Des Kaisers neue Kleider

Seit drei Monaten erhält eine von mir in der IT betreute Zahnarztpraxis Angebote ihres Dentalsoftwarelieferanten (System CGM Z1, VPN-Konnektor ca. 2600 €, neues Kartenterminal ca. 400 €, Installation und weitere Chipkarten zur Identifikation ca. 900 €, laufender Betrieb je Monat zus. ca. 80 €.)

Ich war nun gefordert, mich auch mit dem Thema der Telematik genauer auseinanderzusetzen. Mir war bekannt, dass der Gesetzgeber eine für den Zahnarzt kostenneutrale Einführung der Telematik über Kostenerstattung vorgesehen hat.
(§ 291a Sozialgesetzbuch V, „Wer zahlt dafür und wie erhalte ich mein Geld?“ Link + Pauschalen)

Ein Vergleich der Kostenerstattungspauschalen und dem Angebot ergab die 100% Übereinstimmung, wenn das „Early-Bird“ Angebot wahrgenommen wird. Durch einen Anruf beim Softwarehersteller wurde mir dies so bestätigt. So weit, so gut.

Nebenbei bemerkt, die Auswahl einer Praxisverwaltungssoftware ist ein Vendor lock-in Link. Friss oder Stirb heißt es da für alle Folgeprodukte.

Die von der Kassenzahnärztlichen Bundesvereinigung KZBV vorgegeben Kostenpauschalen nehmen ab Ende 2017 stetig ab. Es gilt für die Auszahlung das Datum der Installation und nicht das Datum der Bestellung.

Organisatorisch ist es mir schleierhaft, wie das Monopol CGM an die 200.000 VPN-Konnektoren rechtzeitig bereitstellt und technisch so aktivieren kann, dass die Kassenzahnärztlichen Vereinigungen auch den 100% Zuschuss bezahlen. (Nun sollen ev. noch T-Systems u. RISE im Frühjahr 2018 hinzukommen.)
Ich habe daraufhin einen Vertreter einer Kassenzahnärztlichen Vereinigung zu diesem Widerspruch gefragt, der mir dies auch so bestätigt hat - die Pauschalen sind halt so mit den Herstellern (genauer dem einem Hersteller!) ausgehandelt. Es scheint also so gewollt, dass es nichts mit kostenneutraler Einführung für eine Zahnarztpraxis wird.

Verweigert ein Zahnarzt die Teilnahme an der Telematik, würden nach der Übergangsfrist sogar 1% seiner Auszahlung als Zwangsmaßnahme von der Kassenzahnärztlichen Vereinigung einbehalten werden. Mit der Peitsche wird hier versucht ein System einzuführen. Das Zuckerbrot sehe ich nicht, denn der kostenneutrale Ansatz für den Zahnarzt und die Absenkung der Kostenpauschalen, um die Praxen zur schnellen Einführung der Telematik zu bewegen, beinhaltet sogar einen Verlust für den Zahnarzt. Aus sicherheitstechnischer und organisatorischer Sicht gibt es noch weitere Gründe, die Telematik nicht einzuführen, dazu aber später.

Die Kassenzahnärztliche Vereinigung schiebt den schwarzen Peter auf die Ärzte, die sollen sich halt einen günstigeren Anbieter für die Telematik suchen. Welche das sein sollen (T-Systems ?, RISE ?) ist bisher noch offen, aber schnell eingeführt soll es werden, sonst drohen dem Arzt finanzielle Verluste...
Gerade weil ein Zahnarzt an seine Praxissoftware gebunden ist und diese mit dem VPN-Konnektor (Treibersoftware im PC) zusammenarbeiten soll, kann er als Dienstleister für die Installation nur seinen Softwarelieferanten der Praxisverwaltung und den vom ihm vorgegebenen VPN-Konnektor wählen.

Dieses Monopol nutzt zumindest unser Softwarehersteller aus, denn nur er ist auch berechtigt, die Telematik zu installieren (nur wer von der Gematik zertifiziert ist - noch so ein Punkt). Ich bin als bisheriger IT-Betreuer nicht zugelassen, die zwei weiteren Geräte an einen Praxis PC und den Internet-Router anzuschließen und den Software-Treiber zu installieren. Das wäre für weit unter 900 € Installationspauschale bei mir möglich. (Alles andere, also PC-Hardware, Router, Software-Updates und sogar das zertifizierte Praxisverwaltungssystem mit dem ZOD-Kartenleser, durfte ich noch selbst installieren – na mal sehen, wann sich das auch ändern wird.)
Kleinere Marktanbieter für Praxissoftware und IT-Betreuung können, aufgrund der geringen Kundenanzahl, ihre Anpassungs- und Zertifizierungskosten vermutlich noch schlechter ihre Kalkulation in den (Betriebs-)Pauschalen unterbringen und werden noch mehr vom Arzt verlangen müssen.
Zahnärzte, die eine Praxis neu gründen, überlegen sich dann eher einen günstigeren Marktführer zu wählen, wenn eine Entscheidung zur Praxissoftware anliegt. Neben der erzwungenen Techniker-Zertifizierung wird dieses die Marktteilnehmer auf wenige Großanbieter reduzieren.

Möglicherweise könnte ein Verweigerer die einbehaltenen 1% einklagen, da die Kassenzahnärztliche Vereinigung ihrer Verpflichtung der 100% Kostenübernahme ja auch nicht nachkommt, weil sie die Pauschalen stetig senken und die Anbieter mit ihren Preisen nicht nachziehen.
Eine Klage von einzelnen Zahnärzten wird vermutlich nicht erfolgen, denn sie stehen in einem starken Abhängigkeitsverhältnis von ihren Kassenzahnärztlichen Vereinigungen, besonders wenn sie einen Großteil ihres Einkommens über Kassenpatienten erwirtschaften. Zudem wurde von einem Vertreter einer Kassenzahnärztlichen Vereinigung angedeutet, dass Verweigerer mit weiteren Zwangsmaßnahmen zu rechnen hätten.
Ich kann mir gut vorstellen, dass ein renitenter Zahnarzt dann halt mal zu einem persönlichem Informationsgespräch zur Kassenzahnärztlichen Vereinigung eingeladen wird, um über seine Punktestatistik und einen eventuellen Einbehalt von Teilen der Auszahlung oder eine Strafzahlung zu diskutieren.
- Also lieber die Kröte schlucken. -
(Dieser Sachverhalt ist den auserwählten Hof-Lieferanten der Telematik selbstverständlich bekannt und bietet sich als solide Grundlage für deren Preisgestaltung geradezu an;-)

Nicht jeder Zahnarzt hat die erforderliche Grundausstattung in Hard- und Software für die Telematik (Internetzugang, Router, und Betriebssystem ab Win7, ja es gibt noch Praxen mit win95! und DOS "Der Zahnarztrechner"..-) und wird nun gezwungen aufzurüsten. (In wie weit ein technisches Upgrade ansonsten sinnvoll erscheint, will ich hier nicht diskutieren.)

Warum müssen sich die (Zahn-)Ärzte um die Details der Telematik, also Kosten und Verträge zur Technikorganisation kümmern? Die KZBV scheint kein Interesse an effizienter Unterstützung der Zahnärzte beim Rollout zu haben.
Wäre es nicht ihre Aufgabe sämtliche Kosten für Installation und Betriebsaufwand mit den Herstellern selbst zu regeln? Das wäre für mich fast (bis auf Strom und etwas Mehrarbeit) 100% kostenneutral für den Zahnarzt.

Im übrigen wird eine Reduktion der Pauschalen mit der Anzahl zunehmender Wettbewerber (aktuell nur einer!,Jan. 2018) und der dadurch sinkenden Kosten begründet. Dem Zahnarzt entstehen also keine weiteren Kosten, wenn er später den Auftrag gibt?
Ein kostenbewusster Zahnarzt wartet den Preisverfall ab. Die billigeren Angebote sind dann doch eher ein Argument, die Telematik möglichst spät einzuführen, oder?

Aufgrund der erforderlichen Gematik-Zertifizierung für die Techniker und momentan nur einem VPN-Konnektor-Anbieter, erscheint mir der Preisverfall der VPN-Konnektoren als sehr unwahrscheinlich. (Zumindest bisher zeigen sich keine Preisänderungen in den Angeboten von CGM/Feb 2017. Ich könnte also mit meiner These recht haben.) Es wird vermutlich so kommen, dass die Angebote des Herstellermonopols oben bleiben, die Ärzte aber nur noch die dann aktuelle Kostenpauschale erstattet bekommen. -Es war ja von der KZBV schließlich so festgelegt -. Diese Diskrepanz wird in den Werbeanzeigen sehr schön mit „.. Sichert ihnen damit die maximale finanzielle Förderung“/CGM) umschrieben.

Eine subtile Ungewissheit scheint beabsichtigt zu sein, um die Zahnärzte zur schnellen Einführung der Telematik zu bringen und nötigt sie quasi den teuren Vertrag ihres Softwareherstellers vorzeitig abzuschließen. Hier wird meiner Ansicht nach das Wirtschaftlichkeitsgebot ausgehebelt. Zudem sieht das Gesetz (immer?) eine 100% Kostenübernahme der Kassenzahnärztlichen Vereinigungen vor. Ist die Regelung mit den Pauschalen dann überhaupt so zulässig? Letzten Endes ist es zu immer Lasten der Versicherten und Patienten, das muss hier mit erwähnt werden.

Mit dieser Flexibilität in der Auslegung von Gesetzen hätte eine ernsthafte Zahnärztevertretung die Zwangs-Telematik ganz verhindern können.

Mit dem Konstrukt der Entkopplung von Kostenübernahme (Pauschalen) und dem davon getrennten Vertragsabschluss mit dem Softwarehersteller/Dienstleister, wird das Kostenrisiko von den Kassenzahnärztlichen Vereinigungen auf die Zahnärzte verlagert.
Ein großer Anbieter hat es nun einfacher, einen zusätzlichen Gewinn über unzureichend organisierte Zahnärzte einzustreichen, da hier nicht ansatzweise in Augenhöhe verhandelt wird. (Expertise im Verhandlungsgegenstand, keine Rabattverhandlungen bei Großabnahmen, keine technische Kompetenz und Überforderung der Zahnärzte, eine Vertragsgestaltung ist aufgrund der Hersteller/Softwareabhängigkeit faktisch nicht möglich). Für marktorientierte Unternehmen ist es selbstredend, die angebotenen Pauschalen bis zur Grenze auszunutzen und darüber hinaus ihre Zwangskunden, die keine Wahlmöglichkeit haben, noch weiter zu schröpfen. Mit der 1% Zwangsregelung vom Gesetzgeber, wurden die Zahnärzte an die Verkäufer ihrer Praxisverwaltungs-Software ausgeliefert.
Die Erwartungshaltung der Aktionäre von CGM bestätigt mir das zumindest bis Ende 2017 (Link Group_Medical-Aktie).

Der Telematik-Vertrag mit CGM ist auf 2 Jahre begrenzt. Was passiert danach? Kann dann ein anderer Anbieter gewählt werden, wenn die Betriebskosten/Mietkosten der PC-Software (bestimmt) angehoben werden. Einen Wechsel halte ich aufgrund des Vendor lock-ins für ausgeschlossen. Die KZBV entkoppelt sich auch hier von den zu erwarteten Kostensteigerungen.

Wird das Telematik-Projekt wieder erwarten doch eingestellt (keine Zuschüsse mehr etc.), bleiben die "Early Bird" Zahnärzte vermutlich, aufgrund der entkoppelten Verträge, auf ihren Vereinbarungen mit den Telematik-Lieferanten sitzen. Auch hier scheint die Kassenzahnärztliche Vereinigung das Ausfallrisiko durchzureichen. Sehr geschickt eingefädelt, muss ich schon sagen.

Wirkungsloser als Homöopathie

Gerade die Wirksamkeit/Effizient einer Maßnahme muss doch in der Medizin vorher nachgewiesen werden, um von den Krankenkassen bezahlt zu werden (s. § 12 SGB V Wirtschaftlichkeitsgebot Link). Hier fand ich nur die Argumentation der Krankenkassen, dass der Versicherungsbetrug, der in die Millionen durch Kartenbetrug geht, nur mit der eGk verhindert werden kann. Zahnärzte teilten mir mit, dass, seitdem es ein Patientenbild auf der eGk gibt, einen Betrugsversuch über Identitätsbetrug nur noch selten ist (Hinweise über die generelle rechtliche Problematik des Patientenbildes sind unter Link ab S. 4 zu finden). Hier fehlt es mir an Statistiken, die Kartenbetrug weiterhin als Argument bestätigen. Kartenbetrug ist ein sehr umfassender Begriff. Betrugsfälle wie hier(Link) können auch nicht durch einen Abgleich der eGk-Daten verhindert werden. Warum noch der technische Aufwand für den Abgleich? Warum soll ein geringer Schaden über wenige Millionen Euro einen Geldabfluss aus dem Gesundheitssystem über Milliarden Euro rechtfertigen?
Im übrigen wurden viele Patienten, die einen Identitätsbetrug begangen haben, ja auch behandelt. Wie vorgesehen wurde das Geld für die Gesundheit ausgegeben. Eine Solidargemeinschaft, nur halt eben nicht nachvollziehbar;-) Selbst Homöopathie trägt durch ihren Placeboeffekt mehr zur Heilung bei.
Mit der Telematik hofft man auf zukünftige Verbesserungen. Dem Gesundheitssystem werden aber vorerst permanent erhebliche Summen (s. u.) ohne Nutzen für die Versicherten entzogen. Selbstverständlich gibt es u. a. die Argumente zum besseren Austausch von Patienten- und Notfalldaten. Der bessere Austausch kann nur stattfinden, wenn die Patienten ihre Daten zur Verfügung stellen (dies ist freiwillig!). Sind diese neuen Anwendungen in ihrer Gesamtheit dann so effizient, um den Geldabfluss über Telematik durch Einsparungen kompensieren zu können? Denn erst ab hier ist der Break-Even Punkt erreicht. Ob dann wirklich ein Gewinn durch Telematik für das Gesundheitssystem entsteht, das steht für mich in den Sternen.

Einfache zielorientierte Maßnahmen (s. Patientenbild) wirken schon. Notfalldaten auf Papier, bei der eGk abgelegt, sind sogar ohne Lesegerät zu entnehmen. Da braucht es weder ein zeitintensives Auslesen der Daten vom Notfallhelfer, noch ein aufgeladenes Mobiles-Lesegerät (gibt es die überhaupt schon?).

Lizenz zum Geld drucken

Als ich das Angebot für die technische Infrastruktur gelesen hatte, fielen mir der Posten für den VPN-Konnektor auf. Ca. 2600 € sind für diese Box (KoCoBox MED+) vorgesehen (die selbstverständlich vom Hersteller auch abgerufen werden).
Mich würde interessieren, wie sich diese Kosten zusammensetzen? Ich habe hier den Eindruck, dass der Anwender und die KZBV mit diesen Modulkosten ziemlich übervorteilt wurden.
Für das KV-SafeNet gibt es auch zertifizierte VPN-Router, die allerdings bei weitem nicht so teuer sind (ab 189 € oder Mietbasis, Link). Warum werden diese nicht verwendet?
Generell können VPN-Verbindungen auch mit Software auf den Praxis-PCs selbst etabliert werden. Der oft schon vorhandene Praxisrouter (FritzBox/AVM, ca. 200 €) bietet ebenfalls einen VPN-Service an. Eine VPN-Verbindung kann auch über Minicomputer (bspw. RaspberryPi, ca. 30 €), aufgebaut werden. Kommerzielle VPN-Boxen kosten ab ca. 100 €.
Welche zwingenden technischen Anforderungen waren für die teure, ausgelagerte Hardwarelösung maßgebend? Die Übertragung der verschlüsselten Abrechnungsdatensätze mittels ZOD-Karte und zertifiziertem Kartenlesegerät (Bspw. Cherry ST-2000UCZ für nur ca. 50 €!) wird bisher auch ohne weitere VPN-Hardware über das Internet ermöglicht.

Die Spezifikation/Produktdatenblatt des VPN-Konnektors ist hier zu finden Link,
Beim BSI ist ein Zertifizierungsbericht mit weiteren technischen Details zu finden Link.
(Betriebssystem Linux Debian, CPU ist ein i.mx 6 ...).

Im Wesentlichen entspricht die Technik des VPN-Konnektors der eines Minicomputers (bspw. RaspberryPi), nur mit zus. zweitem LAN, kleines Display und 3 gSMC-K (vergleichbar mit den Sim-Cards im Smartphone).

Blicke ich mal über den Tellerrand, dann machen unsere EC-Kartenlesegeräte als „all-in-one Gerät“ auch einen gesicherten Datenabgleich der EC-Karte (Kaufpreis ab ca. 500 € oder Monatsmiete ca. 10 €). Hier geht es sogar um Geld und nicht nur um Patientendaten;-)

Worin begründet sich der vielfach höhere Preis für den VPN-Konnektor und des neuen eGk-Terminals gegenüber kommerziellen Produkten?
Die Hardwarekomponenten scheinen es nicht zu sein (s.o). Ziehen wir mal 50% Gewinnmarge ab, dann bleiben ca. 1400 € anscheinend notwendige Umlage je Gerät für die SW Entwicklung → bei 200.000 Geräten entspräche dies einer Geräteentwicklung allein für Software von ca. 280 Mio € für eine Hardware, welche einem RaspberryPi entspräche – Aha!)

Vermutlich wurde zuerst die Pauschale mit Hilfe eines potentiellen Anwärters geschätzt, um dann für diesen Betrag einen Anbieter der Technik zu finden;-). Technische Spezifizierungen und andere Anforderungen können so hoch getrieben werden, dass eine Kostenvorgabe ausgefüllt wird. Besonders auffallend ist, dass nur ein Anbieter (CGM) bisher in der Lage ist einen VPN-Konnektor anzubieten, der sich natürlich seinen Claim über Zertifizierung der Geräte und zertifizierte Techniker sichert. Später sollen dann möglicherweise noch T-Systems und RISE (Anfang 2018?) VPN-Systeme anbieten.
Etwas verstehe ich nicht. Warum wurden nicht wie sonst üblich, vorher genug Angebote für ein Gesamtpaket der neuen Technik eingeholt (Entwicklung, Herstellung, Zertifizierung und Betrieb), um dann erst den Zuschlag an den günstigsten Anbieter zu geben? Das wäre für mich ein sauberes marktwirtschaftliches Vorgehen. Aktuell muss die sehr teure Entwicklung von Hardware, Software und deren Zertifizierung nun bis zu drei mal (CGM, T-Systems, RISE) von den Versicherten, als eingepreister Aufschlag in die Technik bezahlt werden. Jeder weitere Mitberwerber verschärft zudem die Kalkulation seiner Konkurrenten. Alle Beteiligten müssen die Amortisation ihrer Entwicklungskosten und die Kosten ihrer Infrastruktur (Chefs, die auch bezahlt werden möchten) nun auf weniger Geräte aus ihrer Herstellung/Verkauf verteilen. Das führt meiner Ansicht nach eher zu anhaltend hohen Stückpreisen, als zu einer Absenkung, oder?
Ich habe den Eindruck, dass hier massiv die Vorgaben zur Angebots- und Auftragsvergabe, zu Lasten der Versicherten missachtet wurden. Vielleicht, um die gesetzlich vorgegebenen Termine einhalten zu können (Welche selbst auch nicht mal eingehalten werden konnten – Verlängerung des Rollouts bis 31.12.2018). Vielleicht auch, um im Nachhinein, mit einen künstlich erzeugtem Wettbewerb, den Vorwürfen von Monopolisierung und mangelhafter Auftragsvergabe aus dem Weg gehen zu können. Wurde sogar mit anhaltend hohen Preisen geworben, um weitere Wettbewerber dafür zu interessieren?

Den Zahnärzten könnten die Kosten eigentlich egal sein, denn der finanzielle Aufwand für das Grundpaket Technik und Installation (ca. 4000 €) und die weiteren Betriebskosten werden über die Kassenzahnärztlichen Vereinigungen an die Krankenkassen weitergereicht. Es wird also aus den Beiträgen der Versicherten entnommen bzw. durch Zuschüsse vom Staat (der Versicherter ist auch Steuerzahler) ergänzt.

Arbeitserleichterung war gestern

Mit Einführung der Telematik sind übrigens zwei weitere Chipkarten erforderlich. Zum einen für das neue eHealth-Kartenterminal und der neue eArztausweis (noch nicht erhältlich/ersetzt später die ZOD). Für beide sind ebenfalls monatliche Mietgebühren an die Zertifikatsstellen/Herausgeber zu entrichten (Preisliste bspw. Medisign Link). Zusammengefasst kommt das neue System auf „praktische“ drei Chipkarten für die jeweils die Pinnummern zu merken sind (eGk, eHealth-Kartenterminal-Sim und eArztausweis/ZOD, die gSMC-K im VPN-Konnektor habe ich nicht mit eingerechnet). Besonders weil viele Patienten gerne noch eine weitere eGk PIN lernen, lässt eine ausgiebige Nutzung weiterer Dienste erwarten;-) Die eGk PIN ist sechsstellig(!) und kann durch den Versicherten geändert werden. Wird dreimal nacheinander eine falsche PIN eingegeben, kann die Karte nur durch die PUK vom Patienten entsperrt werden (Link) (Total einfach also;-).
(Wer sich das ausgedacht hat, sollte als Strafe nur noch 100stellige PINs verwenden dürfen.)

Nebenbei bemerkt, wie lange benötigt Tante Erna ihre sechsstellige PIN einzugeben? Bzw. der Zahnarzt soll ja ebenfalls Vorgänge mit seiner PIN bestätigen. Gegenüber einer Unterschrift auf einem Rezept, dauert das nun mindestens zehn mal so lange – Das ist also der organisatorische Fortschritt mit dem die Telematik beworben wird. (Selbiges gilt u. a. auch für Apotheken: s. „Das eRezept war langsamer als Papierrezepte“ Link)
Diese Zeiten sollten nun auf jeden Fall mit in den Praxisablauf, mit weiteren und kostenintensiven eGk-Terminals an den Beratungsplätzen, mit eingeplant werden.

Außerhalb der Öffnungszeiten von Praxen und Apotheken hat ein Versicherter fast keine Möglichkeit, Medikationspläne, Befunde oder Notfall-Daten auf der eGk bzw. in der Telematik-Cloud zu prüfen.
Diese Einschränkungen von Zeitpunkt und Ort erhöht natürlich enorm die Akzeptanz der eGk bei den Versicherten, wenn sie am Wochenende oder nach Arbeitsende erst einen Notdienst aufsuchen müssen, um ihre eGk-Daten und Medikationspläne einsehen zu können. Schilda lässt grüßen, wenn jetzt argumentiert wird, dass ein Versicherter ja immer noch sein Rezept mit der notierten Einnahmeverordnung ausdrucken lassen kann. Solange nicht 100% der Apotheken ein eGk-Lesegerät vorweisen können und Rezepte auf der eGk für Versicherte nur optional sind, wird es Rezepte auf Papier geben müssen. Bei Auslandsreisen sind Notfalldaten weiterhin auf Papier mitzunehmen, …
Ich werde bei Rezept, Notfalldaten, Impfpass etc. auf Papier bleiben.

Dazu fällt mir gerade ein:
Notfallhelfer werden vermutlich aus strafrechtlichen Gründen (Unterlassung, Fahrlässigkeit) **immer** dazu gezwungen sein, erst einmal die eGk zu suchen und auf vorhandene Notfalldaten zu überprüfen. Der Karte ist nicht anzusehen, ob ein nicht ansprechbarer Patient seine Daten freiwillig bzw. sie aus Anlass dort abgelegt hat. So eine Karte einzulesen und dann meistens nichts zu finden, hilft jedem Notfallopfer immens, besonders wenn Zeit kostbar ist.
Kollabiert ein Patient in einer Praxis, sind auch erst einmal die Notfalldaten zu suchen, sonst muss sich sich der Zahnarzt so Sachen anhören wie: „ Ja haben Sie denn nicht vorher die eGk auf aktuelle Notfalldaten überprüft?“ Patienten müssen also ab jetzt, mit jedem Besuch einer Praxis und nicht nur 1x im Quartal, ihre eGk einlesen und aktualisieren lassen. Na ja, das trainiert wenigstens das Gedächtnis mit der PIN. Übertreibe ich hier?

-Notfalldatenmanagement Link
Besonders an Herz lege ich jedem, Kap 3.4 ab s 11. „Aktualisierung der Notfallrelevanten Medizinischen Daten“ Link. Da freut sich bestimmt jeder Hausarzt, wenn er zusätzlich noch die Aktualisierung der Notfalldaten auf der eGk in seinen Praxisablauf mit einplanen muss. Zitat: „Nach Abschluss der Aktualisierung versieht der Arzt den gesamten Datensatz mit seiner qualifizierten elektronischen Signatur.“ … dazu brauch ich wohl nichts mehr zu sagen.

Unter diesen Gesichtspunkten würden normalerweise weitere Dienste der Telematik, erst gar nicht zur Anwendung kommen. Dank der „Verdongelung“- der Praxisverwaltung mit dem VPN-Konnektor wird dem Zahnarzt aber keine Wahl gelassen. Es muss nun jede neue Applikation mit ihren technischen Fehlern und Unzulänglichkeiten und in ihren organisatorischen, finanziellen und rechtlichen Konsequenzen akzeptieren.

Sicherheit der Daten und Netze

Gesetzliche Vormünder dürfen zusätzlich die PINs ihrer Kinder oder die ihrer dementen Schützlinge lernen. Da wird es viele PINs mit „123456“ oder dem aufgedrucktem Geburtsdatum geben. Gut, dass mit dem Unterschriftenfeld auf der Kartenrückseite für so etwas Platz gelassen wurde. Das nenn ich Sicherheit;-). Wer die schlechten Angewohnheiten der Anwender mit seinem Sicherheitskonzept nicht ausschließt, der darf nicht mit „Höchster Sicherheit“ werben und hat seine Aufgabe nicht verstanden.

Der neue VPN-Telematik-Aufbau macht mein Sicherheits-Konzept zum Praxisverwaltungssystem (PVS) kaputt.
Meine bisherige Lösung besteht aus einem Intranet für die Patientenverwaltung (Win7 PCs mit der Dentalsoftware und ohne extra Virenscanner - nur Defender ...). Linux-PCs setze ich ausschließlich für den Internetzugang ein, also für Recherchen, E-Mail und zur Übermittlung der Abrechnungsdaten. Zum Überbrücken des Air-Gaps werden USB-Sticks verwendet. (Eine genauere Beschreibung der Gründe für dieses Konzept und Risikoabwägung würde hier den Rahmen sprengen.) Ein Intranet ist in der Medizin üblich, wenn etwas besonders abgesichert betrieben werden muss. Eine VPN-Verbindung in ein anderes (Intra-)Net verringert die Sicherheit enorm, besonders, wenn der verantwortliche IT-Techniker nicht die vollständige Kontrolle über beide Netze/Verbindungspunkte hat. Der VPN-Konnektor der Telematik ist eine Black-Box im Praxisnetz und daher sicherheitstechnisch ein No-Go. Wer hier über wen eine gute Kontrolle haben möchte, sollte nun klar sein.

Optional wird von der Telematik/KZBV auch eine Offline-Variante angeboten. Die zusätzlichen ca. 4000 € mit zus. Betriebskosten, für einen weiteren Kartenleser und VPN-Konnektor, werden nicht von der KZBV bezuschusst. Möchte ein Zahnarzt also sein eigenes, nicht öffentliches und wesentlich sicheres Intranet weiterhin betreiben, dann muss er dies aus eigener Tasche bezahlen!

Ich kann nicht nachvollziehen, warum das ausgemusterte/bisherige eGk-Kartenlesegerät nicht weiter in einem Intranet verwendet werden kann und quasi nochmals ein abgekoppeltes VPN installiert werden muss? Selbst Verweigerer dürfen/können ja auch ihr bisheriges eGk-Lesegerät weiter verwenden. Zahnärzte sollen also zur Aufgabe ihres sicherheitstechnisch besseren Systems (Intranet) bewegt werden.

Auf einer Dentalmesse hatte mir ein CGM-Mitarbeiter geraten, dass es mit der Telematik und den VPN-Konnektoren sinnvoll sei, auf unseren PCs zur Patientenverwaltung wieder Virenscanner einzusetzen.

Dieser Wink mit dem Zaunpfahl bedeutet eigentlich, dass eine grundsätzliche Verschlechterung in der Sicherheit erwartet wird. Spätesten ab hier werden „höchste Sicherheitsanforderungen“ nicht mehr erfüllt. Denn gegenüber einem nicht mehr von außen zugänglichem Intranet, ist nun ein anderes Netz -über VPN-Konnektoren- mit diesem permanent verbunden. Der VPN-Netz-Zugang ist nun als mögliche Quelle für Angriffe anzusehen (Virenschleuder).

Ein Virenscanner kann sogar den Angreifern helfen, einen Schaden anzurichten. (bspw. „Notfall-Patch für Windows & Co.: Kritische Sicherheitslücke im Virenscanner von Microsoft“ Der Virenscanner musste die Datei nur scannen, um den Schadcode darin zu aktivieren.)
Mit Hilfe der Telematik sollen Zahnärzte zukünftig noch einfacher Dokumente und E-Mails austauschen können. Befindet sich Schadcode darin, betrifft dessen Ausführung sofort deren PCs zur Praxisverwaltung. Beispielsweise eine E-Mail mit Ransomware wird, zum Kollegen über die Telematik gesendet und zerschiesst, dank Zwangsverbindung des VPN-Konnektors mit dem PVS, dort das gesamte Praxis IT-System.

Na klasse und wer übernimmt jetzt wenigstens die Kosten für die nun erforderlichen (wirkungslosen) Virenscanner, die sogar Angriffe unterstützen?

Eine VPN erzeugt einen abgesicherten, geschlossenen Kommunikations-Verbund. Die Sicherheit gilt allerdings nicht für die Eigenschaften des übertragenen Inhalts selbst. Bspw. eine E-Mail von einem Patienten (aus dem Internet und mit Schadsoftware) wird an den Kollegen (nun VPN) weitergeleitet.

Patientendaten sollen verschlüsselt in der Telematik-Cloud aufbewahrt werden. Nach dem eGk-Gesetz kann nur eine eGk mit PIN den Datensatz ihres Versicherten freigeben. Geht die eGk verloren oder ist sie unbrauchbar geworden, wird dem Versicherten eine neue Karte ausgestellt. Es muss also noch einen Nachschlüssel oder Kopien seiner elektronischen Schlüssel geben, um neue Karten mit diesen zu programmieren, sonst könnten die zuvor verschlüsselten Daten von der neuen Karte nicht mehr freigegeben werden.
Wer kontrolliert/besitzt diese Nachschlüssel? Allein das zeigt, dass ein Versicherter keine 100% Kontrolle über seine Daten haben kann. Gleiches gilt natürlich für den eHealth-Ausweis des Zahnarztes, mit dem er beispielsweise seine elektronischen Briefe verschlüsseln soll.

Was bedeutet Zertifizierung tatsächlich

Eine BSI-Zertifizierung verhindert über standardisierte Testverfahren nur bekannte Designfehler. Ich verstehe eine BSI-Zertifizierung als Absicherung nach Unten, die eine eingehaltene Mindest-Sicherheit nachweisen soll. Mit den Tests wird das Einhalten von Mindest-Standards bestätigt bzw. es werden die vorgegebenen Normen und Spezifikationen überprüft. Eine BSI-Zertifizierung ist für mich kein Nachweis, dass das maximal mögliche getan wurde.
Dieser Nachweis dient im wesentlichen auch dazu, dass Schadensersatzansprüche (Fahrlässigkeit) an den Techniklieferanten auch von diesem abgewiesen werden können.

Eine System-Zertifizierung ist weiterhin nur als Momentaufnahme zu verstehen, sie ist eine Updatebremse und nicht fehlerfrei (s. a. Unsichere Verschlüsselung – trotz Zertifikat vom Bundesamt: Link.).
Standardisierte Testverfahren können auch vom Hersteller umgangen werden (s. Dieselskandal). Wenn ein Produkt mit Zertifizierung (schnell) auf den Markt kommen muss, wird sich ein Hersteller im wesentlichen nur auf das Bestehen der Tests zur Zertifizierung konzentrieren.
Des weiteren verhindert eine Zertifizierung ein zeitnahes Beseitigen von neu erkannten Sicherheitslücken (0-Days! Link). Denn nach jeder Systemänderung ist eine erneute Zertifizierung erforderlich, sonst verliert das System seine Zertifizierung/Betriebserlaubnis. Es ist daher eher davon auszugehen, dass Sicherheitsupdates erst mit großer Verzögerung (Wochen, Monate?) in den PC bzw. VPN-Konnektor eingespielt werden. Neue Zertifizierungskosten fallen selbstverständlich wieder mit an. Dies ist oft ein Grund, warum ältere Medizinprodukte keine Updates bekommen und auch nicht mehr an ein IP-Netz angeschlossen werden dürfen, denn auch eine günstigere Re-Zertifizierung würde wieder viel Zeit und Geld verschlingen. Die oben genannte nachteiligen Eigenschaften von „Zertifiziert“ kennen bestimmt nur wenige. Anders kann ich mir nicht erklären, warum der Begriff „Zertifiziert“ als Marketingargument verwendet wird, um ein Produkt als „herausragend“ zu bewerben.

Ist erst einmal die Zertifizierungslawine über einzelne Systemkomponenten losgetreten, macht sie bestimmt nicht vor den Praxis-PCs und anderen Komponenten eines PVS halt (Drucker, Tastatur, Angestellte...). Mit mit dem Argument des „schwächsten Kettengliedes“ wird bestimmt der Zahnarzt selbst bald einen „IT-Führerschein“ vorweisen müssen;-)
Es ist mit noch mehr Fremdeinfluss (von wenigen Anbietern) auf eine Praxis-IT zu rechnen.

VPN (Virtuelles Privates Netzwerk)

Eine VPN-Verbindung ist die technische beste Lösung, um weit voneinander entfernte IT-Infrastrukturen, sicher zu einem Netz zu verschmelzen. Mit VPN wird nur der Transportweg gegen Datenmanipulation und Datenspionage abgesichert. Die Daten müssen vor der Übertragung durch den VPN-Tunnel nicht zusätzlich Verschlüsselt werden. VPN vereinfacht die Steuerung und Kontrolle von entfernten IT-Komponenten.

Selbst die Firewall der Praxis-Router hat bei einem nachgeschalteten VPN-Modul nichts mehr zu sagen. Dank VPN-Konnektor können so Schadsoftware, Hacker und Kontrollinstanzen von der anderen Seite noch einfacher auf ein Praxisnetz zugreifen.
Im VPN-Konnektor befindet sich auch eine Firewall. Wer darf diese Firewall konfigurieren, wenn neue Praxiskomponenten hinzukommen, bzw. die Konfiguration einsehen und überprüfen? Bestimmt nicht der eigene Praxis-IT-Techniker, der für diese trivialen IT-Basics erst noch teuer zertifiziert werden muss.
Wenn es wiederum nur zertifizierte/zugelassenen Techniker dürfen, dann werden sehr viele Betreuer von Praxis-IT aus diesem Markt verdrängt. Die technische Abhängigkeit der Praxen geht zu den wenigen IT-Betreuern mit Zertifizierung und deren Preisgestaltung.

Die Anwendung von VPN sollte organisatorisch und sicherheitstechnisch sinnvoll sein, freiwillig und mit dem IT-Techniker des Vertrauens abgesprochen und von diesem gewartet werden können. VPN ist für Firmennetzwerke sehr gut geeignet, die eine gemeinsame Vertrauensbasis haben. All das sehe ich als nicht geben an.

Warum VPN?

Wird eine starke Verschlüsselung (Public-Key-Verfahren, PGP etc.) angewendet, muss nur die Sicherheit der Endkomponenten gewährleistet werden. Die Komponenten zur Übertragung der verschlüsselten Daten können „Banane-Produkte“ sein und der Datenweg kann auch über nicht gesicherte Gebiete/Verbindungen, sogar ohne VPN, geführt werden. Die Vertraulichkeit und Integrität der Daten ist dadurch nicht gefährdet.

Spezialisierte Hardwaremodule wie den VPN-Konnektor zu verwenden, deutet für mich darauf hin, dass zukünftig eher mit hohen permanenten Datenabgleich in beide Richtungen durch das VPN-Netz gerechnet wird.
Für den Abgleich der eGk-Karte oder um gelegentlich Patientenakten zu versenden, hätte es bestimmt auch (wenn überhaupt) die VPN der Fritz!Box oder ein nicht zertifizierter VPN-Konnektor getan. Nicht jede kleine Praxis muss das Datenvolumen einer Klinikkommunikation verschlüsseln. Technische Alternativlösungen zur Kostenreduktion (PGP, Enigmail etc.) wurden also nicht vorgesehen oder sind nicht erwünscht.

Ich habe den Eindruck, dass die Praxis-IT vereinnahmt werden soll, mit möglichst wenig Risiken für den Telematik-Betreiber selbst (s. Firewall in VPN-Konnektor). Die Sicherheitsprobleme bleiben einer Praxis-IT erhalten. Sie werden aufgrund der permanenten Zwangsverbindung des Praxisverwaltungssystems sogar noch verschärft, denn weitere Dienste die Schadprogramme transportieren können (bspw. E-Mail/ Dokumentenaustausch mit Ransomware?) sollen über die Telematik genutzt werden.

Unabhängigkeit

Vielen Zahnärzten scheint nicht bewusst zu sein, dass sie mit dem VPN-Konnektor ganz dicht an ihre Kassenzahnärztliche Vereinigung rücken. Der von der Kassenzahnärztlichen Vereinigung beauftragte Telematikanbieter kann, technisch gesehen, die Praxissysteme nun bestens kontrollieren (Wer zahlt, der bestimmt...).
Das fängt mit dem Mitschreiben/Zeitstempel/Logs der genutzten Anwendungen und Verbindungen an, die in den Rechenzentren generiert werden. Beteuerungen von den Betreibern der Netzwerke, dass es zu Auswertung der Daten nicht kommen wird, halte ich für illusorisch. Ein heimliches Ausspionieren wird nicht erforderlich sein, denn über das Abhängigkeitsverhältnis der (Zahn-)Ärzte werden diese ganz offiziell nach und nach dazu gezwungen, ihre Systeme für weitere „Dienste“ und Daten freizugeben. Das mit den 1% Zwangsmaßnahmen wird ja gerade trainiert. Weitere Softwaremodule über Fernwartung zu installieren wird dann trivial, denn die Hardware ist nun vorhanden und die Systeme sind permanent miteinander verbunden. Da wäre es doch einfacher, gleich reine Clients in den Praxen zu installieren!
Mit dem VPN-Konnektor wird jedes Praxissystem Teil einer großen EDV-Zwangsgemeinschaft - dazu fällt mir nur eines ein: „Wir sind die Borg. Sie werden assimiliert werden…;-)

Kosten:

Bisherige Kosten 1.7Mrd € Link

Weitere Kosten für die Einführung eines Basissystems:
Einmalig für Borg-Konnektor + neues eGk Terminal+ Installation ca. 4000.- €
Betriebskosten ca. 80.- € je Monat. → ca. 1000.- € / Jahr

Es sollen mindestens 200.000 Konnektoren installiert werden.

- Installationskosten einmalig: 200.000 *4000 € → 800 Mio €
- Laufender Betrieb/Jahr: 200.000 *1000 € → 200 Mio €

Aufgrund des Marktmonopols erwarte ich keine wesentliche Kostenreduktion bei der Erstinstallation. Als Kalkulationsgrundlage habe ich die Anzahl der Grundsysteme aus diesem Bericht (Link) genommen und stark abgerundet.

Ich nehme an, dass alle Kassen(zahn)ärztlichen Vereinigungen eine ähnliche Preisgestaltung festlegen und habe mich an den Pauschalen der KZBV orientiert – Tabelle der Pauschalen Link Textende von Link. Bzw. Link zur Praxisinfo unter http://www.kzbv.de/anbindung-an-die-telematikinfrastruktur.1068.de.html

Mindestens ein eHealth-Kartenterminal muss je Praxis auch neu für mehrere hundert Euro gekauft werden, denn das alte, welches vor wenigen Jahren zum Auslesen der der neuen eGk erworben werden musste, ist mit dem VPN-Konnektor nun nicht mehr zulässig. Die damaligen Zuschüsse zu den alten eGk-Kartenterminals von 355.- € je Gerät + 215.- € Installation Link sind ebenso als Verlust zu sehen. → 200.000 * 570.- € → 114 Mio €.
Diese offensichtliche technische Fehlplanung hat die Versicherten nur ca. 114 Mio. gekostet.

Die Subventionen zu den anderen, nun zu ersetzenden IT-Netzen (KV-SafeNet?), sind ebenfalls als Verlust anzurechnen.

Die Versicherten sollten sich diese Summen als nicht erfolgte Behandlungen, also ihnen vorenthaltene Gesundheit, vergegenwärtigen.

Es wäre einmal interessant herauszufinden, ob die Telematik durch ihre Zusatzdienste mehr Menschenleben rettet oder durch den verursachten Geldmangel und zusätzlichen Mehraufwand im Gesundheitssystem mehr Menschenleben kostet.

Zusammenfassung

Durch eine Teilnahme an einem Zahnärztetreffen zur Telematik und über Gespräche mit bekannten Zahnärzten habe ich den Eindruck gewonnen, dass allgemein die Berufsgruppen der Ärzte und Zahnärzte überrumpelt wird. Den (Zahn-)Ärzten ist noch nicht bewusst, dass sie mit einem VPN-Konnektor weitreichende organisatorische und rechtliche Verpflichtungen eingehen und dies sogar automatisiert mit jeder neuen Applikation und ohne Widerspruchsmöglichkeit.
Die Vertreter der Kassenzahnärztlichen Vereinigungen (hier habe ich mal verallgemeinert) erscheinen mir als Erfüllungsgehilfen der Medizintechnik-Lobby, um möglichst viel Geld, ohne tatsächlichem Nutzen für den Patienten, aus dem Gesundheitssystem abzuziehen.

Zahnärzte werden dazu gezwungen, für Kassenpatienten neue Technik einzuführen, auch wenn diese, entgegen dem Gesetz, für die Zahnärzte nicht kostenneutral (Absenkung der Kostenpauschale, Vendor lock-in Abhängigkeit) ist. Unter marktwirtschaftlichen und organisatorischem Gesichtspunkten hat eine Zahnarztpraxis keinen Mehrwert von Telematik, sie verschlechtert zudem die IT-Sicherheit und Praxisorganisation und führt zur mehr Überwachung der Zahnärzte. Sämtliche, sogar durch Zertifizierung noch aufgeblähte Kosten, werden dem Gesundheitssystem durch ein Monopol entzogen und der Versicherte erhält auch langfristig betrachtet keinen Gegenwert.

Es spricht für mich Bände, wenn etwas unter Zwang eingeführt wird, weil es nicht durch Qualität und Mehrwert überzeugt.

Meine Forderungen wären:

- Wenn schon Telematik, dann freiwillig. Keine 1% nach §291 Abs.2b SGB 5

- Keine zentrale Speicherung von Daten und elektronischen Schlüssel

- Technisch erforderliche Änderungen (Internetzugang, neue Praxis IT, neues Betriebssystem bzw. neue Praxisverwaltungssoftware erforderlich) sind ebenfalls von der KZBV zu übernehmen.

- Die Telematik muss den Betrieb von höheren Sicherheitsstandards (Intranet) zulassen und ebenfalls mit 100% Kostenübernahme weiterhin ermöglichen. Eine VPN-Blackbox mit unbekannten Teilnehmern erhält nicht den sicheren Status eines Intranets.

- Wird über den Telematik-VPN-Zugang das Praxissystem beschädigt (Viren, Hacker), müssen die Kosten von der KZBV übernommen werden. (Wer das System so will, muss auch für die Folgekosten /Schäden aufkommen). Es soll dabei unerheblich sein, wie das Praxissystem sonst noch abgesichert wurde. Werden Virenscanner im Zusammenhang mit dem VPN-Konnektor gefordert, sind diese auch genau zu benennen und die Kosten ebenfalls von der KZBV zu übernehmen. Im Schadensfall hat sonst der Zahnarzt immer den falschen Virenscanner gewählt und bleibt auf den Kosten des Schadens sitzen.

Hintergrund: Virenscanner sind nie 100%tig. Sie sind nie aktuell und sie sind sogar ein Sicherheitsrisiko, s. Beispiel oben – Ein Virenscanner, der Angriffe sogar erst ermöglicht.
Hacker testen ihre Schadsoftware auch gegen aktuelle Virenscanner, bevor sie ihre Neuentwicklung ins Internet entlassen. Der Code wird solange umgeschrieben, bis dieser nicht mehr erkannt wird.

Das macht selbst aktuelle Virenscanner wirkungslos. Daher ist der Sicherheitsgewinn mit Virenscannern marginal und muss sogar gegen ihren Sicherheitsverlust aufgerechnet werden. Ein Virenscanner suggeriert eine Sicherheit, die nicht existiert.

- Aufbau, Kontrolle und Wartung der praxisinternen Hardware muss durch den Zahnarzt bzw. einem IT-Service seines Vertrauens möglich sein. Eine Zertifizierung als Zugangs- und Kontrollbeschränkung ist für diese Tätigkeiten daher abzulehnen.

- Der Zugriff auf die Telematik muss auch ohne weitere zertifizierte Komponenten ermöglicht werden. (Beispiel.: Abrechnungsübermittlung mit ZOD-Karte. Hier sind nur ZOD-Karte und Lesegerät, aber weder PC-Hardware noch Router sind zertifiziert, Dito wäre mit verschlüsselter E-Mail möglich…)

- Vorhandene Technik soll (weiterhin) genutzt werden können. (s. alte eGk-Lesegeräte, VPN-Dienst des Praxis-Routers)

Offene Fragen:

- Ist eine halbwegs plausible Aufstellung über Kosten und Nutzen der Telematik möglich?

- Ist der Identitätsbetrug überhaupt noch ein Thema?
  Bspw. Bei EC-Karten reicht auch der Perso aus.
Zitat:„..Bei der EC-Kartenzahlung mit Unterschrift des Karteninhabers kann die stichprobenartige *Kontrolle* eines Ausweises zur Betrugsbekämpfung erfolgen.„ Link)
Warum also noch ein Bild auf der eGk, das zudem rechtlich Fragwürdig ist? (Eine Begründung ist ab S. 4 von Link zu finden.)

- Ist die Absenkung der Kostenpauschale bzw. eine Kostenpauschale, aufgrund der 100% Vorgabe, überhaupt zulässig?
  Das Gesetzt ist Unabhängig vom der erwarteten Marktentwicklung. Preise können auch steigen!

- Wie setzt sich die Kalkulation/Preisfindung/ Festlegung/Verhandlung der Pauschalen besonders bei der Hardware im VPN-Konnektor zusammen?

- Wie schätzen die Hersteller (genauer der Hersteller) aktuell den Preisverfall ihres VPN-Konnektors ein?

- Wie wird die Monopolisierung der Praxis-IT zu Lasten der Versicherten gerechtfertigt/ermöglicht?
  Die Monopolisierung/Zertifizierung reduziert zudem den freien Wettbewerb im IT-Service.

- Ist aufgrund des Vendor lock-ins und/oder der 1% Zwangsvorgabe überhaupt eine freie Marktentwicklung möglich?

- Warum übernimmt die KZBV nicht das (langfristige) Kosten- und Vertragsmanagement der Telematik für die Praxen? Kurz gesagt, der Zahnarzt bekommt das Basispaket für seine Praxis zur Verfügung gestellt / kostenlos geliehen, alles andere regelt die KZBV.
Dann wären auch mögliche Kostensteigerungen für den Zahnarzt kostenneutral.

- Warum wurde nicht auf schon bestehende Hardware (altes eGk-Kartenterminal, KV-SafeNet , EC-Kartenterminal) zurückgegriffen und eine Neuentwicklung angestrebt?
Hinweis: Jede Neu-Entwicklung beinhaltet ein zus. Sicherheitsrisiko, da wieder neue Fehler erzeugt und alt bekannte Fehler eingebaut werden können.

- Zahnärzte mit alter, inkompatibler IT- Infrastruktur werden zur Anschaffung neuer Technik gezwungen.
Müssten nicht auch diese Folgekosten nach § 291a übernommen werden?

- Wie schnell werden sicherheitsrelevante Updates bereitgestellt? Rezertifizierung?

- Wie ist die Haftungsfrage bei Schäden ohne erfolgtes SW-Update (offene Sicherheitslücke) bzw. Schäden durch ein SW-Update (Betriebsausfall) geregelt?

- Wie wird sichergestellt, dass fehlgeschlagene Remote-Updates des VPN-Konnektors, den Praxisbetrieb nicht stilllegen? Das kann tausende Praxen gleichzeitig treffen!

- Wie wird sichergestellt, dass ein Hardwaredefekt des VPN-Konnektors, den Praxisbetrieb nicht stilllegt?

- Wie sind zukünftige Praxis-Neugründungen von der Reduktion der Pauschalen betroffen? Sie können nicht an den „Early-Bird“ Angeboten teilnehmen.

- Wie ist eine Praxisübernahme geregelt? Kann das VPN-System den so bestehen bleiben, oder muss ein neuer VPN-Konnektor gekauft werden? Welche Kosten fallen an und werden diese auch von der KZBV übernommen? (vermutlich sind nur die gSMC-K-Module auszutauschen.)

- Wann steht das Mobile-Terminal für ambulante Behandlungen zur Verfügung?

- Wenn die Daten vor dem versenden lokal verschlüsselt werden können (s. ZOD + Abrechnung), warum ist dann noch ein VPN-Konnektor erforderlich?

- Was passiert mit anderen VPN-Angeboten wie bspw. KV-SafeNet?

- Sind die eGk oder andere Komponenten der Telematik von dem RNG-BUG (CVE-2017-15361) Link betroffen?

- Im BSI-Zertifizierungsbericht von 2016 (Link) sind 6 LAN Anschlüsse an der KoCoBox MED+ zu sehen. Im Produktdatenblatt hat der VPN-Konnektor nur 2 LAN-Anschlüsse. Welche Hardware wurde/ist nun zertifiziert und zugelassen? Ist der aktuelle VPN-Konnektor dann überhaupt zertifiziert? Eine Klarstellung wäre hilfreich.

- Welche besonderen Gründe erfordern eine Zertifizierung der Techniker zur Installation der Komponenten? Ich sehe weder besondere Risiken noch eine besondere Anforderung an eine Qualifikation, die über IT-Basics hinausgeht. Das installieren der zertifizierten Praxisverwaltungssoftware setzt beispielsweise keinen zertifizierten IT-Techniker voraus.

- Wird Windows10 den hohen Sicherheitsanforderungen gerecht?

- Wie beurteilen Rettungsdienste und Notaufnahmen die Ablage von Notfalldaten auf der eGk?

- Ist es Unterlassung bzw. fahrlässig, wenn die eGk nicht auf Notfalldaten überprüft wird?

- Was ist mit Behandlungsfehlern aufgrund nicht aktueller oder falscher Notfall-Datensätze auf der eGk?
Ein Notfallhelfer kommt hier sehr schnell in einen Zwiespalt, wenn er etwas anders beurteilt, als es die eGk vorgibt. Die Daten auf der eGk sind immer als veraltet anzusehen und werden bestimmt nur von wenigen Versicherten sorgfältig auf dem aktuellen Stand gehalten. Es ist sehr umständlich für die Versicherten ihre Daten einzusehen und zu kontrollieren.

So sehe ich es:

Lasst das Ding sterben, wir können keine IT.
Muss hier wirklich nach den Prinzip „Lernen durch Schmerz“ verfahren werden, bis die Telematik wieder abgeschafft wird?
Lieber kleine, zielorientierte Lösungen, die wirklich einen Mehrwert bringen.

Ein Praxis-ITler

Feb. 2018, irgendwo in Deutschland

Mal so bemerkt:

Auf der Webseite der KoCo Connector GmbH (Link) zum Datenschutz steht: „Datenschutz ist uns wichtig und wir nehmen ihn sehr ernst. Daher möchten wir, dass Sie sich beim Besuch unserer Webseite sicher fühlen...“

Allerdings ist die Webseite nur über http: und nicht über https: zu erreichen. Die schaffen es also nicht einmal, die Kommunikation zur Webseite mit SSL/TLS abzusichern!

Das ist schon mal eine klasse Referenz für deren Produkt. Dann darf ich mich auch beim VPN-Konnektor wenigstens sicher fühlen, technisch gesehen bin ich es allerdings nicht;-)
22.2.18

Quellen:

Produktdatenblatt VPN-Konnektor:
https://www.kocoboxmedplus.de/de/index.de.jsp

BSI Zertifizierungsbericht KoCoBox MED+:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte09/0950b_pdf

KZBV Info zur elektronischen Gesundheitskarte:
http://www.kzbv.de/elektronische-gesundheitskarte.92.de.html

CGM Aktie:
http://www.finanzen.net/aktien/CompuGroup_Medical-Aktie

Unsichere Verschlüsselung – trotz Zertifikat vom Bundesamt, Zeit.online, 19. Oktober 2017:
http://www.zeit.de/digital/datenschutz/2017-10/infineon-verschluesslung-personalausweis-tpm-bsi-zertifiziert
und
https://www.heise.de/security/meldung/Hunderttausende-Infineon-Sicherheits-Chips-weisen-RSA-Schwachstelle-auf-3864691.html
und
https://www.golem.de/news/rsa-sicherheitsluecke-infineon-erzeugt-millionen-unsicherer-krypto-schluessel-1710-130691-3.html

Virenscanner als Sicherheitsrisiko Heise Security, 08.12.2017: Notfall-Patch für Windows & Co.: Kritische Sicherheitslücke im Virenscanner von Microsoft“:
https://www.heise.de/security/meldung/Notfall-Patch-fuer-Windows-Co-Kritische-Sicherheitsluecke-im-Virenscanner-von-Microsoft-3913800.html

Bei Krankenkassen: Millionenschaden durch Betrug Merkur.de 18.08.16 :
https://www.merkur.de/wirtschaft/krankenkassen-millionenschaden-durch-betrug-6671348.html

Kosten und Anwendungen
https://www.heise.de/newsticker/meldung/Elektronischer-Gesundheitskarte-Aerzte-aergern-sich-ueber-Verzoegerungen-3901541.html

Elektronische Gesundheitskarte: Von VPN-Konnektoren, Lesegeräten und fehlenden Vorteilen Heise.de 12.08.2017
https://www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Von-VPN-Konnektoren-Lesegeraeten-und-fehlenden-Vorteilen-3798708.html

KV-SafeNet Anbieter/Kosten:
http://www.kbv.de/html/7145.php

§ 291 Abs. 2b SGB 5 , 1% Zwangsmaßnahme

http://www.sozialgesetzbuch-sgb.de/sgbv/291.html

Gematik Whitepaper 27.09.2016
https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_whitepaper_web_Stand_270916.pdf

RISE-Konnektor
https://www.rise-konnektor.de/index.html

Versandapotheken: Das eRezept war langsamer als Papierrezepte
https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/06/01/das-e-rezept-war-langsamer-als-papierrezepte-br

Aktion: Stoppt die e-Card!
http://www.stoppt-die-e-card.de

Die dunkle Seite der eGk:
https://ddrm.de/wp-content/uploads/Die-dunkle-Seite-der-eGK-3.pdf

IT-ler analysiert die eGk:
http://www.ocmts.de/egk/html/2___oneview.html

Vorlesungsfolien zur Komplexität von sehr großen Softwareprojekten am Beispiel der eGk, Lutz Prechelt, 2012
http://www.inf.fu-berlin.de/inst/ag-se/teaching/V-SWT-2012/12_eGK.pdf

Zuschüsse zum alten eGk Kartenlesegerät
https://www.kvb.de/fileadmin/kvb/dokumente/Praxis/Serviceschreiben/2011/KVB-RS-110329-Zuschuesse-eGK-Lesegeraete.pdf

§ 12 SGB V Wirtschaftlichkeitsgebot für Gesetzliche Krankenkassen
http://www.sozialgesetzbuch-sgb.de/sgbv/12.html

Freie Ärzteschaft: Pleitenprojekt „elektronische Gesundheitskarte“ endlich einstellen!
http://www.mediteam-muenster.de/download/Freie-Aerzteschaft-Pleitenprojekt-Elektronische-Gesundheitskarte-endlich-einstellen.pdf

digitalcourage: Fünf Gründe gegen die eGK
https://digitalcourage.de/themen/elektronische-gesundheitskarte/fuenf-gruende-gegen-die-egk