

Zentrale Telematik-Infrastruktur – die Arztgeheimnis-Cloud

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

Central Telematic Infrastructure – the Medical Secrecy Cloud Digitalization of Health Care: a Patient-Oriented Plea for More Democracy and Understandable Terminology

Wilfried Deiß

Die Digitalisierung der innerärztlichen Kommunikation betrifft jeden aktuellen oder potenziellen Patienten, somit die gesamte Bevölkerung. Das zentrale Projekt dazu ist in Deutschland die elektronische Gesundheitskarte/Telematik-Infrastruktur. Obwohl jeder betroffen ist, ist der Informationsstand der Bevölkerung auffällig schlecht. Insbesondere über den Kern des Projekts, die elektronische Patientenakte, besteht Unwissenheit. Es handelt sich nämlich um eine zentrale, dauerhafte Cloud-Speicherung von intimen Patientendaten, die dem Arztgeheimnis unterliegen. Der Autor plädiert für mehr Offenheit, mehr Demokratie und verständliche Erklärungen.

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 z.T. nicht verstanden, worum es geht.

Und die Patienten? Bei ihnen ist erwartungsgemäß der Informationsstand noch schlechter. Die elektronische Gesundheitskarte ist inzwischen bekannt als Versichertenkarte mit Foto, und manche Patienten haben gehört, dass irgendwann die per-

sönlichen 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 [1].

Diese Desinformation ist allerdings kein Zufall. Seit Start des Projekts eGesundheitskarte/Telematik-Infrastruktur 2005 bleibt die Notwendigkeit der zentralen Datenspeicherung als Kern des Gesamtprojekts systematisch 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. Meine 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 potenziell repräsentative Hände geraten.

Eine gesicherte digitale Informationsübertragung im Gesundheitswesen

Kurz ein Schritt zurück in der Technik-Historie zum Hightech der 70er- und 80er-Jahre. Als damals die Faxgeräte aufkamen, musste niemand aufwendig zur Anschaffung überzeugt oder gezwungen werden. Der Sinn und die Praktikabilität/Alltagstauglichkeit des Geräts waren sofort zu erkennen. Beim Telematik-Projekt gibt es nicht einmal ein vollständig funktionierendes Modellprojekt, an dem man Praktikabilität und Nutzen zumindest der wichtigsten medizinischen Anwendungen überprüfen hätte können.

Retrospektiv ist das Faxgerät (in seiner ursprünglichen, analogen Form) zudem ein gutes Beispiel für den Unterschied zwischen Einzelfallrisiko und Kollektivrisiko. Faxen ist eine Punkt-zu-Punkt-Kommunikation (heutzutage sind allerdings Fax-Server dazwischengeschaltet, 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 [2].

Unehrlige oder ehrliche Fragen an Patienten?

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, mithilfe 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?“

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 oder vielleicht noch Gesundheitsdaten-Cloud, sondern stattdessen: **Arztgeheimnis-Cloud**. Es sind nämlich ganz besondere Daten, um die es hier geht, nicht die üblichen Nutzerdaten, die bei Facebook, Whatsapp, Amazon, Google anfallen (und selbst da ist das Missbrauchspotenzial 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? Wo sind die großen Modellversuche, die den Nutzen nachweisen? Man muss sich klarmachen, dass der persönliche Schaden bei Gesundheitsdaten-Missbrauch irreparabel sein kann, da reicht es nicht, einen Account zu löschen oder ein Passwort zu ändern [2]. Und wie sind Rechtslage/Haftungsfragen, wenn wie in 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? Sicher ist, dass die erforderliche Einverständniserklärung des Patienten die Risiken auf den Patienten verlagern wird.

Authentischer Begriff: Arztgeheimnis-Cloud

Wissen wir, was wir tun, wenn wir die dauerhafte Gesundheitsdaten-Cloud-Speicherung favorisieren (Abb. 1)?

- Im Zentrum der Abbildung 1 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 schon heute sehr einfach zur Verfügung

stellen kann, herkömmlich analog auf Papier oder zeitgemäß digital, z.B. auf speziellen USBSticks [3]), soll dies nun in der Arztgeheimnis-Cloud für die gesamte Bevölkerung geschehen (nach aktuellem Stand noch als „freiwillige Anwendung“).

- **Versicherten-Stammdaten-Management (VSDM):** Die erste Anwendung der TI. Keine medizinische Anwendung, sondern eine bürokratische: Abgleich der Verwaltungsdaten auf der eGesundheitskarte mit dem Datenstand im Krankenkassen-Server. Dies ist sozusagen der Test der digitalen Infrastruktur auf Funktionsfähigkeit. Außerdem die Verlagerung der Verwaltungstätigkeit der Kassen in die Arztpraxen sowie (vielleicht) die Einsparung von Verwaltungskosten bei den Kassen.
- **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, sodass die dauerhafte zentrale Speicherung noch im Nebel bleibt. Aus meiner Sicht ist der Notfalldatensatz in der Form wenig praxisrelevant und vor allem ein Akzeptanzvehikel.
- **Medikationsplan:** Den gibt es schon auf Papier, und 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 digital gespeicherte 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

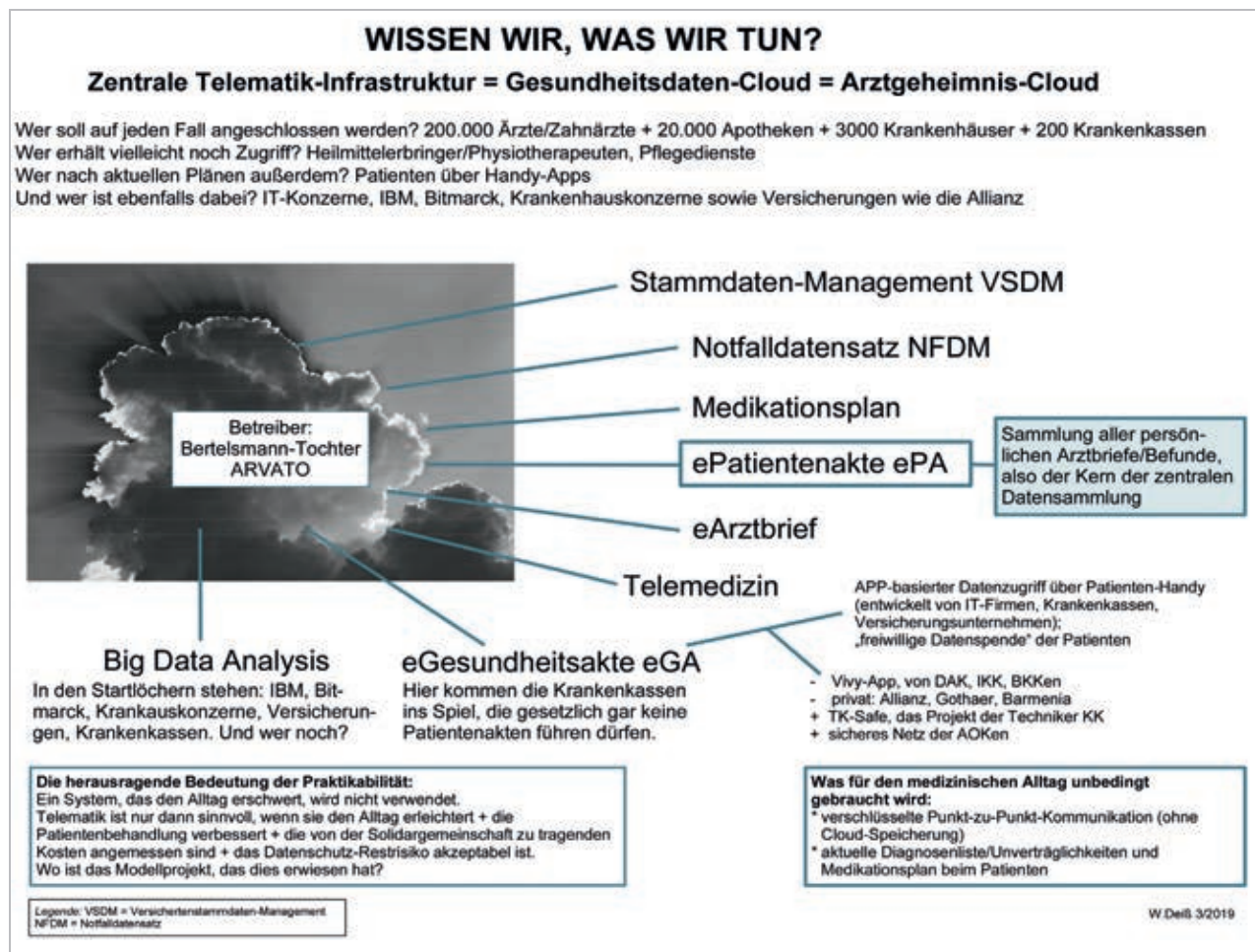


Abbildung 1 Arztgeheimnis-Cloud

Hausarzt. Wenn das nicht geregelt ist, wird aus dem System, das unerwünschte Wirkungen und Wechselwirkungen vermeiden soll, eine potenzielle medikamentöse Gefahr für den Patienten, zumindest aber ein Durcheinander mit Tendenz zur Polymedikation [4].

- eArztbrief: Dass es dringend notwendig ist, in Zukunft Arztberichte von Ärzten und Krankenhäusern in digitaler gesicherter/verschlüsselter Form zu versenden, stimmt. Im TI-System gibt es das noch nicht. Es existiert in Anfängen im KV-Connect-System der Kassenärztlichen Vereinigungen [5]. Man könnte die Informationsübermittlung auch Punkt-zu-Punkt gestalten, d.h., die Nachricht wird nach Abruf durch den Empfänger automatisch im Zwischenspeicher gelöscht. In der Arztgeheimnis-Cloud ist es definitiv nicht Punkt-zu-Punkt, im Gegenteil. Grundprinzip ist ja gera-

de, dass alle medizinischen Dokumente nicht nur versendet und abgerufen werden, sondern dauerhaft gespeichert bleiben. Womit wir wieder beim kollektiven Datenschutz-Risiko sind.

- Der Kern der Cloud: die elektronische Patientenakte ePA: 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 Informationen wie aktuelle Diagnose-Liste und aktuellen Medikationsplan findet, ist eine andere Frage, siehe weiter unten [6].
- 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 ist 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 aufwendig und dauert länger als eine normale Konsultation. Mit Sicherheit ersetzt in ländlichen Gebieten die Telemedizin nicht die externe Versorgungsassistentin [7]. 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 Big Data, wird es noch viel komplizierter [8].

- Elektronische Gesundheitsakte (eGA): 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 eine Art Teilmenge der ePA, nämlich der Teil, den der Patient im PC oder auf dem Handy sehen darf. 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 sind 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, z.B. für Werbung und Benutzerunterstützung [6].
- Bis hierhin ist das vielleicht noch Small Data. Wenn sich aber irgendwann massive Datenmengen in der Arztgeheimnis-Cloud angesammelt haben, 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 den zusätzlichen Zugangswegen über Handys wird die Frage der Datensicherheit endgültig ad absurdum geführt. Diesbezüglich verweise ich auf den letzten Kongress des CCC, Chaos-Computer-Club, und die dortigen Gefahrenanalysen bezüglich Patientenakten/ Gesundheitsakten [2, 9].

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 entstand das damals unter völlig anderen Bedingungen: eine Krankenkasse für alle Esten. Damit gelten gleiche Bedingungen für alle, und es gibt



Wilfried Deiß ...

... Facharzt für Innere Medizin und Hausarzt. Jahrgang 1960, seit 1997 niedergelassen als Hausärztlicher Internist in Siegen/Nordrhein-Westfalen.

keine Konkurrenz von Krankenkassen untereinander. Damit einher geht ein hoher Grad von Gemeinwohlorientiertheit und Transparenz. Big Data war damals noch kein Thema, es gab auch keine Interessen von Großkonzernen und der Pharmaindustrie. Ob das in Estland auf Dauer gut gehen wird, weiß ich nicht. Jedenfalls sind die Voraussetzungen ganz anders als in Deutschland.

In Norwegen, Dänemark und den USA sind bereits Millionen von Pa-

tientenakten gehackt worden [2]. Patientenakten werden aktuell im Internet für etwa 60–100 Dollar gehandelt, bestens geeignet für Identitätsdiebstahl oder Erpressungen.

Ansonsten möchte ich – gerade auch aus hausärztlicher Sicht – eine Art Lackmuestest für die Digitalisierung im Gesundheitswesen anregen, basierend auf einer einfachen Erkenntnis: Digitalisierung bezüglich 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 Informationswerkzeug im Gesundheitswesen ist eine aktuelle Diagnoseliste (mit Unverträglichkeiten/Allergien) in Verbindung mit einem aktuellen Medikationsplan. Die Kombination aus beidem nenne ich Diagnosen-Medikations-Dokument. Bei unseren Patienten ist das ein im lokalen Praxisverwaltungssystem digital gespeichertes Dokument, aus dem mit einem Tastendruck ein DIN-A4-Ausdruck erstellt werden kann. Dieses wichtige Blatt Papier gibt der Arzt persönlich in die Hand des Patienten. 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 Spezialisten oder Krankenhaus er das Dokument vorlegt.

Nun der Test: Schafft es ein 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 noch eine Anmerkung 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,
- Vermeidung des Kollektiv-Datenrisikos bei Akzeptanz eines geringen Einzelfall-Restrisikos unter der Voraussetzung des nachgewiesenen medizinischen Nutzens,
- Erleichterung des medizinischen Alltages,
- Verbesserung der Versorgung.

Vielleicht sind wir ja demnächst nicht rückständig, sondern das einzige Land weltweit, in dem einerseits ein funktionierendes digitales Informationsaustauschsystem im Gesundheitswesen ohne dauerhafte zentrale Speicherung von Patienteninformationen existiert

und andererseits 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 dem 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 gleichzeitigen Defizit von Demokratie.

Genau deshalb die Frage: Wissen wir, was wir tun?

Interessenkonflikte:

Keine angegeben.

Literatur

1. Grätzel von Grätz P. E-Akte: gematik will Serverakte mit variablen Zu-

griffsrechten. Ärztezeitung, 4. Juni 2018

2. Wasner A. Schaden für den Einzelnen unheilbar – Berufshacker deckt Sicherheitsmängel in E-Health-Anwendungen auf. Medical Tribune, 18. Jan 2019, S. 24
3. Sichere Lokale Patientenakte auf USB-Stick. www.sichere-patientenakte.de/index.php?page=sitemap&f=2 (letzter Zugriff am 21.2.2019)
4. Korzilius H, Osterloh F. Medikationsplan im Praxistest. Dtsch Arztebl 2018; 115: A-364
5. Brief ohne Marke – der Elektronische Arztbrief ermöglicht die sichere Kommunikation in Echtzeit. KVWL kompakt 2018; 10: 14
6. EFA, EPA und Co – Was können die verschiedenen elektronischen Aktensysteme und wer steckt dahinter? KVWL kompakt 2019; 1: 4
7. Glied K. Auch Telemedizin will gelernt sein. Allgemeinarzt 2019; 41: 34–36
8. Capurro R. Digitalisierung in der Medizin – Skepsis gegenüber Hype. Dtsch Arztebl 2018; 115: A-1425
9. 35th Chaos Communication Congress 2018. <https://youtu.be/82Hfh1AltiQ> (letzter Zugriff am 21.2.2019)

Korrespondenzadresse

Wilfried Deiß
Koblenzer Str. 109, 57072 Siegen
praxis.deiss@posteo.de



DEGAM-NEWSLETTER

Immer gut informiert

Seit einigen Jahren verschickt die DEGAM-Bundesgeschäftsstelle exklusiv an die Mitglieder den E-Mail-Newsletter DEGAM aktuell. Dieser Informationsdienst beinhaltet Neuigkeiten aus dem Präsidium, den Sektionen und Arbeitsgemeinschaften sowie der Leitlinien-Geschäftsstelle und der JADE. Auch aktuelle Mitteilungen zu den Rubriken Personalia, Veranstaltungen und Stellenausschreibungen finden sich im Newsletter. Die bisher versandten Ausgaben können im passwortgeschützten internen Bereich unter

www.degam.de

eingesehen werden. Sind auch Sie an den aktuell in der DEGAM diskutierten Themen und Entwicklungen interessiert? Schicken Sie einfach eine E-Mail mit dem Betreff „DEGAM aktuell“ an:

geschaeftsstelle@degam.de