KVB
Kassenärztliche Vereinigung Bayerns

Stellungnahme der psychotherapeutischen Berufsverbände und der KVB zum Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)

Zahlreiche Vertreter psychotherapeutischer Berufsverbände in Zusammenarbeit mit der Kassenärztlichen Vereinigung Bayerns begrüßen zunächst die mit dem Entwurf verfolgte Zielrichtung, die Verarbeitung von Patientendaten im Rahmen der Digitalisierung des Gesundheitswesens bzw. der Nutzung der in diesem Zusammenhang aufgebauten Telematikinfrastruktur gesetzlich zu regeln und dabei den Anforderungen des Datenschutzes gerecht zu werden.

Eine erfolgreiche psychotherapeutische Behandlung steht und fällt mit dem Vertrauensverhältnis zwischen Psychotherapeut und Patient. Dieses Vertrauensverhältnis basiert wiederum zum Großteil darauf, dass der Patient sich sicher sein kann, dass die sensiblen, gesundheitsrelevanten Informationen, die er mit seinem Psychotherapeuten teilt, dort gut aufgehoben sind. Es muss demnach in jedem Fall ausgeschlossen werden, dass die angesprochenen sensiblen Informationen durch gesetzliche Regelungen in falsche Hände geraten und so das Vertrauensverhältnis nachhaltig gestört wird.

Um den hohen Schutzbedarf der besonderen Kategorien personenbezogener Daten (Art. 9 Abs.1 DSGVO) gerecht werden zu können, bedarf es normenklarer gesetzlicher Regelungen, die dem Bestimmtheitsgebot Rechnung tragen und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) stehen. Diesen Vorgaben wird der Gesetzesentwurf an wesentlichen Stellen nicht gerecht. Dies nicht zuletzt vor dem Hintergrund, dass die medizinischen Daten nicht nur Informationen über den Patienten, sondern auch über dessen (Kindes-)Kinder und Eltern beinhalten können und Informationen minderjähriger Patienten ungeschützt von Sorgeberechtigten eingepflegt, eingesehen und bearbeitet werden können. Diese Implikationen sind oftmals noch unerforscht und die Konsequenzen der freien Verarbeitung dieser Daten sind somit heutzutage nicht absehbar. Da wir hier Neuland betreten, ist es auch nicht verwunderlich, dass es in diesem Bereich keine Standards zum Schutz der Privatsphäre gibt. Folglich müssen im ersten Schritt unbedingt geeignete Standards entwickelt werden, bevor die Daten zugänglich gemacht werden.

Mehrere Punkte sehen wir gerade aus psychotherapeutischer Sicht mehr als kritisch:

1. Angebot und Nutzung zusätzlicher Inhalte und Anwendungen – Unspezifische Öffnungsklausel (§ 345) und Einsicht der Krankenkassen in Sozialdaten der Versicherten (§ 284 Abs. 1 Satz 1 Nr. 20)

Hintergrund:

- Ermöglicht Krankenkassen durch Einwilligung des Versicherten an Informationen zu gelangen, die der ärztlichen Schweigepflicht unterliegen (Gefahr Case-Management der Krankenkassen)

Forderung:

- Daten dürfen trotz Einwilligung betroffener Patienten nur verarbeitet werden, wenn Daten im SGB V ausdrücklich vorgesehen
- Darf sich nicht um medizinische Daten handeln
- Konkretisierung, um welche Daten es sich handelt
- Es muss für Patienten nachvollziehbar sein, wann zu welchem Zweck auf welche Daten zugegriffen wurde
- *Anpassungsvorschlag für den § 345 SGB V*

Ein wichtiger Grundsatz der elektronischen Patientenakte war an sich klar definiert: Krankenkassen sollte grundsätzlich der Zugang zu den in der elektronischen Patientenakte gespeicherten Daten verwehrt bleiben. Die Hoheit über seine besonders sensiblen Gesundheitsdaten darf einzig und allein

der Versicherte selbst haben. Wir ärztlichen, psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten halten es für essenziell, dass die Patientenakte ausschließlich dem Versicherten gehört, der umfassend über Fragen zu Datenschutz und Datensicherheit informiert werden sollte. Dies gilt auch für minderjährige Patienten.

Mit diesem Grundsatz sollte verhindert werden, dass Krankenkassen von sich aus Versicherten, aufgrund der Kenntnisnahme von spezifischen Gesundheitsdaten versichertenbezogene Leistungen nicht mehr anbieten oder gewähren.

Mit den im PDSG nunmehr vorgesehenen Regelungen zu § 345 SGB V sowie § 284 Abs. 1 Satz 1 Nr. 20 SGB V wird von diesem Grundsatz massiv abgerückt. Durch die Regelung in § 284 Abs. 1 Satz 1 Nr. 20 SGB V wird für die Krankenkassen eine ausdrückliche Befugnisnorm geschaffen, die es den Krankenkassen zukünftig ermöglicht, Sozialdaten ihrer Versicherten zu erheben und zu speichern, soweit dies für das Angebot zusätzlicher Anwendungen i.S.d. § 345 Abs. 1 SGB V erforderlich ist. Diese Regelungen führen zu dem oben beschriebenen Worst-Case-Scenario. Verstärkt wird dies durch die Tatsache, dass der Verarbeitungsbefugnis der Krankenkassen keinerlei Beschränkungen oder Grenzen gesetzt wurden. Zwar ist vorgegeben, dass die Krankenkassen die erforderlichen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit der zusätzlichen Anwendungen ergreifen müssen, konkrete Vorgaben, die die Krankenkassen verpflichtend einhalten müssten, sind aber in keinster Weise vorgesehen. Das hat letztlich zur Folge, dass jede Krankenkasse selbst über die jeweiligen Schutzmaßnahmen entscheidet.

Das Resultat: Krankenkassen können an Informationen gelangen, die eigentlich der ärztlichen Schweigepflicht unterliegen. Es besteht so die große Gefahr, dass auf diese Weise die Türe zum Case-Management durch die Krankenkassen geöffnet wird und somit nicht mehr die ärztliche oder psychotherapeutische Expertise Therapieentscheidungen leiten.

Neben namhaften Datenschutzrechtlern, die erhebliche datenschutzrechtliche Bedenken in diesem Zusammenhang äußern, kritisiert auch der Gesundheitsausschuss des Bundesrates die vorgesehene Regelung und fordert deren Überarbeitung. Gerade vor dem Hintergrund, dass Krankenkassen von jeglichen Pönaleregelungen nach der Datenschutz-Grundverordnung ausgenommen sind, ist es umso wichtiger, dass die Krankenkassen nur eng begrenzte und klar formulierte Datenverarbeitungsbefugnisse bekommen.

Deswegen fordern wir:

Die Regelungen zu § 345 SGB V müssen dahingehend überarbeitet werden, dass Krankenkassen eine strikte Beschränkung hinsichtlich der Verarbeitung der von den Versicherten freigegebenen Daten auferlegt wird. Sensible Gesundheitsdaten dürfen nur verarbeitet werden, wenn eine Datenverarbeitung im SGB V ausdrücklich vorgesehen ist. Die Erhebung, Verarbeitung und Speicherung medizinischer Daten ist auszuschließen. Für den Patienten muss klar nachvollziehbar sein, welcher Akteur zu welchem Zeitpunkt mit welcher Absicht auf seine Daten zugegriffen hat.

Dateneinsicht, Zugriff, Verarbeitung, Speicherung oder Löschen von Daten ist Minderjährigen nicht zumutbar und aufgrund persönlicher Schutzrechte Jugendlicher durch Sorgeberechtigte zu verhindern, weswegen das Einpflegen von Daten Minderjähriger gesondert behandelt werden muss und evtl. nur eingeschränkt erfolgen kann, z.B. keine Dateneinspeisung aus psychotherapeutischem Behandlungskontext.

2. Berechtigungskonzept (§ 342)

Hintergrund:

- ePA im 1. Jahr ohne feingranulares Berechtigungskonzept

Forderung:

- Einführung der ePA erst, wenn feingranulares Zugriffsberechtigungsmanagement umgesetzt
- Muss sichergestellt sein, dass alle Patienten diskriminierungsfrei eine feingranulare Möglichkeit haben, Dokumente freizugeben, auch wenn sie nicht über ein mobiles Endgerät auf ePA zugreifen
- *Änderungsvorschlag für § 342 Abs. 2 SGB V*

Bei der Einführung der ePA muss zwingend bereits von Beginn an die Datensouveränität der Versicherten gewährleistet sein. Dies ist allerdings erst dann gegeben, wenn ein differenziertes feingranulares Berechtigungsmanagement für die Versicherten zur Verfügung steht und sie einzelnen Behandlern den Zugriff auf ausgewählte Dokumente erlauben oder verwehren können.

Aus psychotherapeutischer Sicht bestehen starke datenschutzrechtliche Bedenken hinsichtlich dieser zeitversetzen Regelung. Der Versicherte muss zu jedem Zeitpunkt die Möglichkeit besitzen, ausgewählten Leistungserbringern zeitlich und inhaltlich eingrenzbare Zugriffsberechtigungen auf Daten seiner ePA zu erteilen, diese inhaltlich auszuweiten, zeitlich zu verlängern und erteilte Zugriffsberechtigungen wieder vollständig zu entziehen.

Die aktuell vorgesehene Regelung konterkariert diese unbedingt notwendigen Kriterien und steht damit im Gegensatz zu dem Grundkonzept einer versichertengeführten, transparenten elektronischen Patientenakte.

Darüber hinaus ist es inakzeptabel, dass Versicherte ohne geeignetes Endgerät ihre Zugriffsrechte an den im PDSG vorgegeben Terminals nur mittelgranular verwenden können. Das würde eine Diskriminierung von etwa 16 Millionen Versicherten zur Folge haben. Die datenschutzrechtlich gebotenen Berechtigungsmöglichkeiten müssen allen Versicherten diskriminierungsfrei und unabhängig von deren technischer Ausstattung bzw. Know-How zur Verfügung gestellt werden.

Deswegen fordern wir:

Mit Einführung der ePA ist seitens der Krankenkassen ein feingranulares Berechtigungskonzept vorzuhalten; sollte dies bis zum 01.01.2021 nicht realisierbar sein, ist die Einführung der ePA zu verschieben. Zudem muss sichergestellt sein, dass alle Versicherten diskriminierungsfrei eine feingranulare Möglichkeit haben, einzelne Dokumente freizugeben, auch wenn sie hierfür nicht über ein geeignetes (mobiles) Endgerät verfügen .

Dem der Gesetzesbegründung zu entnehmenden Argument, wonach die Regelung für Versicherten ohne Endgerät unproblematisch sei, da die Anwendung noch immer freiwillig sei, kann nicht gefolgt werden.

3. Datenschutzrechtliche Verantwortlichkeit (§ 307 SGB V)

Hintergrund:

- Verantwortlichkeit der Umgebung der genutzten Komponenten der dezentralen Infrastruktur

Forderung:

- Haftungsumfang der Leistungserbringer eingrenzen
- *Änderungsvorschlag für § 307 SGB V*

Der § 307 SGB V regelt die datenschutzrechtliche Verantwortlichkeit und differenziert dabei nach Teilen der Telematikinfrastruktur. Laut der Gesetzesbegründung (siehe BR-Drs. 19/18793) sind insbesondere Ärzte und Psychotherapeuten für die Verarbeitung der Gesundheitsdaten der Versicherten mittels der in ihrer Umgebung genutzten Komponenten (vor allem der Konnektor) der dezentralen Infrastruktur verantwortlich. Die Verantwortlichkeit erstreckt sich schwerpunktmäßig auf die Sicherstellung der bestimmungsgemäßen Nutzung der Komponenten, deren ordnungsgemäßen Anschluss und die Durchführung der erforderlichen fortlaufenden Software-Updates. Diese einseitig zu Lasten der Ärzte und Psychotherapeuten verlagerte datenschutzrechtliche Verantwortung für von der gematik zugelassenen Komponenten ist abzulehnen und widerspricht im Übrigen dem Petitum der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aus dem September 2019.

Nicht ausreichend ist die nunmehr vorgesehen „Auffangregelung“ in § 307 Abs. 5 SGB V, wonach die gematik nur dann verantwortlich ist, wenn sie im Rahmen ihrer Aufgaben nach § 311 Abs. 1 SGB V die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen des § 307 begründet ist. Dies bildet mitnichten die tatsächlichen Gegebenheiten einer gemeinsamen Verantwortlichkeit ab und wird insofern auch nicht den Anforderungen an die Datenschutz-Grundverordnung gerecht.

Auch in den Empfehlungen des Gesundheitsausschusses des Bundesrates vertritt man diese Ansicht, wonach die gematik kein bloßer Vermittlungsdienst ist und somit Teil einer vollen, gemeinsamen Verantwortlichkeit sein sollte: *„Durch die Zuweisung von technischen Hilfsdiensten, wie das Betreiben eines Netzes, die technische Umsetzung von Zugangsdiensten und Diensten der Anwendungsinfrastruktur an andere Stellen kann diese datenschutzrechtliche Verantwortlichkeit der Gesellschaft für Telematik nicht pauschal verneint werden“* (BR Drucksache 164/1/20, S. 6-7). Demnach dürfe, so die Empfehlung, auch keine Stelle durch die Gesetzgebung als allein verantwortlich bezeichnet werden.

In der Begründung des Kabinettsentwurfes wird zu § 307 SGB V ausgeführt, dass sich die Zuweisung der Verantwortlichkeit daran orientiert, ob sie für die jeweiligen Strukturen, d.h. den Ärzten und Psychotherapeuten, überblickbar und beherrschbar ist. Bezüglich der Datenverarbeitung mit den Komponenten der Telematikinfrastruktur ist dies jedoch sicher nicht gegeben. In der spezifischen Ausgestaltung der Telematikinfrastruktur sind die Leistungserbringer weder geschult noch können sie die Risiken einschätzen. Anders sieht die Ausgangslage bei der gematik aus, die für die Verarbeitung, insbesondere soweit sie von ihr vorgegebene Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist, verantwortlich ist.

Deswegen fordern wir:

Es muss klargestellt werden, dass Ärzte und Psychotherapeuten ausschließlich für die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten der TI verantwortlich sein können. In dem Gesetz müssen die Regelungen und Vorgaben der gemeinsamen Verantwortlichkeit gebührend zum Ausdruck gebracht werden. Die aktuelle Regelung bestimmt nicht zweifelsfrei, wer im Falle eines Datenlecks zur Verantwortung gezogen wird. Im Zweifelsfall wird sich der Versicherte in der Realität an seinen Arzt oder Psychotherapeuten wenden. Eine Tatsache die nicht hinnehmbar ist. Dies muss im Sinne einer gemeinsamen Verantwortlichkeit klar geregelt werden.

4. Datenfreigabe aus der ePA zu wissenschaftlichen Forschungszwecken (§363 SGB V)

Hintergrund:

- PDSG ermöglicht freiwillige und umfassende Datenfreigabe für Forschungszwecke

Forderung:

- Gesonderte Informationen zur Datenfreigabe
- Datenfreigabe nur zu medizinisch-wissenschaftlichen Forschungszwecken
- Ausschluss Re-Identifizierung, auch bzgl. (zukünftiger) Angehöriger des Versicherten
- *Änderungsvorschlag für § 363 SGB V*

Spätestens ab dem Jahr 2023 soll es möglich sein, auf Basis einer informierten Einwilligung eine freiwillige Datenfreigabe für Forschungszwecke zu tätigen. An dieser Stelle ist es entscheidend, dass eine solche Freigabe von Daten freiwillig und unabhängig von der Nutzung von Anwendungen der Telematikinfrastruktur durch die Versicherten sein muss. Das bedeutet auch, dass Patienten sich nicht unter Druck gesetzt fühlen und auch nicht durch finanzielle Anreize zu einer Datenfreigabe durch die Krankenkassen bewegt werden. Die ePA darf sich am Ende nicht zu einem Lieferanten von Forschungsdaten entwickeln.

Deswegen fordern wir:

Es ist dabei sicherzustellen, dass eine Verarbeitung von Daten der ePA ausschließlich zu **medizinisch-wissenschaftlichen** Forschungszwecken erfolgen darf Zudem sollte die Datenfreigabe nicht pauschal, d.h. inhaltlich und zeitlich unbeschränkt erfolgen können, sondern immer auf konkrete Forschungsvorhaben bezogen sein. Es muss außerdem in jedem Fall die Möglichkeit der Re-Identifizierung der Versicherten sowie seiner (zukünftigen) Angehörigen unabhängig vom Grad der Verwandtschaft ausgeschlossen sein, da die medizinischen Daten – wie eingangs bereits ausgeführt – nicht nur Informationen nur über den Patienten, sondern auch über dessen (Kindes-)Kinder und Eltern beinhalten können. Die Freigabe sensibler Daten muss eine individuelle und höchstpersönliche Entscheidung bleiben. Sie darf nicht von anderen Personen, z.B. Sorgeberechtigten getroffen werden. Deshalb kann die freiwillige Datenspende zu Forschungszwecken erst ab dem 18. Lebensjahr erfolgen. Diese Implikationen sind oftmals noch unerforscht und die Konsequenzen der freien Verarbeitung dieser Daten sind somit heutzutage nicht absehbar. Um dies zu erreichen, ist sicher zu stellen, dass die Anonymität des Versicherten allumfassend, d.h. auch über seinen Tod hinaus (postmortal) gewährleistet ist.

5. Honorarverlust bei Nicht-Anschluss an die TI (§ 291b und § 341 Abs. 6 SGB V)

Hintergrund:

- 1 Prozent Honorarverlust bei fehlendem Datenabgleich auf elektronischer Gesundheitskarte (TSVG)
- Durch DVG ab 01.03.2020: Erhöhung dieses Honorarverlusts auf 2,5 Prozent
- Neu durch PDSG: Honorarverlust von 1 Prozent, wenn Vorkehrungen für ePA nicht bis zum 30.06.2021 getroffen werden
- gematik hat weiterhin keine Datenschutz-Folgenabschätzung durchgeführt

Forderung:

- *Ersatzlose Streichung von § 341 Abs. 6 (PDSG) sowie § 291b Abs. 5 SGB V (TSVG/DVG)*
- Alternative: Sanktionierung darf nicht erfolgen, wenn der Leistungserbringer diese nicht zu vertreten hat
- Sanktionen müssen ausgesetzt werden, bis die Datenschutz-Folgenabschätzung durch die gematik ordnungsgemäß durchgeführt wurde

Nach der aktuellen Regelung im PDSG droht den Leistungserbringern ein erneuter Honorarverlust in Höhe von 1 Prozent, wenn Vorkehrungen zur ePA bis zum 30.06.2021 nicht getroffen werden. Sanktionen und Zwang sind kein adäquates Mittel um das Vertrauen der Ärzte und Psychotherapeuten in die Telematikinfrastruktur zu erhöhen.

Viele Ärzte und Psychotherapeuten, die sich lange und intensiv mit diesem Thema befasst haben, haben sich aus nachvollziehbaren Gründen und datenschutzrechtlichen Überlegungen bewusst dazu entschieden, sich unter den jetzigen Gegebenheiten nicht an die Telematikinfrastruktur anzuschließen. Die gematik ist bisher nicht ihrer aus der Datenschutz-Grundverordnung resultierenden Verpflichtung nachgekommen, die erforderliche Datenschutz-Folgenabschätzung zu beauftragen und vorzunehmen. Unter diesen Voraussetzungen ist es nur konsequent und logisch, dass Ärzte und Psychotherapeuten skeptisch gegenüber einem Anschluss an die Telematikinfrastruktur sind.

Eine sanktionsbewehrte Einführung der Telematik hingegen ist kontraproduktiv. Die verfehlte Politik der Sanktionierung sollte sich bei der Einführung der ePA nicht wiederholen.

Deswegen fordern wir:

Zwang und Sanktionierungen sind im Zusammenhang mit dem Anschluss an die TI und die Nutzung der ePA kontraproduktiv und müssen gestrichen werden. Eine nutzbringende TI, die die berechtigten Datenschutzinteressen adäquat berücksichtigt, wird von den Ärzten und Psychotherapeuten auch ohne Sanktionierungen genutzt werden. Entscheidend ist es dafür, dass die gematik unverzüglich die Datenschutz-Folgenabschätzung nach der DSGVO durchführt.

6. Elektronische Gesundheitskarte (eGK) als Authentifizierungsinstrument (§ 336 SGB V)

Hintergrund:

- Anpassungen im Kabinettsentwurf zum PDSG nicht ausreichend

Forderung:

- Sichere, d.h. eindeutige Identifizierung des Versicherten
- Begrenzung der möglichen Anzahl an PIN-Eingabeversuchen
- *Änderungsvorschlag für § 336 Abs. 5 SGB V*

Grundvoraussetzung für eine sichere Datenhaltung in der ePA ist eine elektronische Gesundheitskarte (eGK), die höchste Sicherheitsstandards erfüllt. Dazu muss gewährleistet sein, dass die eGK und die PIN für den Zugriff auf die ePA an die richtigen Personen ausgehändigt werden. Dies allerdings stellt der Gesetzentwurf der Bundesregierung nicht auf höchstem Schutzniveau sicher. Vor dem Zugriff auf Daten der ePA muss zwingend sichergestellt sein, dass die Zugangsdaten ausschließlich an die richtige Person gelangt sind.

Deswegen fordern wir:

Es ist unerlässlich, dass der Zugriff auf die ePA immer und ohne Ausnahme über eine 2-Faktor-Authentifizierung erfolgt. Dieser Authentifizierungsstandard muss unabhängig von der Art des Zugriffs und des genutzten Mediums erfolgen. Zudem müssen die Ausgabe der eGK **und** die PIN hohen Sicherheitsstandards entsprechen.

Eine große Gefahr geht von sogenannten Brute-Force-Angriffen aus, durch welche Hacker relativ problemlos Zugriff auf sensible Daten erhalten können. Mit dieser Methode werden in kürzester Zeit eine Vielzahl an verschiedenen Zeichenketten und Buchstabenfolgen wahllos und automatisiert ausprobiert, bis das Passwort letztendlich herausgefunden werden kann. Um dem vorzubeugen, muss zudem sichergestellt sein, dass die Anzahl an PIN-Eingabeversuchen begrenzt werden.

7. Evaluation der Richtlinie zum Schutz von Sozialdaten (§ 217f Abs. 4b SGB V)

Hintergrund:

- Die Anforderungen an die Evaluation der Richtlinie des Spitzenverband Bund der Krankenkassen (GKV-SV) zum Schutz von Sozialdaten sind unzureichend

Forderung:

- **Jährliche** Evaluierung und nicht lediglich im Zwei-Jahres Rhythmus
- Beauftragung eines unabhängigen und geeigneten Expertengremiums als Sicherheitsgutachter unter Beteiligung der Leistungserbringer
- **Einvernehmen**, statt Benehmen mit BfDI und BSI

Der GKV-SV ist beauftragt, eine Richtlinie zum Schutz von Sozialdaten der Versicherten zu erstellen. Durch das PDSG wird festgelegt, wie diese Richtlinie zu evaluieren ist. In Anbetracht der enormen Bedeutung des Schutzgutes der Richtlinie und der besonderen Gegebenheiten des digitalen Zeitalters sind die bisherigen Anforderungen an die Evaluation der Richtlinie nicht ausreichend.

Deswegen fordern wir:

Die Richtlinie sollte in Anbetracht der Dynamik der digitalen Veränderung jährlich, und nicht wie im Kabinettsentwurf des PDSG vorgesehen alle zwei Jahre, evaluiert werden. Außerdem ist es nicht ausreichend einen einzelnen Gutachter mit der Evaluation zu beauftragen. Es ist vielmehr dringend notwendig, dass sich eine Expertengruppe dieser komplexen Aufgabe widmet. Das Gutachten sollte durch Vertreter der Leistungserbringer mit in Auftrag gegeben werden. Darüber hinaus reicht es nicht aus, dass die Richtlinie lediglich im Benehmen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik anzupassen ist. Hier muss das Einvernehmen hergestellt werden.

unterstützt von folgenden Berufsverbänden

VPP Berufsverband Deutscher Psychologinnen und Psychologen e.V.

PK Vereinigung psychotherapeutisch und psychosomatisch tätiger Kassenärzte e.V.

bkj BERUFSVERBAND der Kinder- und Jugendlichenpsychotherapeutinnen und Kinder- und Jugendlichenpsychotherapeuten e.V.

Berufsverband Bayerischer Psychoanalytikerinnen und Psychoanalytiker BB Landesverband der DGPT Deutsche Gesellschaft für Psychoanalyse, Psychotherapie, Psychosomatik und Tiefenpsychologie e.V.

BVDP

DPtV Bayern

bvvp

bkjpp Berufsverband für Kinder- und Jugendpsychiatrie, Psychosomatik und Psychotherapie in Deutschland e. V. – Bayern –

BPM Berufsverband der Fachärzte für Psychosomatische Medizin und Psychotherapie e.V.

dgvt-BV Berufsverband Psychosoziale Berufe

SAV e.V.

Stationär-ambulanter Verbund

zur Rehabilitation Hirnverletzter

VAKJP Vereinigung Analytischer Kinder- und Jugendlichen-Psychotherapeuten in Deutschland e.V. gegr. 1953