ dienen. Weiters kann einer Person des Vertrauens, z.B. Verwandte, Arzt, die Super-Identität freigegeben werden, sodass diese Person den PHR ebenfalls moderieren kann. Um in Notfällen medizinisch relevante Informationen zur Verfügung zu stellen, könnte die Gruppe der Notfallmediziner berechtigt werden die Identität „NF“ einzusehen.

An dieser Stelle muss noch einmal betont werden, dass durch dieses Konzept erstens ausschließlich der Benutzer durch die entsprechende Authentifikation bestimmt welche Daten präsentiert und zweitens keinerlei Informationen über weitere Identitäten preisgegeben werden. Folglich kann der Benutzer durch Authentifikation gegenüber der Identität „NK“ plausibel abstreiten, dass weitere

Identitäten und somit medizinische Daten existieren. Das Konzept der Pseudonymisierung, das nachfolgend erläutert wird, verhindert zusätzlich, dass Insider Informationen über Identitäten eines Benutzers ermitteln können [7,8] (siehe *Abbildung 2* rechte Seite). Wie in *Abbildung 2* dargestellt, sind im System für alle Parteien nur Objekte sichtbar, jedoch keine Beziehungen zwischen Objekten bzw. Objekten und Benutzern.

4. 2. Pseudonymisierung

Im Gegensatz zur Anonymisierung versteht man unter Pseudonymisierung das Ersetzen von benutzeridentifizierender Information durch ein so genanntes Pseudonym. Der Prozess der Pseudonymisierung kann dabei unter Zuhilfenahme von zusätzlicher Information rückgängig gemacht werden. Diese Information steht jedoch ausschließlich berechtigten Personen zur Verfügung. Damit kann grundsätzlich jede Zuordnung zwischen zwei Objekten verschleiert werden, sodass diese ohne die zuvor genannte Information nicht ermittelt werden kann. In [7] wurde gezeigt, dass konzeptionelle Modelle, die bestimmte Voraussetzungen erfüllen, in ein so genanntes pseudonymisiertes konzeptionelles Modell überführt werden können. Unter Beachtung dieser Voraussetzungen kann nun ein konzeptioneller Entwurf für die obige Problemstellung entwickelt und in weiterer Folge pseudonymisiert werden. Durch diese Pseudonymisierung ist es folglich weder für Insider, noch für Außenstehende möglich, Zuordnungen zwischen Personen, Identitäten, Ordnern und medizinischen Dokumenten und weiters zwischen verschiedenen Personen zu eruieren.

5. Konklusion

Auch bei Verwendung der zuvor beschriebenen Pseudonymisierung und dem damit erreichten Schutz vor Angriffen durch Insider, können durch Protokollierung der Zugriffe auf einen PHR unerwünschte Schlüsse gezogen werden [8]. Um dies zu verhindern sollten zusätzlich anonyme Kommunikationskanäle und anonyme Authentifikationsverfahren verwendet werden. Im Gegensatz zum ersteren Aspekt, der unabhängig vom PHR eingesetzt werden kann, muss jedoch der zweite Bereich speziell an die Systemvoraussetzungen angepasst werden.
Zusammenfassend kann festgehalten werden, dass das Missbrauchspotential erheblich reduziert und folglich das Vertrauen der Benutzer in einen PHR erhöht werden kann, wenn Sicherheitskonzepte angewendet werden, die unabhängig vom Vertrauen in den Betreiber des PHR sind.

6. Literatur

[1] CSI. Computer Crime and Security Survey 2007, Computer Security Institute. http://www.gocsi.com/forms/csi survey.jhtml.

[2] HI. Harris Interactive, Survey on Medical Privacy. http://www.harrisinteractive.com/news/newsletters/ healthnews/HI HealthCareNews2004Vol4 Iss13.pdf.

[3] ISO/TR 20514:2005. Health informatics - Electronic health record - Definition, scope and context. ISO 2005.

[4] PREDD, J., PFLEEGER, S. L., HUNKER, J., and BULFORD, C. Insiders Behaving Badly. IEEE Security and Privacy 6, 4 (Jul. 2008), 66-70, 2008.

[5] PYPER, C., AMERY, J., WATSON, M., and CROOK, C. Access to Electronic health records in primary care – a survey of patients views. Med Sci Monit, 10(11):17–22, 2004.

[6] SLAMANIG D., STINGL C. How to Preserve Patient's Privacy and Anonymity in Web-based Electronic Health Records. In: Azevedo, L. and Londral , A.R. (eds.) Proceedings of the Second International Conference on Health Informatics, HEALTHINF 2009, (pp. 257-264), INSTICC Press, 2009.

[7] SLAMANIG D., STINGL C., LACKNER G., and PAYER U. Schutz der Privatsphäre in einem webbasierten Multiuser-System. DACH-Security 2007, pages 98–110. IT-Verlag, 2007.

[8] STINGL, C. and SLAMANIG, D. Privacy-Enhancing Methods for e-Health Applications: How to Prevent Statistical Analyses and Attacks. Int. J. Bus. Intell. Data Min. 3, 3 (Dec. 2008), 236-254, 2008.