Wilfried Deiß Facharzt für Innere Medizin - Hausarzt

Koblenzer Str. 109 D-57072 Siegen
www.praxiswilfrieddeiss.de

ZENTRALE TELEMATIK-INFRASTRUKTUR in einfacher Sprache: **ARZTGEHEIMNIS-CLOUD**

Ein patientenorientiertes Plädoyer für mehr Demokratie und verständliche Begriffsbildung bei der Digitalisierung des Gesundheitswesens

Die Begriffe sind die Griffe, mit denen wir die Dinge greifen und hoffentlich begreifen. Wer begreift „Zentrale Telematik-Infrastruktur“?
Selbst Ärztinnen und Ärzte in Deutschland, die nun nach aktueller Gesetzeslage mitsamt Sanktionsandrohung gezwungen werden, ihre Praxen bis zum 1.7.2019 an die Telematik-Infrastruktur anschließen zu lassen, haben zum Teil nicht verstanden, worum es geht.
Und die Patienten? Da ist erwartungsgemäß der Informationsstand noch schlechter. Die Elektronische Gesundheitskarte ist inzwischen bekannt als Versichertenkarte mit Foto, und manche haben gehört, dass irgendwann die persönlichen Arztberichte AUF DER KARTE gespeichert werden sollen.

„Auf der Karte“ ist NICHT auf der Karte, sondern ganz woanders

Dass die Karte nur der Schlüssel zum bundesweiten Netzwerk ist, in dem Arztberichte dauerhaft gespeichert werden sollen, wissen nur die Wenigsten.
Die Desinformation ist allerdings kein Zufall. Seit Start des Projektes eGesundheitskarte / Telematik-Infrastruktur um 2005 bleibt systematisch die Notwendigkeit der Zentralen Datenspeicherung als Kern des Gesamtprojektes unerwähnt. Noch heute ist auf der Homepage der Gematik bei den Erläuterungen zur Elektronischen Gesundheitskarte zu lesen: „Neben den Versichertenstammdaten können - mittels der Elektronischen Gesundheitskarte - später auch medizinische Daten gespeichert werden.“ Die zentrale und dauerhafte Speicherung wird nirgends beschrieben und erläutert.
Selbstverständlich benötigen wir eine zeitgemäße und tatsächlich auch praktikablere Informationsübertragung im Gesundheitswesen. Der Medienbruch von digital zu analog (Post, Fax) und zurück nach digital (Einscannen) ist unsinnig, umständlich und antiquiert. Wir benötigen unzweifelhaft eine gesicherte, verschlüsselte Punkt-zu-Punkt-Übertragung von Dokumenten im Gesundheitswesen. Aber es besteht KEINE ZWINGENDE NOTWENDIGKEIT für eine dauerhafte, zentralisierte Datenspeicherung von Patienteninformationen in einer Daten-Cloud. Mein Grundeinstellung diesbezüglich: das Internet ist eine GENIALE Erfindung. Aber nur für Informationen, die für die Öffentlichkeit gedacht sind. Oder gerade eben noch für Informationen, bei denen kein relevanter Schaden entsteht, wenn sie versehentlich an die Öffentlichkeit oder in kriminelle oder potentiell repressive Hände geraten.

Selbstverständlich benötigen wir eine gesicherte digitale Informationsübertragung im Gesundheitswesen

Kurz ein Schritt zurück in der Technik-Historie zur „HighTech“ der 70er und 80er Jahre. Als damals die Faxgeräte aufkamen, musste niemand aufwändig zur Anschaffung überzeugt oder gezwungen werden. Der Sinn und die Praktikabilität /Alltagstauglichkeit des Gerätes war sofort zu erkennen. Gleichzeitig ist das Faxgerät ein gutes Beispiel für den Unterschied zwischen Einzelfallrisiko und Kollektivrisiko. Faxen ist eine Punkt-zu-Punkt-Kommunikation

(heutzutage sind allerdings Fax-Server dazwischen geschaltet, weil die analogen Faxdaten für den Transport digitalisiert werden). Selbstverständlich sind schon unzählige zufällige Faxe fälschlicherweise an unzählige zufällige falsche Empfänger versendet worden. Allerdings ist die Wahrscheinlichkeit, dass das Irrläufer-Fax erstens eine kriminell verwendbare Information enthält und außerdem an jemanden gerät, der diese verwenden will und kann, extrem klein. Im Gegensatz dazu wird bei einer dauerhaften, zentralen Speicherung das Einzelfallrisiko zum Kollektivrisiko und der Datenspeicher (Cloud) zur idealen Angriffsfläche für kriminelle Aktivitäten.

Einzelfall-Risiken sind möglicherweise tolerabel, Kollektivrisiken nicht

Nun wieder zur Patientenperspektive: Es gibt eine unehrliche und eine ehrliche Frage an Patienten. Die Unehrliche: „Möchten Sie, dass in Zukunft alle Ärzte, denen Sie das erlauben, mit Hilfe Ihrer Elektronischen Gesundheitskarte ihre medizinischen Befunde einsehen können?“ Fragen dieser Art sind in Akzeptanzstudien oft gestellt worden und von Patienten überwiegend bejaht worden. Die ehrliche Variante aber lautet: „Damit Sie allen Ärzten zu jeder Zeit die Erlaubnis erteilen können, Ihre medizinischen Befunde einzusehen, müssen alle Arztberichte in einer Zentralen Datenbank dauerhaft gespeichert werden. Möchten Sie, dass in Zukunft Ihre persönlichen Arztberichte, die allesamt dem Arztgeheimnis unterliegen, nicht mehr nur bei Ärzten gespeichert werden, sondern zusätzlich alle zusammen und dauerhaft in einer bundesweiten Zentralen Datenbank, also in einer Daten-Cloud?“.

Unehrliche oder ehrliche Frage an Patienten?

Genau darum geht es aber. Der Kern der Telematik-Infrastruktur (=TI), die Zentrale Telematik-Infrastruktur, der Sitz der Elektronischen Patientenakte (=ePA), ist nichts anderes als eine Daten-Cloud. Ich selbst habe mich daher entschieden, einen Begriff zu verwenden, der besser verständlich ist. Nicht mehr Zentrale Telematik-Infrastruktur, vielleicht noch Gesundheitsdaten-Cloud, sondern stattdessen: ARZTGEHEIMNIS-CLOUD. Es sind nämlich ganz besondere Daten, um die es hier geht, nicht die üblichen Nutzer-Daten, die bei Facebook, WhatsApp, Amazon, Google anfallen (und selbst da ist das Missbrauchspotential hoch), sondern persönliche und intime Informationen über Menschen insbesondere in somatischen und psychischen Ausnahmesituationen. Eine Foto-Cloud speichert Fotos. Eine Musik-Cloud speichert Musik. Die Arztgeheimnis-Cloud speichert Arztgeheimnisse - wenn wir das wirklich wollen. Ich plädiere für eine sorgfältige Nutzen-Risiko-Abwägung. Selbstverständlich hat die Cloud-Speicherung von Patienteninformationen einen Verfügbarkeitsvorteil. Aber ist der medizinische Nutzen wirklich groß genug, um die Risiken zu rechtfertigen? Man muss ich klar machen, dass der persönliche Schaden bei Gesundheitsdaten-Missbrauch irreparabel sein kann, da reicht es nicht, einen Account zu löschen oder ein Passwort zu ändern. Und wie ist die Rechtslage/ Haftungsfragen, wenn wie ein einigen Ländern schon geschehen nicht nur einzelne sondern gleich Millionen Patienten-Datensätze entwendet werden, mit denen jetzt schon ein lukrativer Handel im Darknet betrieben wird?

Authentischer Begriff für „Zentrale Telematik-Infrastruktur“: ARZTGEHEIMNIS-CLOUD

Wissen wir, was wir tun, wenn wir die dauerhafte Gesundheitsdaten-Cloudspeicherung favorisieren?
Dieser Satz findet sich auch auf der beigefügten Grafik. Ab hier ergänzt dieser Text die beigefügte Grafische Darstellung.
* Im Zentrum steht die „Wolke“= Cloud. Sie ist die Schaltstelle und Umschaltstelle für Alles, was im Netzwerk passiert. Während traditionell der Hausarzt die Arztberichte seiner

Patienten in seiner Praxis sammelt (und als lokaler Akteur dem einzelnen Patienten seine Patientenakte auch zur Verfügung stellen kann, analog oder digital), soll dies nun in der Arztgeheimnis-Cloud für die gesamte Bevölkerung geschehen (nach aktuellem Stand noch als „freiwillige Anwendung“).
Kurz die Stichworte der Grafik:
* Funktion Versicherten-Stammdaten-Management VSDM: Die erste Anwendung der TI. Keine medizinische Anwendung, sondern bürokratisch, Abgleich der Verwaltungdaten auf der eGesundheitskarte mit dem Datenstand im Krankenkassen-Server. Dies ist sozusagen der Test der digitalen Infrastruktur auf Funktionsfähigkeit. Außerdem die Verlagerung von Verwaltungstätigkeit der Kassen in die Arztpraxen sowie (vielleicht) die Einsparung von Verwaltungskosten bei den Kassen.
* Dann der Notfalldatensatz NFDM: vielleicht auch „erweiterter Notfalldatensatz“. Dann sind es nicht nur Allergien und Unverträglichkeiten, sondern auch die wichtigsten Dauerdiagnosen, denn erst dann hat der Datensatz relevante Bedeutung. Diese zweite Anwendung ist psychologisch geschickt gewählt. Denn der Notfalldatensatz passt tatsächlich noch auf die eGesundheitskarte, ist also tatsächlich AUF DER KARTE gespeichert, so dass die dauerhafte zentrale Speicherung noch im Nebel bleibt. Aus meiner Sicht ist der Notfalldatensatz in der Form wenig praxisrelevant und vor allem ein Akzeptanzvehikel.
* Nun der Medikationsplan. Den gibt es schon, auf Papier. Den gab es auch schon immer, auf Papier. Auch der würde noch AUF DIE KARTE passen, natürlich mit „Original“ in der Cloud. Wirklich praktikabel ist der Medikationsplan, wenn jederzeit durch Tastendruck ein Ausdruck davon angefertigt werden kann, und zwar in der AKTUELLEN Form, allein schon deshalb, weil der Patient den Plan als Einnahmeplan benötigt. Der jederzeit aktuelle und medizinisch auf Indikation, Interaktion und auf patientenindividuelle Besonderheiten geprüfte Medikationsplan wird aber nur dann funktionieren, wenn für seine Anfertigung EIN Arzt hauptverantwortlich ist, in der Regel der Hausarzt. Wenn das nicht geregelt ist, wird aus dem System, das unerwünschte Wirkungen und Wechselwirkungen vermeiden soll, eine potentielle medikamentöse Gefahr für den Patienten, zumindest aber ein fürchterliches Durcheinander mit Tendenz zur Polymedikation.
* Jetzt der eArztbrief. Stimmt, es ist dringend notwendig, in Zukunft Arztberichte von Ärzten und Krankenhäusern in digitaler gesicherter/verschlüsselter Form zu versenden. Im TI-System gibt es das noch nicht. Es existiert in Anfängen im KV-Connect-System der Kassenärztlichen Vereinigungen. Man könnte das auch so machen, dass die Informationsübermittlung Punkt-zu-Punkt ist, das heißt, die Nachricht wird nach Abruf durch den Empfänger automatisch im Zwischenspeicher gelöscht. In der Arztgeheimnis-Cloud ist das definitiv NICHT Punkt-zu-Punkt, im Gegenteil. Grundprinzip ist ja gerade, dass alle medizinischen Dokumente nicht nur versendet und abgerufen werden, sondern dauerhaft gespeichert bleiben. Womit wir wieder beim kollektiven Datenschutz-Risiko wären.

Der Kern der Cloud: die Elektronische Patientenakte ePA

* Damit kommen wir zur wichtigsten Komponente der Cloud-Speicherung: die elektronische Patientenakte. Dort werden (beim jetzigen Stand der Dinge nur mit Zustimmung der Patienten) ALLE Berichte dauerhaft gespeichert, damit jeder behandelnde Arzt bei Vorlage der eGK, PIN-Nummer sowie Vorhandensein von Arztausweis/ Praxisausweis die Berichte des Patienten zu jeder beliebigen Zeit rund um die Uhr abrufen kann. Inwieweit der Arzt die wirklich dringenden Dinge wie aktuelle Diagnosenliste und aktuellen Medikationsplan findet, ist eine andere Frage, siehe weiter unten.
* Telemedizin: Behandlung /Beratung auf Entfernung. Machen Ärzte schon lange, nämlich meist per Telefon. Telefonisch lassen sich sehr viele Fragen und Probleme lösen. Der Hausarzt-Alltag wäre gar nicht zu bewältigen, wenn jede Fragestellung im persönlichen Arzt-Patient-Kontakt bearbeitet werden müsste. Nun kommt telemedizinisch die Video-

Komponente dazu. Das sieht gut aus, ergibt ein gutes Marketing, aber der Zusatznutzen ist noch nicht bewiesen. Zudem ist die Videosprechstunde technisch aufwändig und dauert länger als eine normale Konsultation. Mit Sicherheit ersetzt in ländlichen Gebieten die Telemedizin nicht die externe Versorgungsassistentin.
* BIS HIERHIN kann man den medizinischen Sinn bei Vielem noch erkennen und mit viel gutem Willen und Vertrauen an die Möglichkeit einer hohen Datensicherheit glauben. Aber nun, wir sind im Zeitalter von Handy-Apps und BigData, wird es noch viel komplizierter.

BIG DATA in den Startlöchern

* Jetzt kommt nämlich die elektronische GESUNDHEITSakte eGA ins Spiel. Ja, das ist etwas anderes als die ePatientenakte. Hier sind die Krankenkassen am Zug. Krankenkassen dürfen nämlich keine eigenen Patientenakten führen. Nun ist die eGA so eine Art Teilmenge der ePA, nämlich der Teil, den der Patient sehen darf im PC oder Handy. Zusätzlich kann der Patient eigene Daten, z.B. Handy-App-Daten von Fitnesstrackern, in seine Gesundheitsakte laden und wenn er möchte, irgendwann dem Arzt vorlegen. Das alles läuft unter der Flagge der Krankenkassen. Wer als Patient dem zustimmt, leistet sozusagen eine freiwillige Datenspende an seine Krankenkasse. Ob dadurch die medizinische Behandlung besser wird, ist sehr fraglich. Mit Sicherheit aber ist per Datenanalyse eine bessere Selektion von Patientenrisiken möglich. Insofern ist es kein Zufall, dass die diesbezüglichen (unterschiedlichen) Projekte von Krankenversicherungsunternehmen massiv unterstützt werden, von IT-Firmen sowieso. Die derzeit wohl bekannteste eGesundheitsakte über die Vivy-App hat übrigens einen eigenen Server in Frankfurt, der an die TI angeschlossen werden soll. Beteiligte gesetzliche Krankenversicherungen sind DAK, IKK, und BKKen. Mit an Bord auch private Versicherer wie Allianz, Gothaer, Barmenia. Der Datenschutzerklärung von Vivy ist zu entnehmen, dass verschiedene Dienste (auch in den USA) genutzt werden, um die Daten zu unterschiedlichen Zwecken zu verwenden, zum Beispiel für Werbung und Benutzerunterstützung.
* Bis hierhin war das vielleicht noch „Small Data“. Wenn aber irgendwann massive Datenmengen in der Arztgeheimnis-Cloud angesammelt sind, dann wird es für die Big-Data-Firmen interessant. In den Startlöchern stehen private Krankenversicherungen, gesetzliche Krankenkassen, Krankenhauskonzerne und IT-Firmen wie Bitmarck, IBM. Je größer der Datenpool, desto mehr Interessenten werden folgen. Und wie es scheint, ist es den Lobbyisten gelungen, die entsprechenden Türen vorsorglich offen zu halten. Die Betreiber der Arztgeheimnis-Cloud selbst ist übrigens die Bertelsmann-Tochter ARVATO.
* Mit diesen zusätzlichen Zugangswegen wird die Frage der Datensicherheit endgültig ad absurdum geführt.

App-Zugang oder: die Selbstvernichtung der Datensicherheit

Bezüglich der Digitalen Rückständigkeit der Bundesrepublik Deutschland wird oft auf das Beispiel von Estland verwiesen, wo es schon seit über 15 Jahren eine Zentrale Datenspeicherung von Patientendaten gibt. In Estland damals unter völlig anderen Bedingungen: EINE Krankenkasse für alle Esten. Damit gleiche Bedingungen für alle und keine Konkurrenz von Krankenkassen untereinander. Hoher Grad von Gemeinwohlorientiertheit und Transparenz. Damals Big Data noch kein Thema. Keine Großkonzerninteressen. Keine Pharmaindustrie. Ob das auf Dauer gut gehen wird in Estland, weiß ich nicht. Jedenfalls sind die Voraussetzungen ganz anders als in Deutschland. Jedenfalls sind Norwegen, Dänemark, USA bereits Millionen von Patientenakten gehackt worden.

Ansonsten möchte ich -gerade auch aus hausärztlicher Sicht- eine Art Lackmustest für die

Digitalisierung im Gesundheitswesen anregen, basierend auf einer einfachen Erkenntnis: Digitalisierung betreffend einer konkreten Problemstellung ist nur dann sinnvoll, wenn sie mehr kann, als schon analog geht. Wie folgt:

Was für die allgemeine Patientenbehandlung und im Notfall unbedingt nützlich ist....

Das wichtigste Informations-Werkzeug im Gesundheitswesen ist eine aktuelle Diagnosenliste (mit Unverträglichkeiten/ Allergien) in Verbindung mit einem aktuellen Medikationsplan. Die Kombination aus beidem nenne ich Diagnosen-Medikations-Dokument. Bei unseren Patienten ist das ein DIN-A4 Ausdruck, der in Sekundenschnelle aus dem Praxisverwaltungssystem ausgedruckt werden kann und in die Hände des Patienten gegeben wird. Bei jeder Änderung von Medikamenten, Dosierungen, Diagnosen, Unverträglichkeiten (das passiert etwa bei jedem 2. oder 3. Patientenkontakt!) wird neu ausgedruckt. Das Dokument kann der Patient selbst lesen. Er kann Fragen dazu stellen. Er kann Fehler erkennen, die ich vielleicht als Arzt beim Eintragen gemacht habe. Er kann selbst entscheiden, welchem Facharzt oder Krankenhaus er das Dokument vorlegt.
Nun der Test: schafft es eine Digitales System wie die TI / Arztgeheimnis-Cloud, diese alltagsrelevanten Informationen (mit denen sich übrigens JEDER Notfall bewältigen lässt) genauso sicher, unkompliziert und praktikabel zur Verfügung zu stellen, wie das Stück Papier namens Diagnosen-Medikamenten-Dokument? Oder finden sich die relevanten Informationen lediglich in einem Meer von Datenmüll nach stundenlangem Suchen und nur unter der Voraussetzung, dass der Arzt Internetverbindung hat?

Aus Digitalisierung wird Digitalismus

Abschließend zur Digitalen „Rückständigkeit“ in Deutschland. Inzwischen hat man den Eindruck, aus Digitalisierung ist eine Art Digitalismus geworden, eine Entwicklung, die wie ein Schicksal hinzunehmen sei und nicht hinterfragt werden darf. Wie wäre es denn, wenn wir zurück auf den Boden der Demokratie kommen, den Patienten die ehrlichen Fragen stellen, und danach mit Patienten und Ärzten zusammen die fraglos großen Möglichkeiten digitaler Technik praxistauglich nutzen: Einfache und praktikable Punkt-zu-Punkt-Kommunikation, Erleichterung des Alltages, Verbesserung der Versorgung bei akzeptablen Datenschutzrisiken? Vielleicht sind wir ja demnächst NICHT RÜCKSTÄNDIG, sondern das einzige Land weltweit, in dem einerseits ein funktionierendes digitales Informationsaustauch-System im Gesundheitswesen OHNE dauerhafte zentrale Speicherung von Patienteninformationen existiert und anderseits die Arztgeheimnisse der Patienten NICHT gehackt worden sind und auch nicht gehackt werden können. Und die komplette Patientenakte? Die kann als digitale Kopie der lokalen, hausärztlichen Daten auch heute schon mit wenig Aufwand dem Patienten in verschlüsselter Form an die Hand gegeben werden, wenn der Patient das wünscht.

Eine sehr alte Regel, die noch immer gilt

Wir Ärzte würden dann das tun, was wir seit Altertum schon immer tun sollten: Primum nil nocere. Vor allem nicht schaden. Die notwendige Abwägung von Nutzen und Schaden gilt nicht nur für Medikamente und Operationen, sondern auch für die Verwendung von Technik. Der Gegner dieser Menschlichkeit in der Medizin sind Machtverhältnisse und Profitinteressen bei einem gleichzeiten Defizit von Demokratie.
Genau deshalb nochmal die Frage: Wissen wir, was wir tun?

Wilfried Deiß, Hausarzt-Internist, Siegen Januar 2019