

Alexandra Obermeier
Ärztin für Psychiatrie und Psychotherapie
Hörwarthstraße 51
80804 München

München, den 17.11.2019

Tel.: 089 /27 27 38 21
Fax: 089 /27 27 38 22

An den Vorstand
Der Kassenärztlichen Bundesvereinigung
Herbert-Lewin-Platz 2

10592 Berlin

**TI – Rechtssicherheit in Praxen – Artikel im Deutschen Ärzteblatt, Heft 45:
Datensicherheit -Mehr Rechtssicherheit für Praxen**

Sehr geehrter Herr Dr. Gassen,
sehr geehrter Herr Dr. Hofmeister,
sehr geehrter Herr Dr. Kriedel,

die Ereignisse überschlagen sich wieder einmal, und fast zeitgleich erschienen die Nachrichten in der Presse über unsicher angeschlossene Praxen sowie der oben genannte Artikel.

In den Berichten von SZ und NDR wurde einigermaßen kritisch berichtet und die reflexmäßige Schuldzuweisung an die Ärzte durch das Ministerium auch im Sinne der Ärzte relativiert.

Im Artikel des Deutschen Ärzteblatts elektrisierten mich zwei Aussagen. *Zum einen:* Aus Sicht des Gesetzgebers bestehe dennoch auch für die im ambulanten Sektor eingesetzten IT-Systeme ein großes Bedrohungspotenzial. Ferner betonen Sie, Herr Dr. Kriedel, dass die Terminvorgabe für die zu erarbeitenden IT-Sicherheitsanforderungen „überaus sportlich“ sei. Hierzu möchte ich anmerken, dass den niedergelassenen Ärzten bereits seit Anfang des Jahres zugemutet wird, die TI- Komponenten zu installieren, ohne dass Sicherheitsanforderungen ausgearbeitet und mitgeteilt worden wären, die der enormen Komplexität der technischen und organisatorischen Konstruktion von TI und ePA entsprechen.

Ich selbst habe mich viel mit der unausgereiften Technologie beschäftigt, was meinen Entschluss untermauert hat, mich nicht anzuschließen. Nach zahlreichen Vorträgen von Sicherheitsanalysten wurde mir vor allem klar, dass die Dinge extrem komplex sind, sodass ich das als Ärztin niemals allein beherrschen können werde. Die Darstellung in den Medien, die „IT-Dienstleister“ der Herstellerfirmen hätten einen seriellen Anschluss meist gar nicht angeboten, ist irreführend. So hat mir mein Praxisinformatiker erzählt, dass er einmal zufällig in einer Praxis gewesen sei, während die TI installiert wurde. Er habe den „Techniker“ dreimal darauf hingewiesen, dass der Anschluss so nicht sicher sei, was diesen gar nicht interessiert habe. Auch von Kollegen habe ich gehört, dass die Anschlüsse eben *nicht* entsprechend den Vorgaben der Gematik durchgeführt wurden, auch wenn die daneben stehenden Ärzte ausdrücklich dazu aufgefordert hätten.

Beim präferierten Reihenanschluss sei ja der Konnektor der entscheidende Schutz gegen Zugriffe aus dem Internet, jedoch nur, wenn die darin enthaltene Firewall regelmäßig konfiguriert wird. Das dafür notwendige Zugangskennwort zur Administratoroberfläche sei jedoch von TI- Installateuren regelmäßig nicht herausgegeben worden, wodurch die Vorgaben des BSI nicht erfüllt werden können und die betroffene Praxis allein deswegen

Haftungsprobleme im Falle eines Datenabflusses bekomme. Wurde das schon kommuniziert?

Zum anderen: Die unabhängige Datenschutzkonferenz (DSK) hat am 12.09.2019 beschlossen, dass die Gematik und die Praxen gemeinsam verantwortlich seien. Eine entsprechende gesetzliche Regelung ist nach wie vor nicht geschaffen worden.

Deshalb verstehe ich nicht, wie es sein kann, dass im Grunde sämtliche deutschen Arztpraxen sich an ein Netz anschließen sollen, dessen IT-Sicherheitsanforderungen nicht ausgearbeitet sind, und das auf einer nach wie vor unklaren asymmetrischen Rechtsbasis, mit der derzeit die Ärzte die ganze und die gematik samt Regierung überhaupt keine Verantwortung tragen.

Das einzige, was klar ist, ist dass das Bundesgesundheitsministerium, das ja die Oberhand über die Gematik hat, sich bisher von der Verpflichtung, eine Datenschutzfolgenabschätzung vorzulegen, befreit sieht, während die einzelnen Praxen seit Mai 2018 ein Verzeichnisse und Datenschutzerklärungen entsprechend der DSGVO bereithalten und regelmäßig darauf hingewiesen werden, nach welchem Artikel der DSGVO sie wann wofür bestraft werden. Andererseits zeigt sich, dass das Ministerium die DSGVO bestens kennt, wenn es darum geht, den Art. 23 zu bemühen und das Einsammeln der Krankheits- und OP-Daten von Implantat-Empfängern sozusagen zur nationalen Katastrophenabwehrung zu stilisieren. Hier wird mit sehr verschiedenem Maß gemessen.

Die KVB appelliert, dass das Ministerium Kollegen mit gehackten Praxisverwaltungssystemen nicht im Regen stehen lassen dürfe. Das ist freundlich, greift aber dem Ministerium gegenüber zu kurz. Da braucht es meines Erachtens einen schärferen Ton. Denn es war für den kritischen Beobachter selbstverständlich zu erwarten, dass Herr Spahn ohne Zögern die Ärzte für jegliche Datenpannen sowie die unsicheren TI-Anschlüsse verantwortlich machen wird, während er selbst im Januar 2019 noch kühn öffentlich mitgeteilt hat, wohl im treuen Glauben, wir würden das vergessen: „Ich werde die Telematik und die elektronische Patientenakte vorantreiben, Hacker hin oder her.“ Ob irgendein Kollege im Hagelschauer oder seinem Praxisruin gegenüber steht, dürfte Herrn Spahn völlig gleichgültig sein. Ihm kommt es darauf an, an Daten zu kommen, schnell und alle, wie er beim Implantate-Registererrichtungsgesetz und jetzt im Rahmen des DVG gezeigt hat.

Mitteilungen über unsichere TI-Anschlüsse wurden monatelang ignoriert. Die Kosten für einen seriösen Systemadministrator, der Interesse daran hat, Sicherheitslücken zu finden und das auch kann, sind überhaupt kein Thema. So kostet ja nun ein solcher Spezialist circa 120,- bis 225,- Euro pro Stunde plus MwSt. Sie sind jedoch kaum zu finden, denn es gibt gar nicht genug von ihnen.

So haben wir im Bereich der niedergelassenen Ärzte derzeit eine Situation, die an Abwegigkeit kaum mehr zu überbieten ist: Während die Kollegen, die ihrem Instinkt und zunehmender Erkenntnis folgen und den Anschluss an die TI unterlassen, von „Gesetzes wegen“ bestraft werden, beugen sich die anderen dem Druck und machen sich wiederum strafbar, jedoch nach höheren Recht. Es ist unfassbar, dass Praxen, die bisher aus gutem Grunde überhaupt nicht am Internet waren, nun womöglich auf ein gehacktes Praxisverwaltungssystem blicken, und das für einen völlig versorgungsfremden Versichertenstammdatenabgleich!

Ich denke, es ist an der Zeit, dass sich die Kassenärztlichen Vereinigungen neu definieren. Denn die Vorgaben des BMG entsprechen nicht mehr geltendem Recht, so dass die KVen eben nicht mehr Körperschaften des öffentlichen Rechts sind, sondern verhängnisvoller Weise dem Vollzug von Unrecht adjustieren. Sie haben als KBV das unglückliche Los gezogen, um das ich Sie nicht beneide, Mitglied der Gematik zu sein, die ja der Kontrolle des Gesundheitsministeriums unterliegt. Aber gerade, weil die KBV, wie auch die Bundesärztekammer, Mitglied ist, meine ich, dass hier von innen heraus ein Bereinigungsprozess stattfinden müsste, der das, was auf dem Kopf steht, wieder auf die Füße stellt. Sie sollen wissen, dass in der Kollegenrunde nicht mehr ganz selten Assoziationen an die Zeiten des Nationalsozialismus auftauchen, in denen Ärzte ebenfalls folgsam Gesetze erfüllt haben. Was im BMG an Gesetzen aus der Wiege gehoben wird, verstößt gegen die Verfassung, das ärztliche Berufsrecht und die DSGVO. Wenn die Bevölkerung aufwacht, steht zudem zu befürchten, dass das Ansehen der Ärzte nachhaltig beschädigt wird, wenn die Ärztevertretungen diesem Treiben zusehen und nichts unternehmen. Vielleicht müssen einmal 17x3 KV-Vorstände und eventuell noch 17 Kammerpräsidenten dem Minister gegenüber treten und ihm mitteilen: „So geht es nicht, Herr Spahn!“

So erwarte ich, und ich glaube, ich darf behaupten, nicht nur ich, dass die KBV und die LänderKVen sich entschieden dafür einsetzen, dass die TI ausgesetzt wird, bis die IT-Sicherheitsanforderungen ausgearbeitet, bezüglich Praxistauglichkeit überprüft und die Haftungsfragen belastbar und transparent geklärt sind, das alles unter Wahrung von Grundgesetz, Berufsrecht und DSGVO. Es kann nicht sein, dass die Praxisinhaber quasi auf dem Drahtseil über die Niagarafälle getrieben werden mit der Botschaft: Wenn Ihr nicht geht, zahlt Ihr Strafe. Wenn Ihr geht und abstürzt, seid Ihr selbst schuld und die Beerdigung dürft Ihr auch selbst zahlen.

Mit freundlichen Grüßen