Praxisadresse:

An die
Kassenärztliche Vereinigung

__.__.2020

Widerspruch gegen den Honorarabrechnungsbescheid des Quartals 3/2019
Ergänzung für die Quartale 1+2/2019

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit haben wir am 15.01.2020 den Honorarabrechnungsbescheid für das oben genannte Quartal erhalten. Gegen diesen legen wir

Widerspruch

ein.

Der Widerspruch erfolgt zunächst zur Fristwahrung.

Uns ist bekannt, dass zu der Frage nach der Rechtmäßigkeit des Honorarabzugs bei Nicht-Anschluss einer Praxis an die sogenannte Telematik-Infrastruktur und Nichtdurchführung des VSDM ein Musterverfahren gegen die KV Baden-Württemberg geführt werden soll.

Das entsprechende Aktenzeichen wird nachgereicht. Gegenstand dieses

Verfahrens werden zum überwiegenden Teil die auch uns betreffenden Rechtsfragen sein, sodass wir diesen Widerspruch zur Wahrung unserer Rechte einlegen. Wir beantragen bis zum Abschluss dieses Musterverfahrens das Ruhen dieses Widerspruchverfahrens.

Wir bitten um schriftliche Eingangsbestätigung des Widerspruchs und um Bestätigung der Ruhendstellung dieses Widerspruchverfahrens bis zur Entscheidung der Musterverfahren in Baden-Württemberg.

Begründung:

Die Honorarbescheide für das Abrechnungsquartale I +II + III/2019 sind – soweit es den pauschalen Abzug in Höhe von 1 Prozent des Gesamthonoraranspruchs betrifft – aufzuheben, da die seitens des Gesetzgebers auferlegte Pflicht zur Durchführung des Versichertenstammdatenabgleichs (§ 291 Abs. 2b S. 3 SGB V) mit den derzeit von der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zugelassenen Komponenten-Modellen der Telematik-Infrastruktur (TI) für die verpflichteten Leistungserbringer, so also auch für uns als Widerspruchsführer, nur unter Verstoß gegen höherrangiges Recht möglich wäre.

Die Nutzung der TI-Komponenten „Konnektor, eGK (Patientenausweis), Arztausweis und Praxisausweis“ verstößt zumindest in Form der derzeitigen rechtlichen und tatsächlichen Ausgestaltung gegen Vorschriften der Datenschutzgrundverordnung (DSGVO).

Zudem führen diese Datenschutzverstöße sowie die konkret nachweisbaren Sicherheitsmängel der Telematik-Infrastruktur im Ergebnis zu einem von uns nicht hinzunehmenden, unverhältnismäßigen Eingriff in unsere Berufsausübungsfreiheit gemäß Art. 12 GG.

1. Verstöße gegen die DSGVO

Die derzeitige tatsächliche und regulatorische Ausgestaltung des Versichertenstammdatenmanagements (VSDM) verstößt in mehrfacher Hinsicht gegen höherrangiges Recht in Form der Datenschutzgrundverordnung:

Zur technischen Durchführung des VSDM dient die sog. Telematik-Infrastruktur, bestehend aus zwei Zonen: der sog. zentralen Zone (zentrale Vernetzung zwischen allen Beteiligten), und der sog. dezentralen Zone (notwendige technische Ausstattung und Anbindung des jeweils Beteiligten, z. B. in einer Arztpraxis).

Über die dezentrale Zone der TI, nämlich über den in der Arztpraxis zu installierenden Konnektor und das daran angeschlossene Kartenlesegerät, werden die auf der jeweiligen elektronischen Gesundheitskarte gespeicherten Daten eines jeden Patienten ausgelesen und an die zentrale Zone der TI zum Abgleich mit den bei der jeweiligen Krankenversicherung gespeicherten Daten weitergesandt. Das stellt eine Datenverarbeitung personenbezogener Daten im Sinne von Art. 4 Ziff. 2 DSGVO dar.

Neben den eigentlichen Stammdaten des Versicherten (wie z. B. Name, Anschrift, Geburtsdatum, Krankenversicherung) werden auch bereits gesundheitsbezogene Daten gespeichert und verarbeitet. Gemäß dem „Fachkonzept Versichertenstammdatenmanagement“ der gematik und der„technischen Anlage zu Anlage 4 Bundesmantelvertrag-Ärzte (BMV-L)“ wird auf der elektronischen Gesundheitskarte ein „DMP-Kennzeichen“ zu folgenden chronischen Erkrankungen gespeichert:

Diabetes mellitus Typ 2, Brustkrebs, Koronare Herzkrankheit, Diabetes mellitus Typ 1, Asthma bronchiale und/oder COPD.

Hierbei handelt es sich zweifellos um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DSGVO.

Eine Datenverarbeitung ist bereits im Ansatz rechtlich überhaupt nur zulässig, wenn ein „Verantwortlicher“ der Datenverarbeitung im Sinne von Art. 4 Nr. 7 DSGVO feststeht, denn die Pflichten aus Art. 5 DSGVO setzen zum großen Teil der Datenverarbeitung zeitlich vorgelagerte Maßnahmen voraus, so z. B. die Prüfung der Rechtmäßigkeit der Datenverarbeitung (§ 5 Abs. 1 lit. a DSGVO), die Festlegung des Verarbeitungszwecks (§ 5 Abs. 1 lit. b DSGVO) und Gewährleistung der

Datensicherheit durch geeignete technische und organisatorische Maßnahmen (§ 5 Abs. 1 lit. f DSGVO) sowie Art. 24 Abs. 1, Art. 32 DSGVO.

Trotz dieser eindeutigen gesetzlichen Vorgaben und trotz des Umstands, dass über den TI-Konnektor beim VSDM bereits sogar Gesundheitsdaten in einem

ganz erheblichen Umfang verarbeitet werden, ist die datenschutzrechtliche Verantwortlichkeit für die Telematikinfrastruktur unerklärt bzw. niemand hat sich zu dieser Verantwortung bekannt, geschweige denn die daraus erwachsenden Pflichten erfüllt. Das gesamte Pflichtenregime der DSGVO läuft ins Leere, solange sich der „Verantwortliche“ für eine Datenverarbeitung nicht bestimmen lässt. Insbesondere die gematik hat diese Verantwortung bislang nicht anerkannt und auch die Pflichten des „Verantwortlichen“ nicht erfüllt.

Demgegenüber hat die Datenschutzkonferenz (DSK – Konferenz der unabhängigen Datenschutzaufsichtsbehörden Seite 3 des Bundes und der Länder) einen Beschluss am 12.09.2019 dahingehend gefasst, dass sie zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der

Telematikinfrastruktur die Auffassung vertritt, dass die gematik für die zentrale Zone der Telematikinfrastruktur datenschutzrechtlich alleinverantwortlich und für die dezentrale Zone der TI datenschutzrechtlich mitverantwortlich ist. Ferner mahnt die Datenschutzkonferenz an, dass der Umfang der Verantwortung der gematik für die dezentrale Zone einer gesetzlichen Regelung bedürfe, aber führt gleichzeitig aus, dass die gematik für die Verarbeitung verantwortlich sei, soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt sei. Soweit die Datenschutzkonferenz im vorgenannten Beschluss von einer „Mitverantwortlichkeit“ für die dezentrale Zone spricht, wird offengelassen, wer die übrigen Mitverantwortlichen sind bzw. welche Aufgaben und Pflichten die jeweils Beteiligten zu erfüllen haben.

Die fehlende Klärung der datenschutzrechtlichen Verantwortung hat entscheidende praktische Folgen: einerseits die Unklarheit, wer für welche Bereiche der Telematikinfrastruktur die datenschutzrechtliche ex-ante-Sicherheitsbewertung in Form der Datenschutzfolgenabschätzung (Art. 35 DSGVO) oder Meldungen bzw. Maßnahmen bei Datenpannen (Art. 33, 34 DSGVO) vorzunehmen hat, andererseits, wer die Betroffenenrechte gemäß Art. 12ff. DSGVO zu erfüllen hat.

Derzeit ist unklar, an wen sich der Patient wenden muss, wenn er erfahren will, welche Daten über ihn an welcher Stelle im Zuge der TI gespeichert werden und wenn er inhaltlich falsche Daten über sich korrigieren bzw. löschen lassen möchte. Diese fehlende Klärung der datenschutzrechtlichen Verantwortlichkeit

stellt nicht nur einen Verstoß gegen Art. 5 DSGVO, sondern auch einen Verstoß gegen das verfassungsrechtliche Bestimmtheitsgebot dar. Die fehlende Klärung der datenschutzrechtlichen Verantwortlichkeit stellt ferner einen Verstoß gegen Art. 9 Abs.2 lit. i DSGVO sowie § 22 Abs. 1 Ziff. 1 lit. c, Abs. 2 BDSG dar, da eine fehlende Klärung der datenschutzrechtlichen Verantwortlichkeit zwingend dazu führt, dass „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ nicht sichergestellt sind, was nach Art. 9 Abs. 2 lit. i DSGVO jedoch für die Verarbeitung von Gesundheitsdaten zum Zwecke der öffentlichen Gesundheit erforderlich wäre.

Auch wenn nun spätestens mit dem Beschluss der Datenschutzkonferenz vom 12.09.2019 klar ist, dass in Bezug auf die dezentrale Zone der Telematikinfrastruktur, also z. B. der TI-Anbindung in der jeweiligen Arztpraxis, die Konstellation der datenschutzrechtlichen Mitverantwortlichkeit, Art. 26 DSGVO, vorliegt, fehlt ein Regelungswerk im Sinne von Art. 26 Abs. 1 S. 2 DSGVO, aus welchem hervorgeht, wer die Mitverantwortlichen sind und wer von ihnen welche Pflicht aus der DSGVO erfüllt, insbesondere, was die Wahrnehmung der Rechte der betroffenen Personen – also der Patienten unserer Praxis – angeht (Art. 13 bis 21 DSGVO). Eine Vereinbarung bzw. gesetzliche Regelung im Sinne von Art. 26 Abs. 1 DSGVO müsste zumindest in Bezug auf die dezentrale Zone der TI im Verhältnis zwischen gematik und den jeweiligen Praxisinhabern vorgenommen werden, denn die Ärzte sind „Mitverantwortliche“ im Sinne von Art. 26 DSGVO. Sie treffen als Hausherren ihrer Praxis die Entscheidung darüber, ob etwas ein TI-Konnektor an die zentrale Zone der Telematikinfrastruktur angeschlossen wird bzw. ob er anschließend zum Zwecke des VSDM genutztwird. Mit dem Verstoß gegen Art. 26 Abs. 1 S. 2 DSGVO wird somit derzeit im Zuge des VSDM gegen höherrangiges Recht verstoßen.

Gemäß Art. 35 DSGVO hätte eine Sicherheitsbewertung in Form einer sog. Datenschutzfolgenabschätzung (DSFA) vor Beginn der im Zuge des VSDM stattfindenden Datenverarbeitung zwingend erfolgen müssen, was auch seitens des Bundesdatenschutzbeauftragten gegenüber der gematik eingefordert wurde. Eine DSFA liegt seitens der gematik jedoch derzeit weder für die zentrale Zone der Telematikinfrastruktur vor, noch für die dezentrale Zone, also somit auch nicht für den TI-Konnektor und die Datenverarbeitung im

Zuge des VSDM. Mit diesem Verstoß gegen Art. 35 DSGVO wird derzeit im Rahmen des VSDM gegen höherrangiges Recht verstoßen.

Ferner werden Art. 5 Abs. 1 lit. f, Art. 24 Abs. 1 S. 2, Art. 32 Abs. 1 lit. d DSGVO sowie § 291b Abs. 1 S. 1 Ziff. 3 sowie Abs. 1a S. 6 SGB V durch die bereits anfänglichen technischen Vorgaben seitens gematik und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verletzt. Für die Zertifizierung der TI-Konnektoren wurden in Bezug auf das VSDM bislang zwei sog. Schutzprofile von der gematik in der Zusammenarbeit mit dem BSI entwickelt, nämlich BSI-CC-PP-0047-2015 sowie BSICC-PP-0097-2018, in denen die technischen Vorgaben für die TI-Konnektoren gemacht werden.

Das vom BSI angewandte Prüf- und Zertifizierungssystem „Common Criteria“ (ISO/IEC 15408) für die Schutzprofile der TI-Konnektoren sieht Sicherheitsstufen beginnend mit der niedrigsten Stufe EAL1 und der höchsten Stufe EAL7 vor. Die für die TI-Konnektoren geltenden Schutzprofile BSI-CCPP-0047-2015 und BSI-CC-PP-0097-2018 sehen jeweils die Stufe EAL3 vor. Diese Einstufung ist im Ergebnis zu niedrig und kann nur darauf zurückzuführen sein, dass das BSI bei der Einstufung nicht berücksichtigt hat, dass auch bereits im Rahmen des VSDM Gesundheitsdaten (Art. 9 DSGVO) verarbeitet werden.

Bei Gesundheitsdaten ist mindestens die Sicherheitsstufe EAL4 angemessen und erforderlich.

Entgegen Art. 5 Abs. 1 lit. f, Art. 24 Abs. 1 S. 2, Art. 32 Abs. 1 lit. d DSGVO fehlt es zudem an den gesetzlich erforderlichen Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, allein schon aufgrund des Umstands, dass es an Vorgaben für eine regelmäßige Wartung und deren Überprüfung der TI-Konnektoren fehlt, sodass bereits jetzt nachweislich veraltete, nicht gewartete Open-Source-Softwarestände in den TI-Konnektoren verwendet werden, die bekannte Sicherheitsmängel aufweisen.

Das Schutzprofil BSI-CC-PP-0047-2015, Seite 25, erlaubt einen externen Fernwartungszugang auf den TI-Konnektor. Dort werden gleich zwei wesentliche Sicherheitsanforderungen, die heute für Fernwartungszugänge

Stand der Technik sind, nicht gestellt, nämlich eine Zwei-Faktor Authentisierung sowie einen VPN-Tunnel. Angesichts dieser zu niedrigen Sicherheitsanforderungen wäre die Zertifizierung eines TI-Konnektors nach dem Schutzprofil BSI-CC-PP-0047-2015 möglich, wenn ein Fernwartungszugang durch das freie Internet (ohne VPN-Tunnel) erfolgt und der Fernzugriff auf den Konnektor in der Arztpraxis dabei nur mit einem einfachen Passwort oder PIN (ohne ZweiFaktor-Authentisierung) abgesichert wäre. Dies entspricht nicht dem Stand der Technik und stellt einen Sicherheitsmangel dar.

Der Einsatz von Verschlüsselungstechniken ist für die Verarbeitung personenbezogener Daten allgemein in Art. 32 Abs. 1 lit. a DSGVO und vom deutschen Gesetzgeber insbesondere für Gesundheitsdaten in § 22 Abs. 2 Ziff. 7 BDSG vorgeschrieben. Die im Schutzprofil BSI-CC-PP-0047-2015 vorgesehenen Verschlüsselungstechniken („SHA-1“ sowie eine Entropie von 100 bit) genügen diesen Anforderungen nach heutigem Stand der Technik nicht mehr.

In dem Schutzprofil BSI-CC-PP-0047-2015 finden sich entgegen § 291b Abs. 1 S. 4 SGB V keine technischen Anforderungen zum Schutz der Patientendaten im IT-System der Arztpraxis. Das Schutzprofil adressiert ausschließlich den Schutz der Telematikinfrastruktur und des dortigen Datenverkehrs von außen, nicht aber den Schutz des Datenbestands in der Arztpraxis gegen IT Angriffe aus bzw. über die Telematik-Infrastruktur, obwohl der Schutz der in der Arztpraxis gespeicherten Patientendaten (Befunde, Krankheitsgeschichten etc.) wesentlich wichtiger ist als die bloßen Versichertenstammdaten.

Auch mit der fehlenden Regulierung und Überprüfung der Installation der TI-Konnektoren wird derzeit im Zuge des VSDM gegen höherrangiges Recht, nämlich gegen Art. 5 Abs. 1 lit. f, Art. 24 Abs. 1 S. 2, Art. 32 Abs. 1 DSGVO verstoßen, ferner gegen das verfassungsrechtliche Bestimmtheitsgebot mangels hinreichender gesetzlicher Regelungen hierzu. Angesichts der zahlreichen datenschutzrechtlichen Verstöße kann der jeweilige Arzt nicht verpflichtet sein, an der Datenverarbeitung im Zuge des VSDM als datenschutzrechtlich „Mitverantwortlicher“ (Art. 26 DSGVO) mitzuwirken. Der Arzt, somit auch wir als Widerspruchsführer, wären als datenschutzrechtlich Mitverantwortliche nicht nur Teil einer rechtswidrigen Datenverarbeitung,

sondern auch der finanziellen Mithaftung für datenschutzrechtliche Verstöße gemäß Art. 82 Abs. 4 DSGVO sowie dem Bußgeldrisiko gemäß Art. 83 DSGVO mit einem Bußgeldrahmen von bis zu 4 % des Jahresumsatzes bzw. 20 Mio. Euro ausgesetzt, denn z. B. bereits die fehlende Vereinbarung im Sinne von Art. 26 Abs. 1 S. 2 DSGVO erfüllt den Bußgeldtatbestand.

2. Verstoß gegen das Grundrecht auf Berufsfreiheit, Art. 12 GG

Die derzeitige rechtliche und tatsächliche Umsetzung der gesetzlichen Vorschriften zur elektronischen Gesundheitskarte und zum TI-Konnektor gemäß §§ 291, 291a und 291b SGB V verletzt das Grundrecht der Ärzte und somit auch die Widerspruchsführer aus Art. 12 GG, weswegen die Widerspruchsführer nicht zur Teilnahme am Versichertenstammdaten-management verpflichtet sein können und für die bislang unterbliebene TI-Anbindung auch nicht sanktioniert werden dürfen.

Ansatzpunkt für den hiesigen Widerspruch ist nicht die Rechtsverteidigung gegen die Pflicht zum Versichertenstammdatenmanagement an sich, sondern die Rechtsverteidigung gegen die derzeitige konkrete datenschutzrechtliche und technische Umsetzung durch die gematik. Wie in Abschnitt 1 dieses Schriftsatzes konkret dargelegt wurde, begründet die jetzige rechtliche, organisatorische und technische Umsetzung zahlreiche datenschutzrechtliche Verstöße und es gibt umfangreiche konkrete Sicherheitsmängel.

Der derzeitige Zustand führt bei den Ärzten und Psychologischen Psychotherapeuten zu einem datenschutzrechtlich rechtswidrigen Zustand und zu erheblichen Gefährdungen der auf der elektronischen Gesundheitskarte gespeicherten Patientendaten und der im Praxisinformationssystem der Praxis gespeicherten weiteren Gesundheitsdaten.

Der angegriffene Honorarbescheid ist demnach insoweit aufzuheben.

3. Musterverfahren in Baden-Württemberg

Wie wir Ihnen bereits mitteilten, läuft demnächst in dieser Angelegenheit in Baden-Württemberg ein Musterverfahren. Das entsprechende Aktenzeichen

wird nachgereicht. Gegenstand dieses Musterverfahrens werden zum überwiegenden Teil die auch uns betreffenden Rechtsfragen sein, sodass dieser Widerspruch (auch) zur Wahrung unserer Rechte eingelegt wird.

Wir beantragen daher nochmals, das streitgegenständliche Widerspruchs-verfahren bis zum rechtskräftigen Abschluss des Musterverfahrens ruhend zu stellen. Dies nicht zuletzt um eine KV-übergreifende, einheitliche und rechtssichere Entscheidung in dieser Sache zu treffen.

Nach weiteren Informationen zur Sicherheit der einzelnen Komponenten, Kartenlesegerät, Konnektor, Heilberufsausweis und Patientenkarte (sGK), auf dem Jahreskongress des Chaos Computer Clubs in Hamburg Ende Dezember 2019, sowie zur Sicherheit der benutzten Software in den Konnektoren lt. eines Berichtes der Computerzeitschrift c´t im Januar 2020 (Quelle: https://www.heise.de/select/ct/2020/3/1580498856872446), erlauben wir uns diesen Widerspruch jederzeit noch zu ergänzen und hoffen auf Ihr Verständnis.

Wir danken Ihnen für Ihre Geduld und bitten um schriftliche Eingangsbestätigung der Widerspruchsbegründung und um Bestätigung der Ruhendstellung dieses Widerspruchverfahrens bis zur rechtskräftigen Entscheidung der Musterverfahren in Baden-Württemberg.

Mit freundlichen Grüßen