Qualitätszirkel Hausarzt-Internisten Siegen
c/o **Moderator** Wilfried Deiß, Koblenzer Str. 109, D-57072 Siegen
praxis.deiss@posteo.de

DIGITALISIERUNG UND VERSCHLÜSSELUNG IM GESUNDHEITSWESEN

Qualitätszirkel-Sitzung vom 22. September 2014

Der Siegener Qualitätszirkel Hausarzt-Internisten hat sich zum Thema Digitalisierung im Gesundheitswesen getroffen. Den insgesamt 7 Teilnehmern des Zirkels ist bewusst, dass technische Veränderungen in Zukunft große Auswirkung auf die Alltagsarbeit in unseren Praxen und auf die Patientenversorgung haben könnten. Fluch oder Segen der Digitalisierung, das ist die Frage.
Getroffen haben wir uns auf der Grundlage SELBER DENKEN. Wir sind der Überzeugung: Risiken und Nachteile technischer Neuerungen können am ehesten minimiert werden, wenn die Federführung bei denen liegt, die die Alltagsarbeit machen und kennen und die immense Bedeutung des Arztgeheimnisses würdigen.

Zufälligerweise ist exakt in der Woche nach der Sitzung sowohl im Deutschen Ärzteblatt als auch im Westfälischen Ärzteblatt über die aktuellen Entwicklungen beim bundesweiten Telematik-Projekt und Aktivitäten in den Testregionen berichtet worden. Der Schwerpunkt liegt dabei aktuell bei der Erprobung des eArztbriefes, der digitalen Übermittlung von Arztberichten. Das wäre dann die erste Anwendung des seit 10 Jahren laufenden Milliardenprojektes Telematik, deren Sinn für den medizinischen Alltag zu erkennen wäre.

Wir haben bezüglich der verschlüsselten Übermittlung von Arztberichten nach anderen, einfacheren Wegen gesucht, mit Erfolg: am Ende der 90minütigen Sitzung des Qualitätszirkels haben wir uns untereinander die ersten verschlüsselten Mails und verschlüsselten pdf-Texte von Praxis zu Praxis übermittelt. Und das ohne Hilfe von Technikern, Konzernen oder KVen, sondern mit Hilfe der Kompetenz von interessierten Laien. Doch nun der Reihe nach.

Wir teilen die Überzeugung, dass die digitale Übermittlung von Arztberichten sinnvoll ist. Es ist im Alltagsablauf und auch ökologisch unsinnig, Briefe digital zu schreiben, analog als Papier zu verschicken, und beim Empfänger das Papier durch einscannen wieder in digitale Form zu verwandeln.
Bei der digitalen Übertragung sind jedoch ganz entscheidene Prämissen zu beachten. Die Meinung der Qualitätszirkelteilnehmer zu bestimmten Vorgaben unterscheidet sich wesentlich von den Prinzipien des Telematikprojektes.
Wir plädieren für eine digitale Punkt-zu-Punkt-Kommunikation. Im Netz dürfen Patienten betreffende Nachrichten nur zwischen-gespeichert, aber nicht auf Dauer gespeichert werden. So wird vermieden, dass eine gigantische Datensammlung von persönlichen Gesundheitsdaten entsteht. Dass große Datenmengen mit zudem persönlichen und intimen Informationen IMMER Begehrlichkeiten wecken, ist nicht erst seit Snowden bekannt.
Wir lehnen eine zentralistisch organisierte Datensammlung strikt ab. Dabei ist es unerheblich, ob die Gesundheitsdaten auf einer einzelnen große Server-Farm oder in einem anders gearteten Netz gelagert sind. Wir wehren uns damit gegen die Prämisse des Telematik-Projektes, persönliche Gesundheitsdaten der Bevölkerung (bzw. des Teiles der Bevölkerung, der dem zugestimmen würde) so zu speichern, dass sie jederzeit rund um die Uhr nach einem 2-Schlüssel-Prinzip mit Hilfe der eGK des Patienten und des Arztausweises des gerade zuständigen Arztes von überall her abrufbar sind.

Es gibt nämlich keinen Beweis, dass die jederzeitige Verfügbarkeit von Facharztberichten und Krankenhausberichten die Behandlung verbessert. Nachweislich wird im Notfall und Akutfall die Bedeutung von Vorberichten weit überschätzt, zudem in der Notfallsituation auf Intensivstation kaum Zeit ist, umfangreiche alte Akten zu lesen. Es ist vollkommen ausreichend, wenn am nächsten Morgen Berichte schnell verfügbar sind. (siehe auch Deutsches Ärzteblatt / Jg. 105 / Heft 3 / 18. Jan. 2008 / Seite A78 / Notfalldaten - Mehr Schein als Sein?).
An dieser Stelle möchten wir auf den Unterschied zwischen EINZELFALLRISIKO und KOLLEKTIVRISIKO hinweisen. Wenn bei einer Punkt-zu-Punkt-Kommunikation ein Bericht in falsche Hände gerät, ist das ärgerlich, aber in der Regel entsteht kein Schaden. Jeden Tag passiert es, dass ein Fax an eine falsche Nummer gesendet wird. In der Regel kann der fälschliche Adressat nichts damit anfangen und sendet es zurück. Niemand käme auf die Idee, zur Vermeidung eines solchen Fehlers technische Sicherheitsmaßnahmen einzurichten oder ein Gesetz zu verabschieden. Bei einer großen Datenmenge mit Beteiligung von Tausenden oder gar Millionen von Betroffenen, ist das etwas ganz anderes.
Nur wegen des hohen Kollektivrisikos der Telematik-Infrastruktur mit dauerhafter Datenspeicherung ist eine gigantische technische Aufrüstung erforderlich. Bei einer Punkt-zu-Punkt-Kommunikation OHNE dauerhafte Datenspeicherung besteht lediglich ein Einzelfallrisiko. Und wenn dabei sämtliche Texte auch noch verschlüsselt sind, ist die Gefahr von Datenmissbrauch sehr viel geringer als beim Einzelfallrisiko eines Papierbriefes im verschlossenen Umschlages oder eines Fax. Daher dürften sich auch keine rechtlichen Probleme ergeben und keine Probleme bei der Akzeptanz durch Patienten, denn es würde ein sehr sicherer Weg der Informationsübermittlung durch einen noch viel Sichereren ersetzt.
Noch etwa zur milliardenschweren Gigantomanie der Telematik-Infrastruktur: Es wird uns weis gemacht, das brauche man, um in Zukunft CT- und MR-Bilder digital zu übermitteln oder um den Hirnchirurg aus Boston bei der Gehirnoperation in Hannover zuzuschalten. All das ist auch heute möglich, schließlich sind HD-Filme übers Netz längst Alltag, und wenn keine dauerhafte Datenspeicherung besteht, handelt sich auch dabei um ein Einzelfallrisiko.

Wir vom Qualitätszirkel wollen also den langsamen und umständlichen Papier-Brief und das schnelle aber umständliche Papier-Fax durch eine digitale Nachricht ersetzen, die NICHT dauerhaft im Netz gespeichert wird (also eine Art POP3-Protokoll). Das soll in Form einer verschlüsselten Punkt-zu-Punkt-Kommunikation geschehen und im Alltag nicht mehr Arbeit machen als das Versenden einer herkömmlichen eMail.

Die technischen Möglichkeiten zur Umsetzung sind längst vorhanden. Die Mail-Verschlüsselung mit PGP gibt es seit den 90er Jahren. Dabei werden Nachrichten nach dem Prinzip einer "asymmetrischen Verschlüsselung" mit Hilfe eines "öffentlichen" und eines "privaten" Schlüssels verfremdet. Wer die Nachricht ohne Entschlüsselung empfängt, sieht nur Zahlen-und-Buchstaben-Salat. Das Verfahren ist so sicher, dass es immerhin Edward Snowden ermöglichte, seine NSA-Dateien unentdeckt an den Journalisten Greenwald zu senden. Die Einrichtung von PGP auf dem eigenen PC war viele Jahre nur etwas für technisch Versierte. Mittlerweile ist das einfach geworden. Mittelmäßig technisch begabte Anwender schaffen die Installation von PGP für eines der üblichen Mail-Programme auf einem Windows-PC oder Apple-PC innerhalb einer Stunde. Dabei wird sozusagen PGP in das vorhandene Mail-Programm integriert, das Mail-Programm erhält 2 zusätzliche Buttons. Und das muss nur einmal gemacht werden. Dann holt man sich für jeden Adressaten, der auch mit PGP arbeitet, den "Öffentlichen Schlüssel" von einem "Schlüsselserver" im Netz (auch das muss für jeden Adressaten nur

einmal gemacht werden) und schon kann es losgehen. Wenn eine Praxis sagen wir üblicherweise mit 100 anderen Praxen, Krankenhäusern, Apotheken in Kontakt steht, und alle 100 arbeiten mit PGP, dann ist die Vorbereitung für alle 100 einige wenige Stunden Arbeit, die von Laien erledigt werden kann. Ab dann unterscheidet sich das Verschicken und Empfangen von verschlüsselten Mails vom Umgang mit unverschlüsselten Mails nur noch durch einen einzigen Mausklick.
Genau das haben wir am Ende der 90minütigen Sitzung des Qualitätszirkels gemacht und es hat funktioniert. Mit diesem Verfahren können Texte, Bilder, Filme, Audiodateien versendet werden, wie bei "normalen" Mails.
Was brauchen wir dann noch im Gesundheitswesen? Wir brauchen einen gesetzlichen Auftrag an die PVS-Provider, also an die Praxissoftware-Firmen, ihre Praxisprogramme mit einem Mail-Programm zu ergänzen, welches Senden und Empfangen von PGP-verschlüsselten Dateien zulässt und ausserdem sehr praxisorientiert die Sichtung der eingehenden Post und die Zuteilung zur betreffenden Patientenakte zulässt. Wenn die Intensivstation eines Krankenhauses beim Hausarzt anruft und nach Vorberichten fragt, sollten diese sehr unkompliziert mit Tastenklick auswählbar sein und mit einem weiteren Klick als verschlüsselte Datei Punkt-zu-Punkt ans Krankenhaus gesendet werden können. Eine solche Mail-Schnittstelle anzufertigen dürfte für die Softwarehäuser auf wenig Schwierigkeiten stoßen, aber dennoch wenig Freude hervorrufen, weil sich sicher mit der von den Patienten letztlich zu finanzierenden Gigantomanie des Telematikprojektes sehr viel mehr Gewinn machen lassen dürfte. Aus dem Grunde wird vermutlich nur eine gesetzliche Pflicht zum gewünschten Ziel führen.
Ansonsten, so denken wir, dürfte es gut sein, wenn der PGP-Schlüsselserver mit den öffentlichen Schlüsseln aller Teilnehmer im Gesundheitswesen beispielsweise bei der Bundesärztekammer angesiedelt wäre. Die Praxisinhaber, Krankenhausbetreiber, Apotheker und so weiter werden darüber hinaus wohl selbst so klug sein, aus Datenschutzgründen und zum Schutz des Praxisnetzwerkes sonstige, unverschlüsselte Mail NICHT mit dem Praxisnetzwerk zu empfangen, sondern getrennt davon. Das wäre als weitere vertrauensbildende Maßnahme den Patienten gegenüber sicher sinnvoll.

Zusammenfassend zeigt sich an diesem Beispiel: Lösungen, die von den Anwendern erarbeitet werden, die zudem nicht finanziell profitieren und die Kosten für die Versicherten im Blick haben, können einfacher, praktikabler, preisgünstiger und besser sein.

Wilfried Deiß