Stellungnahme zum geplanten eHealth-Gesetz

von
Rolf D. Lenkewitz, Monika Laubach

Bundesgesundheitsminister Gröhe plant, die – nach seiner Zählung – mehr als 200 verschiedenen Informationstechnischen Systeme im Gesundheitswesen zu verbinden und ihre Datenbestände für die Institutionen im Gesundheitswesen nutzbar zu machen. Das e-Health-Gesetz bildet die Rahmenbedingungen für den Aufbau der Telematischen Infrastruktur (TI). Viele Befürworter stellen die Sache so dar, als gäbe es keine zentralen Server. Ab und zu fällt einmal der Begriff "Cloud" - und das war es.

I. Was ist die TI?

Die Telematik-Infrastruktur (TI) besteht aus der kompletten IT-Infrastruktur der Leistungserbringer (EDV/IT der Primärsysteme oder auch KIS-Systeme für Krankenhäuser, AVS-systeme für Apotheken, PVS-Systeme für Arztpraxen) und den geplanten Rechenzentren, die von der gematik beauftragt werden. Das aus Neu und Alt geschaffene informationelle System wird auch als Service-Orientierte-Architektur (SOA), bezeichnet (SOA: bestimmt die grundlegende Organisation und Interaktion zwischen den Komponenten einer Anwendung und ist an Geschäftsprozessen orientiert). SOA ist eine relativ neue Technologie und bekannt für seine ausgeprägten Schwächen.
Wenn die Pläne zur TI Wirklichkeit werden, dann werden alle beteiligten Rechner zu untergeordneten Vasallen in einem führenden Megasystem.
Die einzelnen Computer in den Arztpraxen, Apotheken, Krankenhäusern, bei den Krankenkassen etc. bekommen alle eine Software, mit deren Hilfe ihre Rechner zu „virtuellen" Rechnern in der TI werden. Dort werden die erfassten Rechner in einem einzigen zentralen Datenspeicher zusammengeführt - **sie werden zur TI**. Damit sind die einzelnen Rechner sozusagen immer online und vernetzt. **Wird ein einzelner Rechner angegriffen, so wird die TI angegriffen.** Hierin liegt der große Unterschied. Wird ein einzelner Rechner in einer Arztpraxis (ohne Anschluss an die TI) angegriffen, dann sind „nur" die Patienten dieses Arztes betroffen. Wird ein „virtueller" Rechner in der TI angegriffen, dann stehen Milliarden Daten von ganz Deutschland auf dem Spiel. Ein solch großer Datenpool (wie bei einem zentralen Speicher) weckt große Begehrlichkeiten bei Geheimdiensten und Datenhändlern.
Die medizinischen Daten sind dadurch in der Telematik-Infrastruktur, weil die Primärsysteme Bestandteile sind. Die Vorstellung, die wir uns von dem System machen, muss dringend korrigiert werden.
Es wird z. B. der Anschein erweckt, dass die medizinischen Dokumente, unabhängig von der eGK nur ÜBERTRAGEN werden sollen. Das klingt so, als ginge es um eine Art sichere Post, aber keine dauerhafte Speicherung in der TI. Damit werden die wahren Zielsetzungen und Funktionen verschleiert. Wenn alle Speicherorte der Daten und Dokumente in einer Zentrale erfasst werden, dann ist dies gleichbedeutend mit einer dauerhaften Speicherung.

In der TI soll ein riesiges Datenbanksystem entstehen, das aus den Informationen aller angeschlossenen IT-Systemen "gefüttert" wird, wobei

1.

ein Großteil administrativer und medizinischer Daten durch die Anpassung der IT-Systeme von Kliniken, Arztpraxen, Apotheken und Krankenkassen in ein globales Austauschformat (XML) verpackt und in entsprechenden Datenbanken in den Kliniken, Arztpraxen, Apotheken, Krankenkassen etc. gespeichert werden sollen und

2.

durch die Vernetzung aller dieser Systeme daraus ein globales Datenbank-System entsteht, in dem die gespeicherten Daten abrufbar sind, sofern der Schlüssel hierfür eingesetzt wird.
3.
nahezu alle Daten, die in den Primärsystemen verarbeitet werden mit einem Link versehen (Referenzinformationen), der zu den geplanten zentralen Rechenzentren, z.B. von Arvato Bertelsmann gesendet wird und dort gespeichert wird. Dadurch entsteht eine der größten Datenbanken der Welt. Alle Links laufen hier zusammen und können von denjenigen, die den Link kennen und zugangsberechtigt sind, benutzt werden.
4.
Es ist davon auszugehen, dass aus Sicherheitsgründen nicht nur die Links zu den Gesundheitsdaten in den zentralen Rechenzentren und damit in der TI gespeichert werden. Sehr wahrscheinlich ist eine zunehmende Abspeicherung von Daten- und Dokumenteninformationen auf externen Servern. Ziel des Systems ist es, Daten unbegrenzt auszutauschen und jederzeit zur Verfügung zu stellen.
Damit Ihre Gesundheitsdaten in der TI gefunden werden können, müssen sie eindeutig Ihrer Person zugeordnet werden können. Dazu hat der Gesetzgeber bereits eine lebenslang gültige Krankenversicherungsnummer eingeführt. Sie stellt ein Suchkriterium dar, mit der die bislang verstreuten Informationen personenbezogen zugeordnet werden könnten. Diese lebenslang gleiche Versichertennummer ist einzigartig und kann deshalb nicht mit anderen verwechselt werden, so wie es bei Namen der Fall sein kann. Jede Klinik, jeder Arzt, jede Apotheke, die Daten von dieser Person hat, speichert diese Daten zusammen mit deren Versichertennummer. Mit Hilfe dieses Identifikationsmerkmals lassen sich zu einer Person nahezu alle Diagnosen, die irgendwo in das System eingetragen worden sind, diesem Menschen wieder zuordnen und auswerten.
Es wird alles inventarisiert und unter der Versicherungs-ID und anderen identifizierenden Nummernfolgen, den sogenannten Objektidentifikatoren

ϟ

(OIDs) abgelegt. So kann jedes einzelne Detail, sowohl vom Inhalt als auch von der Bedeutung und der Zuordnung her, erfasst werden.
Neu wäre dabei, die Vernetzung bzw. der Anschluss an die TI, denn sobald die Vernetzung zwischen den so inventarisierten Inhalten hergestellt ist, ist faktisch EIN System geschaffen worden, in dem jeder theoretisch auf alles zugreifen kann, es sei denn er hat keinen Schlüssel (vermutlich noch zusätzlich eine PIN-Nummer). Bei einem illegalen Zugriff wären damit allerdings alle Informationen verfügbar.

II. Weshalb ist XML so wichtig?

XML bedeutet: erweiterte Auszeichnungssprache. Die oft anzutreffende Behauptung, die TI sei lediglich eine Datenautobahn und die Daten seien ja hier oder da und die Vernetzung sei quasi nur eine Art "Zustellservice" zwischen hier und dort stellt eine Illusion und Schönrederei dar. Durch die Vernetzung gibt es kein hier oder da mehr, sondern nur noch ein Netz und Mastersystem, in dem alle Transportinformationen, ähnlich wie in einer Spedition zusammen in einer großen vernetzten, zentral gespeicherten und keineswegs unübersichtlichen Datenbank lagern.
Legt man beispielsweise eine Online-Bibliothek zugrunde, also einen Bibliotheksverbund aus mehreren Bibliotheken, die ihre Bestände vernetzt haben, dann können die (im Gesundheitswesen: nur zugelassene Kunden) Kunden über EIN System auf alles, was in den Bibliotheken zu finden ist, zugreifen. Nach einer Bestellung schickt die Bibliothek A nicht den Artikel per E-Mail aus dem Bibiotheks-Speicher an einen Nutzer, sondern der (im Gesundheitswesen: nur zugelassene Kunde) Kunde nimmt den Artikel selbst "aus dem online-Regal" und liest ihn. Die Vernetzung im Gesundheitssystem soll genau so konstruiert werden, allerdings werden Zugangsrechte installiert und Erlaubnisse zum Abruf von Informationen erteilt.
Damit die Daten WELTWEIT LESBAR sind, werden sie mit einem einheitlichen Austausch- und Regelformat (XML/XSD) verarbeitet und im GLOBAL angelegten Datenverarbeitungs- und Speichersystem zusammengeführt. Für jede Datei und Information steht ein eigener "Container" zur Verfügung. Dort wo es keine Information gibt, bleibt der Container, der dafür bereitstand leer. Auch aus leeren Containern können

Rückschlüsse gemacht werden, z. B. wenn der Container, für den der Eintrag zum Organspendeausweis leer bleibt, dann kann daraus gefolgert werden, dass die Person mit der Spende eines seiner Organe nach seinem Ableben nicht einverstanden ist. Der Betreffende wundert sich dann vielleicht, warum er Zuschriften erhält, die die Wichtigkeit der Organspende in unserem Land betonen.

Eine riesige Datenbank erfüllt nur ihren Sinn, wenn jeder alles jederzeit und schnell heraussuchen kann, was ihn interessiert. Es wird kein Milliarden Euro teures Mammutsystem aufgebaut, damit PDF-Dokumente von a nach b gesendet werden und dann nach Abruf durch den Empfänger wieder gelöscht werden. Dafür gibt es bereits technische Lösungen. Das zentrale Problem ist, dass alle Rechner so vernetzt werden, dass die Inhalte miteinander verknüpft sind und von der TI aus einsehbar, abrufbar, veränderbar und ggf. manipulierbar sind.
Alle Informationen, die über diese Person gespeichert wurden, sind erst einmal quasi "nebeneinander", weil sie alle wie an einer Schnur hängen, die mit der Versichertennummer oder anderen identifizierenden Nummern dieser Person gekennzeichnet ist.
Diese Schnur kann über viele Server und durch verschiedene Krankenhäuser, verschiedene Facharztpraxen, ambulante Reha-zentren, verschiedene Apotheken und über Ländergrenzen (global) hinweg gehen. In der Zentrale ist dann ein "Zettel" (eine Liste von Links) hinterlegt, wo die verschiedenen Informationen gespeichert sind, die mit dieser bestimmten Versichertennummer und anderen identifizierenden Nummern verbunden sind.
Diese *Link-Listen* können dann durchsucht oder abgefragt werden. Nun ist es möglich, dass theoretisch das ganze System nach allem durchsucht werden kann, was mit dieser Versichertennummer verbunden ist.

Durch das Wissen, wie die Struktur aufgebaut ist, könnte ein Programm geschrieben werden, das z.B. aus der gesamten Datenmasse in der Telematik Infrastruktur alle Arztbesuchsdaten herauszieht und diese in Form einer chronologisch sortierten Liste ausgibt. Weil vermutlich nicht alle Arztbesuche aller Patienten interessant sind, wird das Programm zusätzlich angewiesen, nur die herauszusuchen, die mit der Versichertennummer eines bestimmten Patienten gekennzeichnet sind. Vielleicht sind auch nur die Arztbesuchsdaten für ein bestimmtes Jahr gefragt usw.

III. Was haben Metadaten mit der eGK zu tun?

Für den Zugriff auf die Inhaltsdaten werden unterschiedliche Zugangsrechte erteilt. Metadaten (beschreibende Daten) sind u. a. deshalb interessant, weil sie nicht in jeder Hinsicht verschlüsselt werden können. Metadaten sind zum überwiegenden Teil für alle lesbar und zugänglich. Das System ist dann entweder gar nicht mehr funktionsfähig oder - falls es doch eine Möglichkeit zur Verschlüsselung gäbe - durch das viele Ver- und Entschlüsseln so langsam, kompliziert und teuer, dass damit nicht mehr vernünftig gearbeitet werden könnte. Metadaten (Daten über die Daten) sind grundsätzlich dazu da, das Wissen über die Daten wesentlich zu erweitern und neue Beziehungen zwischen Daten und Informationen herstellen zu können. Die Informationsmenge wird dadurch ins Gigantische aufgebläht und es entstehen genug zusätzliche Informationen die auch unabhängig von den Inhaltsdaten ausgewertet werden können. Anhand der vielen Metadaten, wäre es dann ein Leichtes, das Profil einer Person zu erfassen. "Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren…". Diesen Satz hat der Erste Senat des Bundesverfassungsgerichts in seiner Entscheidung vom 16.07.1969 (Aktenzeichen 1 BvL 19/63) den politisch Handelnden in Exekutive und Legislative ans Herz gelegt.
Quelle:
http://www.telemedicus.info/urteile/Allgemeines-Persoenlichkeitsrecht/420-BVerfG-Az-1-BvL-1963-Mikrozensus.html

Der gläserne Patient wäre endgültig Wirklichkeit und die ärztliche Schweigepflicht abgeschafft.
Wenn beispielsweise bei einem Arztbesuch zur Versichertennummer des Patienten, zusätzliche Metadaten wie der Name der Arztpraxis, die Adresse der Arztpraxis und der Zeitpunkt des Arztbesuchs bekannt werden, können auch schon einige Rückschlüsse gezogen werden, z.B.: wer wird von wem behandelt? Wann waren die Arztbesuche? Wie oft fanden die Arztbesuche statt. Es handelt sich hier um Metadaten, die eigentlich dafür da waren, die Rechnung des Arztes an die KK zu stellen. Bei der eGK/TI ergibt sich also aus der Versicherungsnummer des Patienten, den IDs der Arztpraxen und Arztbesuchsdaten eine komplette Arztbesuchshistorie.
Dass es letzlich nicht mal konkreter Anlässe für eine aktive Datenspionage braucht, sondern am Ende selbst Metadaten als Grund genügen, brachte der ehemalige Chef von NSA und CIA auf den Punkt. Wörtlich sagte Michael Hayden in einer Debatte an der Johns Hopkins University im Jahr 2014: „we kill people based on Metadata."
https://www.justsecurity.org/10311/michael-hayden-kill-people-based-metadata/

IV. Was ist mit den sog. freiwilligen Anwendungen?

Die freiwilligen Anwendungen sind ja nur die definierten medizinischen Daten, die über die Karte generiert (abgeleitet) werden.
Diese zustimmungsbedürftigen, freiwilligen Anwendungen werden in § 291a II SGB V benannt. Es handelt sich hier um
- den Notfalldatensatz
- den elektronische Arztbrief
- Daten zur Prüfung der Arzneimitteltherapiesicherheit
- die elektronische Patientenakte
- Daten, die Patienten selbst hochgeladen haben (z.B. Organspendeausweise, Vorsorgevollmachten oder Patientenverfügungen und der Hinweis, wo diese in Papierform zu finden sind)
- die Patientenquittung (Abrechnungsdaten)

Lediglich für diese 6 Anwendungsbereiche soll ein Einwilligungsvorbehalt (nur wenn die Person zugestimmt hat, dass diese Daten gespeichert werden dürfen) des Patienten installiert werden.
Hierzu ist folgendes zu sagen:
1. Was passiert mit den anderen Daten, die nicht vom Einwilligungsvorbehalt erfasst werden, schließlich gibt es Tausende von anderen Anwendungen?
2. Was passiert mit den Anwendungen von den Personen, die der Speicherung dieser 6 Anwendungsbereiche nicht zugestimmt haben?

Ja wo werden Sie dann eigentlich gespeichert?
Die Antwort ist: wahrscheinlich in der TI!

Erinnern Sie sich dabei bitte daran, dass die einzelnen Rechner der Arztpraxen, Krankenhäuser etc. zu abhängigen Rechnern geworden sind, sobald sie mit der TI verbunden worden sind.
Wie bekommt der Hausarzt die Röntgenbilddatei, die vom Radiologen in die TI eingespeist wurde, wenn der Patient der Speicherung der freiwilligen Anwendungen nicht zugestimmt hat? Aus den gematik Dokumenten wird dies nicht detailliert genug ersichtlich. Vorausschauende Folgeabschätzungen für Gefahren und Interaktionen sind dort nicht zu finden. Die einfache Annahme, dass der Patient, der dem Röntgen zugestimmt hat, auch erlaubt, dass das Ergebnis ebenso dem Hausarzt vorliegt, wäre zu kurz gedacht.
Es besteht die Gefahr, dass alle Daten (auch die 6 Anwendungsbereiche mit dem Einwilligungsvorbehalt) von der gematik abgegriffen werden könnten, da sie alle in der Cloud gespeichert werden. Zudem haben viele medizinischen Geräte eine Onlineanbindung. Es ist heute schon gang und gäbe, dass Blutdruckmessgeräte ihre Ergebnisse direkt in die Cloud senden können.
Später soll die TI auch für sog. Mehrwertdienste und Dienstleitungen jeder Art geöffnet werden. Wenn die Versicherten dann ihre "Medizin-Homebanking-Software" öffnen, also versicherter@home oder eKiosk, werden ihnen dort u. U. Werbungen und Services eingespielt, z.B. für

DMP-Programme und andere Gesundheitsprogramme oder Geräte. Hier ist es dann auch wahrscheinlich, dass über die Metadaten profilabhängige Mehrwertdienste angezeigt werden, wenn z.B. jemand Arthrose hat, dann bekommt er zielführend Services von Orthopäden und Medikamenten. Das ist keinesfalls auszuschließen. Ein Beispiel dafür liefert Amazon.
Dass alle Daten automatisch in der TI aufbewahrt werden, ist noch nicht geklärt. Bevor eine fundierte Aussage darüber getroffen werden kann, ob alle Daten in der TI landen, oder nur ausgewählte Dateien dort gespeichert werden, muss zunächst einmal der nachweisliche Prozess der Anpassung der eingesetzten Software in den KIS/AVS-IT-Systemen an die gematik erfasst und beschrieben werden können. Es muss uns also möglich gemacht werden, dass wir eine Aussage dazu machen können, dass nicht alle relevanten Daten in der TI sind oder doch nur manche, ausgewählte Daten dort sind.
Die Anpassung der Praxissoftware muss unbedingt näher untersucht werden. So ist beispielsweise nicht erkennbar, ob ein Datenbank-fähiger Datensatz für das Blutbild von Frau X erst abgespeichert werden muss, wenn das Blutbild vom Facharzt Y abgerufen werden soll. Oder muss davon ausgegangen werden kann, dass die Praxis-, Krankenhaus-Systeme etc. alle Daten und Linkinformationen "vorsorglich" in Datenbank-Formaten speichern, um eine spätere potentielle Einsicht auf einfache Weise zu ermöglichen.
Man kann technisch gesehen sowohl die Blutwerte in eine Datenbank eintragen, als auch in ein Dokument, das zwischen den Zugangsberechtigten ausgetauscht wird. Die Einbindung dieses Vorgangs in das neue System erfordert eine detaillierte Erfassung der möglichen Abläufe, die in dieser Situation entstehen und dafür ist es erforderlich zusätzliche Informationen zu erheben. Das System ermöglicht beide Arten! Was tatsächlich in Zukunft realisiert wird, entzieht sich unserer Kenntnis - und das darf nicht sein!
Was ist jedoch, wenn das falsche Dokument übertragen wird? Oder eines übertragen wird, das nicht übertragen werden soll? Die Antworten hierauf bleiben uns verborgen.

V. Warum schützen Verschlüsselungen nur wenig?

Immer wieder finden wir die Aussage, dass das System doch sicher sei, denn schließlich seien die Daten doch verschlüsselt.
Aber wer ist im Besitz der Hauptschlüssel? Nicht der Versicherte selbst, sondern die gematik. Wer die Schlüssel in der Hand hat, der hat die Hoheit über die Schlüssel - die Macht! Daher gehören die Schlüssel in die Hand des Versicherten!
Dadurch, dass zudem die Schlüssel rekonstruierbar für Dritte werden

sollen, wird ein großes Sicherheitsleck geschaffen. Für den Fall, dass die eGK mit dem geheimen Schlüssel abhandenkommt, gibt es für die gematik die Möglichkeit, den geheimen Schlüssel für die Patientendaten wiederherzustellen. Zwar verfügt die gematik nicht selbst über die "Nachschlüssel", sondern die damit beauftragte "Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH". Diese ist jedoch nicht ausreichend organisatorisch getrennt gehalten, um einen Zugriff durch Behörden oder Krankenversicherungen auf die Patientendaten mit absoluter Sicherheit ausschließen zu können. Mit der Rekonstruierbarkeit der Gesundheitsdaten entsteht die Möglichkeit, ohne Wissen der Patienten auf die Daten der eGK zuzugreifen. Es besteht ferner die Gefahr besteht, dass unbefugte Dritte Gesundheitsdaten abgreifen können.
Quelle: http://www.ccc.de/de/elektronische-gesundheitskarte

VI. Es gibt keine Sicherheit in der TI

Mit Hilfe eines handelsüblichen Auslesegerätes zeigte Professor Oliver Kalthoff (Universität Heidelberg und Hochschule Heilbronn) bei einem Vortrag, wie einfach Daten aus der Gesundheitskarte extrahiert werden können. Dabei ging es nicht nur um die Stammdaten wie Name und Geburtsdatum. Mit wenigen Operationen gelang es ihm grundsätzlich auch, mögliche Rezepte auszulesen.
Quelle:http://www.humanistischeunion.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/baden-wuerttemberg-risiken-derelektronischen-gesundheitskarte-praktisch-demonstriert/
In der technischen Sicherheitsanalyse der elektronischen Gesundheitskarte von Huber/Sunyaev/Krcmar der technischen Universität München vom Februar 2008 wurde darauf hingewiesen dass die Miteinbeziehung erforderlicher Sicherheitsanalyse-Standards für die eGK

ein unbefriedigendes Ergebnis ergibt und es erforderlich wäre zunächst diese fehlenden Standards zu erarbeiten.
Um die TI realisieren zu können, sind die Entwickler der TI auf Markenprodukte angewiesen, beispielsweise Cisco-Router oder Microsoft Software für Datenbanken. Die Primärsysteme arbeiten vorwiegend mit Hardware und Software, die in den USA und Asien hergestellt werden.
Wer im Angesicht von Millionen Zugangsberechtigten glaubt, dass er einen Missbrauch der Daten ausschließen kann, „handelt naiv, fahrlässig oder will absichtsvoll täuschen“ kommentierte Prof. Hartmut Pohl, Professor für Informatik.
Quellen: http://www.gen-ethisches-netzwerk.de/GID/220/linder/patientendaten-pr%C3%A4sentierteller

(Zitat aus seinem Vortrag auf der Tagung „Das System e-Card - Optimierter Zugriff auf die Ressource Mensch“ am 18.04.2012 in Berlin. Bericht zur Tagung im Netz unter www.kurzlink.de/gid220_d.)
Wenn wir das eHealth-Gesetz nicht aufhalten und sobald die TI online-basierend ist und die Benutzer damit arbeiten, ist eine hohe Gefährdung der Datenbestände auszumachen.
Die Firmen gemalto und Giesecke & Devrient (Beides eGK Chipkartenherstellerfirmen) gelten seit 2010 als gehackt. (Warum Verschlüsselungen knacken, wenn man die Schlüssel hat?!)
Durch Edward Snowden wurden wir auf ein unvorstellbares Ausmaß an Möglichkeiten für Datenschutzverletzungen aufmerksam gemacht und wie diese Datenspionage schon in der Wirklichkeit perfekt angewendet wird.
Eine der vielen Angriffsmethoden besteht darin, dass die erspitzelten Daten nicht direkt an den eigenen Rechner transportiert werden, sondern zuerst an die Internetadresse eines unbeteiligten Internetnutzers, den sogenannten Sündenbock-Empfänger (Scapegoat). Von dort aus werden sie wiederum abgefischt. Am Pranger steht jedoch dieser unbekannte Empfänger, der Sündenbock.
[12]

Das fashioncleft protocol ist eine Methode, mit deren Hilfe sich ein Angreifer in den Daten seines Opfers barreirefrei bewegen kann. Hiermit können sämtliche Daten von dem Angreifer "durchgetunnelt" (ohne Beschränkungen Daten herausziehen) werden, d. h. egal ob Textdaten oder Sprachdaten, alles kann abgefischt werden.
Zur weiteren Information sei verwiesen auf die Präsentation zum FASHIONCLEFT Protocol, mit dem Trojaner die Daten aus angegriffenen Computern zur NSA schleusen:
https://www.eff.org/files/2015/01/27/20150117-spiegel-the_fashioncleft_protocol_nsa_uses_to_exfiltrate_data_from_trojans_and_implants_to_the_nsa_0.pdf
http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html
Eine der wichtigsten Erkenntnisse, die durch Edward Snowden gewonnen werden konnte, ist die Einsicht, dass die IT-Systeme von Deutschen nicht mehr ausreichend kontrolliert und gesichert werden können. Die Herstellerfirmen der Hardware, mit denen wir unsere Infrastruktur aufgebaut haben, kommen aus den USA und wir müssen davon ausgehen, dass in Hardware- und Software-Komponenten sog. Backdoors (Hintertüren) eingebaut werden, um jederzeit einen Zugriff ermöglichen zu können. Dies trifft natürlich auch für die Telematik-Infrastruktur zu. (gemalto-Hack! siehe Artikel:
).
Das die Datenspione der NSA, mit an Sicherheit grenzender Wahrscheinlichkeit, bereits illegalen Zugang zu allen Windows-Betriebssystemen haben, gibt Microsoft indirekt selbst zu. Microsoft habe erstmals bestätigt, dass es bei der Softwareentwicklung mit dem US-Geheimdienst NSA kooperiert habe, wolle aber keine Details nennen. Dem Bericht nach, hatte das Redmonder Unternehmen bereits vor vier Jahren die NSA um Gutachten für Windows XP und Windows Server 2003 ersucht. Microsoft habe auch mit anderen, nationalen wie internationalen Behörden und Organisationen, einschließlich der NATO kooperiert, wird ein Microsoft-Mitarbeiter zitiert.
Quellen: http://www.heise.de/newsticker/meldung/Bericht-NSA-half-Microsoft-bei-der-Vista-Entwicklung-132473.html

http://www.welt.de/politik/ausland/article117971277/Microsoft-soll-Zugriff-auf-Outlookermoeglicht-haben.html
Nach den Enthüllungen von Edward Snowden kann es allerdings als gesichert gelten, dass die NSA einen geheimen Zugang zu Windows-Systemen hat und somit jede Verschlüsselung umgehen kann.
Quelle: http://www.pcwelt.de/news/Skandalumwittert-Der-NSA-Key-in-Windows-322794.html
http://www.focus.de/digital/computer/hotmail-outlook-skype-microsoft-erlaubt-nsa-zugriff-auf-kundendaten_aid_1041478.html
Die Entwicklung ist besorgniserregend angesichts des Wertes der Gesundheitsdaten, die lt. einer Studie der TU-München, alleine in Deutschland, mit 90 Milliarden Euro beziffert werden. Das Gesundheitswesen sollte in der Hand des Staates verbleiben. Es ist äußerst gefährlich die sensibelsten und schützenswertesten Daten in unüberschaubare Infrastrukturen der Global Player zu legen. Die eigentlichen Zielsetzungen der Großkonzerne liegen im Wachstum und in der Gewinnorientierung. Die Versichertendaten haben dagegen eine soziale, ethische und moralische Dimension, die von selbstlosen Institutionen und nicht von der Industrie und den Konzernen verarbeitet werden dürfen.

Daher müssten sämtliche IT-Vorhaben gestoppt werden - nicht nur die Telematik-Infrastruktur.
Den technischen Teil des Schreibens zusammenfassend sei erwähnt: Die TI ist, anders als öffentlich dargestellt, keine Datenautobahn und kein sicheres Zustellsystem zum Austausch von Dokumenten. Es sollen hingegen:
14
1. alle Daten in ein globales Austauschformat überführt werden (auch durch die Anpassung der IT-Systeme) und
2. durch die Vernetzung aller Rechner im Gesundheitssystem ein riesiges Datenbank-System entstehen, in dem alle Daten zusammen gespeichert, abrufbar, filterbar, sortierbar, veränderbar (und damit manipulierbar) sind.
Durch die Spionageaktivitäten der NSA und neuartige technische Gefährdungen sind die Gesundheitsdaten der ganzen deutschen Bevölkerung gefährdet, mit Ausnahme derjenigen, die nicht von dem System, erfasst werden (dies gilt z. B. noch für Privatpatienten).
Der Aufbau der Telematik-Infrastruktur muss gestoppt werden - das eHealth-Gesetz darf in der jetzigen Fassung nicht gültig werden.