c/o Alexandra Obermeier
Ärztin für Psychiatrie und Psychotherapie
Hörwarthstraße 51
80804 München

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

München, den 07.09.2020

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

10592 Berlin

Offener Brief:

IT-Sicherheitsrichtlinie für Ärztliche Praxen – Einvernehmen vs. Benehmen mit dem BSI – Risiken für die Praxen

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

die KBV und die KZ BV wurden mit der Aufgabe betraut, eine IT-Sicherheitsrichtlinie für Arztpraxen zu erarbeiten, die jedoch vorerst wegen offener Finanzierungsfragen von der Vertreterversammlung abgelehnt wurde. Wie wir erfahren haben, sollen sich die Kosten für die Praxen im ersten Jahr auf etwa € 10.000 bis 50.000 belaufen, in den Folgejahren dauerhaft auf jeweils € 1.000 - 5.000.

Die vorgesehene IT-Sicherheitsrichtlinie orientiert sich am BSI-Grundschutz-Kompendium, welches sowohl für extern vernetzte wie auch als Inselnetz – also ohne Internet- und TI-Anschluss – betriebene Praxen verbindlich sein wird. Der BSI-Grundschutz realisiert aber nur ein niedriges bis mittleres Schutzniveau. Nachdem Gesundheitsdaten jedoch ein hohes oder sehr hohes Schutzniveau erfordern, werden auf die Praxen daher vermutlich noch weitere Lasten zukommen.

Wie uns von Experten, die professionell mit der Einführung von Grundschutz und ISO 27001 befasst sind, versichert wird, sollten die Aufwände für einen Inselbetrieb erheblich niedriger sein als für einen extern vernetzten Betrieb. Die Differenz der Aufwände zwischen diesen beiden Betriebsmodi stellt unserer Auffassung nach die durch die TI-Einführung bedingten Mehraufwände dar.

Deshalb unsere **1. Frage:**
Können Sie uns die Ergebnisse für diese Aufwandsunterschiede bei der Initialinvestition schon bereitstellen?

Bitte gliedern Sie Ihre Antwort nach Praxisgrößen von einer Person (1 Arzt/Psychotherapeut *ohne* Hilfspersonal), der kleinen Praxis (1 Arzt/Psychotherapeut *mit* Hilfspersonal), der Praxis mit 2 oder mehreren Ärzten *samt* Hilfspersonal sowie Großpraxen ab 20 Personen (Pflicht zur Bestellung eines Datenschutzbeauftragten) und geben Sie bitte die Aufwände für die beiden Betriebsmodi an.

2. Frage:
Können Sie schon die Erhaltungsaufwände für die Sicherheitsmaßnahmen der verschiedenen Betriebsmodi und Praxisgrößen bereitstellen?
Falls Sie die ersten beiden Fragen derzeit nicht beantworten können, bis wann können wir mit einer Antwort rechnen?

3. Frage:
Beabsichtigen Sie, diese Aufwandsunterschiede zwischen den beiden Betriebsmodi als TI-bedingte Mehraufwände politisch geltend zu machen und eine Erstattung zu erwirken?

Auf der Internetseite der KBV ist zu lesen, dass die IT-Sicherheitsrichtlinie im Einvernehmen mit dem BSI zu erarbeiten sei. Vom BVVP (Bundesverband der Vertragspsychotherapeuten) haben wir am 24.8.2020 erfahren, dass die KBV beim BSI den Antrag gestellt habe, dass die IT-Sicherheitsrichtlinie nur noch auf der Basis eines Benehmens mit dem BSI erstellt werden soll.

Zur Minimierung der Datenschutzrisiken müssen die technisch-organisatorischen Maßnahmen in der Praxis dem Stand der Technik entsprechen. Eine Umsetzung des Grundschutzes im Einvernehmen mit dem BSI – also mit dem BSI als Garanten – dürfte dem unzweifelhaft genügen.

4. Frage:
Wie gewährleisten Sie, dass auch im Benehmen mit dem BSI Ihre Sicherheitsvorgaben gleichermaßen unzweifelhaft den Stand der Technik repräsentieren?

Mit freundlichen Grüßen

für das Bündnis