



THESEN DER GESELLSCHAFT FÜR INFORMATIK

ZUR ELEKTRONISCHEN GESUNDHEITSKARTE

Mit 11 Milliarden Transaktionen pro Jahr und einem Datenaufkommen von mindestens 23.6 Terabyte pro Jahr (ohne Bilddaten) gehört die Digitalisierung der medizinischen Versorgung in Deutschland wegen des notwendig hohen Sicherheitsniveaus und der komplexen, hochverfügbaren IT-Infrastruktur zu den anspruchsvollsten IT-Projekten der Welt.

Zugriffsberechtigt sind – neben 80 Millionen Krankenversicherten - größenordnungsmäßig etwa weitere 2 Millionen Personen - Inhaber der Health Professional Card (HPC): 270.000 Arztpraxen sowie etwa 30.000 weitere Ärzte, Heilberufe, Sanitäts- und Pflegedienste, 22.000 Apotheken und 2000 Krankenhäuser sowie Labore, Reha-Zentren und deren Mitarbeiter sowie Krankenkassen, Rentenversicherung, Unfallversicherung, Gesundheitsämter, Statistikämter, Kassenärztliche Vereinigungen und Kammern.

Die Einführungskosten betragen nach Angaben von BITKOM bzw. der KBV bis zu 1,7 Mrd. € bei Betriebskosten im ersten Jahr von bis zu 150 Mio. €. Dem sollen jährliche Einsparungen von bis zu 1.0 Mrd. € gegenüberstehen; das Projekt amortisiert sich dann in 2 Jahren.

Die GI begrüßt die

- Bemühungen, im Gesundheitswesen, verstärkt **Informationstechnik** zu nutzen und damit
- deutliche **Qualitätssteigerungen** (schnelle Verfügbarkeit wichtiger Patientendaten) verbunden mit erheblichen **Einsparungen** im Gesundheitswesen zu erreichen.

Allerdings birgt die Nutzung neuer Techniken auch neue Risiken, die in einer Risikoanalyse bewertet werden müssen. Die GI fordert nachdrücklich, die Sachziele der Informationssicherheit im digitalisierten Gesundheitswesen zu berücksichtigen: Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit mit Authentizität und Beherrschbarkeit. Die GI sieht insbesondere 2 Risiken, die noch intensiv untersucht werden müssen, bevor Lösungsvorschläge umgesetzt werden können:

- Da die Patientenakten (zumindest derzeit) wegen ihrer **Menge** nicht auf der Gesundheitskarte der Patienten gespeichert werden können, müssten sie im Internet gespeichert werden. Eine sichere Speicherung im Internet ist aber trotz Verschlüsselung und Pseudonymisierung nicht möglich: Alle Computer, Server, Bridges, Switches etc. können erfolgreich angegriffen werden.
- Die gespeicherten Patientendaten können **verknüpft** werden mit den Daten aus Genomdatenbanken, der Mautdatenbank, den gespeicherten Verbindungsdaten der Telefongesellschaften, Bankkonten, Maut, Straßenkontrollen, Buchungsdaten von Flügen etc. Damit können Fragen gestellt werden wie: Wer wohnt in Köln, hat im letzten Jahr mehr als 25.000 € verdient, war zweimal in den USA, fuhr mehr als 5-mal mit dem Auto nach Aachen, telefoniert wöchentlich mit München und leidet an Schwerhörigkeit – und es wird eine Antwort geben.



Die Risiken im Einzelnen:

1. Speicherung von Gesundheitsdaten im Internet

Die 'elektronischen' Patientenakten aller Deutschen sollen auf Servern im Internet gespeichert werden – zugreifbar für alle Berechtigten wie Ärzte, Krankenhäuser, Krankenkassen oder – zumindest teilweise – Apotheken, Labore etc.

Angemessene Zugriffskontrolle unmöglich

- Angesichts der Vielzahl Zugriffsberechtigter von etwa 80 Millionen dürfte eine hinreichend sichere Zugriffskontrolle überhaupt nicht machbar sein.
- Dies wird spätestens dann in einem Missbrauchsfall offenkundig werden, wenn nämlich jedermann mit vorgefertigten, im Internet erhältlichen Tools die Daten seines Nachbarn, seiner Bekannten, seines Abgeordneten oder anderer Politiker wie Landes- und Bundesminister etc. lesen kann.

Verschlüsselung

- Eine (asymmetrische) Verschlüsselung der Patientendaten reicht nicht aus, weil die notwendig im Internet gespeicherten und übertragenen Schlüssel ausgelesen oder abgehört werden können.
- Während der Verarbeitung liegen die Patientendaten naturgemäß unverschlüsselt vor.
- Während der gesetzlich vorgeschriebenen jahrzehntelangen Speicherung von Patientenakten müssen diese (aus technischen Gründen) mehrfach entschlüsselt werden; dabei liegen die Daten hinreichend lange unverschlüsselt vor. Die Daten müssen sporadisch mit sichereren Verfahren neu verschlüsselt sowie umsigniert werden.

Dezentralität im Internet

- Im Internet gespeicherte Gesundheitsdaten sind nicht nur zentral zugreifbar, sie sind auch verknüpfbar. Es gibt keine Dezentralität im Internet.

Sicherheit angeschlossener Rechner

- Die IT-Systeme **aller** Berechtigten wie Ärzte, Mitarbeiter von Krankenkassen, Apotheken, Labore etc. können gar nicht - entsprechend der Sensitivität der Gesundheitsdaten - ausreichend abgesichert werden. Die große Menge der angeschlossenen Rechner ist auch nicht kontrollierbar.
- In diesem Zusammenhang müssen außerdem Funktionen wie die übliche Fernwartung der Hard- und Software berücksichtigt werden: Die Anzahl der Zugriffsberechtigten dürfte insgesamt bei mehr als 20 pro Computer/IT-System liegen.
- Es muss ein rollenbezogenes Zugriffskontrollsystem implementiert werden: z.B. benötigen Ärzte als Behandelnde andere Zugriffsrechte als für Gutachten für Behörden und private Versicherer.
- Zentrale Datensammlungen erhöhen die Attraktivität von internen und externen Angriffen und erleichtern Profilbildungen und Zweckentfremdungen.

Die GI lehnt eine Speicherung von Gesundheitsdaten im Internet nachdrücklich ab.



2. Übertragung von Daten im Internet

Die Datenübertragung ist ausreichend abgesichert, wenn eine hybride Verschlüsselung aller Daten – symmetrische Verschlüsselung der Nutzdaten und asymmetrische Verschlüsselung der benutzten Konzelektionsschlüssel - nach dem Stand der Technik eingesetzt wird.

3. Pseudonyme

Statt der Patientennamen oder –nummern Pseudonyme einzusetzen, bringt keinen hinreichenden Sicherheitsgewinn.

- Der Einsatz von Pseudonymen wäre unbedenklich, wenn es sich um tatsächlich anonymisierte Daten handelte. Allerdings lässt sich mit Hilfe von Pseudonymen auf die Patientendaten zurückschließen!
- Eine - äußerst schwer und damit kostenaufwändig herzustellende - Anonymität schießt bei weitem über das Ziel hinaus, weil anonyme Daten nicht mehr – auch Berechtigten wie dem Patienten selbst – zugeordnet werden können: Sie sind damit nicht mehr zweckgebunden verwendbar.
- Pseudonymisierte Daten können immer nur dann hinreichend sein, wenn es um Rechnungskontrolle, Wirtschaftlichkeitsprüfung oder Qualitätssicherung der Leistungen geht.

4. Digitale Signatur

Der vorgesehene Einsatz der qualifizierten elektronischen Signatur sichert die Authentizität der Daten und ihre Integrität. Damit entspricht das vorgesehene Verfahren dem Stand der Technik.

5. Protokollierung: Nachweisbarkeit aller Lese- und Schreibvorgänge

Der Eigentümer der Karte muss alle Lese- und Schreibvorgänge anhand eines leicht lesbaren, aussagefähigen Protokolls nachvollziehen können.

6. Forderungen der GI

Es müssen Lösungen gesucht werden, welche die Persönlichkeitsrechte der Versicherten wahren und schon die Möglichkeit der Entstehung des "gläsernen Patienten" verhindern.

Sensibilisierung und Awareness der Öffentlichkeit

Die GI fordert in erster Linie eine umfassende Information der Öffentlichkeit über die Chancen und Risiken – auch des Einzelnen - des digitalisierten Gesundheitswesens, um die Akzeptanz durch die Benutzer zu erreichen und damit Ängsten vor Missbrauch sensibler Gesundheitsdaten rechtzeitig vorzubeugen.

Datenspeicherung nur auf der Gesundheitskarte

Die GI fordert die Speicherung aller Gesundheitsdaten auf Eigentümer-beherrschbaren Medien (wie der Gesundheitskarte). Dabei müssen Patientendaten insbesondere gegen Verlust, Zerstörung, Beeinträchtigung und unerlaubten Zugriff wirksam geschützt werden.



Vom Patienten im Detail bestimmbare Daten müssen gegenüber bestimmten Berechtigten gesperrt werden können. Der medizinische Sinn, einem behandelnden Arzt Informationen vorzuenthalten, kann nämlich von einem normalen Patienten durchaus beurteilt werden. Informationstechnische Sicherheitsmaßnahmen sind dazu allerdings noch nicht hinreichend erprobt: Daten verschiedener Sperrbereiche müssen unterschiedlich verschlüsselt sein.

Sicherheitsmaßnahmen entsprechend dem Wert der Daten

- Sicherheitsarchitektur und Sicherheitsniveau müssen sich an internationalen Standards und Normen überprüfbar orientieren. Im Detail ist aufbauend auf dem Grundsatz des Bundesamtes für Sicherheit in der IT (BSI) eine (öffentliche) Risikobewertung vorzunehmen und sind Maßnahmen entsprechend den **Hochsicherheitsanforderungen** umzusetzen.
- Dazu müssen alle Schnittstellen und technischen Standards in Fachkreisen veröffentlicht und mit Experten diskutiert werden.

Ein einziger Sicherheitsverantwortlicher

Es muss einen einzigen, für das gesamte (digitalisierte) Gesundheitswesen verantwortlichen Sicherheits- und Datenschutzbeauftragten geben, an den sich Betroffene wenden können, der Kontrollpflichten ausübt und der die Befugnis der Stilllegung unsicherer Bereiche, Verfahren oder Verfahrensteile hat. Der Verantwortliche muss von unabhängigen Dritten überprüft werden (Sicherheits- und Datenschutz-Audits). Dazu müssen keine neuen Behörden oder Instanzen eingerichtet werden.

Breite gesellschaftliche und fachliche Zustimmung

- Alle Sicherheitskonzepte müssen mit Sicherheitsexperten abgestimmt werden.
- Allen Lösungen müssen IT-Sicherheits- und Datenschutzexperten zugestimmt haben.
- Diese Lösungen müssen zusammen mit den unvermeidbaren Restrisiken der breiten Bevölkerung vollständig vermittelt werden.

Grundsätzlich wecken alle Datensammlungen Begierden; und tatsächlich soll schon die Industrie Zugriff auf die Patientendaten gefordert haben; ein weiteres Risiko stellt die Vernetzung der einzelnen Versicherungen (Kranken-, Unfall-, Zusatz-, Lebensversicherung) dar, die sich gegenseitig in die Patientendaten schauen werden.

Die GI warnt ausdrücklich vor Lösungen, die erhebliche Restrisiken bergen und die GI warnt vor einer vorschnellen Einführung unausgereifter oder nicht vollständig ausgetesteter Verfahren.

Die GI arbeitet an allen IT-Lösungen gern konstruktiv mit.

(Stand: 10. März 2005)

Gesellschaft für Informatik e.V. (GI)
Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“
Wissenschaftszentrum, Ahrstr. 45, 53175 Bonn
E-Mail: gs@gi-ev.de, Tel. 0228 / 302 - 145, Fax - 167