Absender/ BSNR

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Vorab per Fax: 0511 380-4657
Vorab per E-Mail: kvn.braunschweig@KVN.de

Kassenärztliche Vereinigung Niedersachsen
Bezirksstelle Braunschweig
Postfach 2725

38017 Braunschweig

__,__,2024

Widerspruch gegen den Honorarabrechnungsbescheid des Quartals III/2023

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit haben wir Mitte Januar 2024 den Honorarabrechnungsbescheid auf dem Postweg für das oben genannte Quartal erhalten. Gegen diesen legen wir hiermit fristgerecht

Widerspruch

ein.

Der Widerspruch erfolgt zunächst zur Fristwahrung. Wir behalten uns das Recht vor, jederzeit diesen Widerspruch zu ergänzen

Der Widerspruch richtet sich gegen

Kürzungen von 2,5 % wegen der Nichtanbindung an die Telematik-Infrastruktur

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 mehrere Musterverfahren existieren.

Wir machen daher darauf aufmerksam, dass die derzeit noch bestehenden Klageverfahren der "Freien Ärzteschaft" und das des "Bündnis gegen Datenmissbrauch in der Medizin"

schwebend sind.

Die entsprechenden Aktenzeichen werden nachgereicht. Gegenstand dieser Verfahren werden zum überwiegenden Teil die auch uns betreffenden Rechts- und Sicherheitsfragen sein, sodass wir diese Widersprüche zur Wahrung unserer Rechte einlegen. Wir beantragen bis zum Abschluss dieser Musterverfahren das Ruhen dieses Widerspruchverfahrens.

Begründung:

Vorab, alle vorherigen Widersprüche werden in allen Punkten aufrecht erhalten. Dieser Widerspruch stellt eine zusätzliche Ergänzung dar und hat nicht den Anspruch der Vollständigkeit, zukünftige Ergänzungen behalten wir uns vor.

Die Honorarbescheide für das Abrechnungsquartale I+II+III+IV/2019, I+II+III+IV/2020, I+II+III+IV/2021, I+II+III+IV/2022 und I+II+III/2023 sind – soweit es den pauschalen Abzug in Höhe von 1 bzw. 2,5 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. Analog dazu betrifft dies auch die Pflicht zu Durchführung des eRezeptes und der eArbeitunfähigkeit.

Die Widerspruchsbegründungen des I.+II.+III.+IV. Quartals 2019, des I.+II.+III.+IV. Quartals 2020, des I.+II.+III.+IV. Quartals 2021 gelten in vollem Umfang auch als Widerspruch für die KVN Abrechnung des I.+II.+III.+IV. Quartals 2022 und dem I.+II.+III. Quartal 2023.

Wir stellen aktuell fest, die TI mit den erforderlichen Komponenten konnte erneut schwer kompromittiert werden. Der entstandene Schaden, kann derzeit noch nicht verifiziert werden. Weiterer Sachvortrag zu diesem Thema bleibt explizit vorbehalten.

Es bleibt an dieser Stelle vorallem auch Widerspruch gegen die ePA (Elektronische Patientenakte) in der aktuellen, geplanten Form und den damit verbundenen Vorstellungen des Gesundheitsministers Karl Lauterbach einzulegen. Deren Umsetzung führt zur unwiderruflichen Abschaffung der Ärztlichen Schweigepflicht und einem nicht reparierbaren Schaden im Vertrauensverhältnisses zwischen Patienten und Ärzten.

Allein die Annahme, dass so sensible Daten, wie die Gesundheitsdaten von Millionen von Bürgern zentral zu lagern und dann noch davon zu sprechen und zu behaupten, dass diese sicher vor dem Zugriff von Unbefugten gelagert sind, zeugt von Naivität oder grenzenloser Gier. Vorallem wenn noch im gleichen Atemzug dann Personen, Institutionen etc. mit "berechtigtem Interesse" der Zugriff auf diese Daten gewährt werden soll.

Das ist zu vergleichen mit dem Bild - "Wasch mich, aber mach mich nicht nass!"

Es gibt im Internet keine Datensicherheit!

Wenn selbst Firmen wie Facebook, Google, Nvidia, Citrix, Sony oder Microsoft zugeben müssen, dass sie gehackt worden sind. Und das tun diese Firmen nur, weil es einfach nicht zu verschweigen ist und früher oder später sowieso ans Tageslicht kommen würde.

Natürlich wird von den Betroffenen immer behauptet, dass keine "wichtigen Daten" von den Hackern ergaunert worden wären. Aber das kann tatsächlich niemand wirklich genau beweisen.

Um auf das Gesundheitssystem in Deutschland zurück zu kommen und die Datensicherheit der hiesigen Krankenkassen, so muss man die Hände über den Kopf zusammenschlagen.

Es wird seitens der Medien, der Krankenkassen und der Politik gemauert was das Zeug hält.

Streng nach dem Motto: " Es kann nicht sein, was nicht sein darf!"

Dabei sind es schwerwiegende Vorfälle von Datenlecks, die der Öffentlichkeit nicht bekannt gegeben werden. Besonders wenn man nun davon ausgeht, dass neben der Daten des VSDM auch die Daten der eAU, der eRp und später auch die der ePA auf den Servern der Krankenkassen gelagert werden sollen, bevor sie in den eHSpace geladen werden.

Und wenn man es sich genauer ansieht, dann sind einige der Lecks durch EDV Dienstleister verursacht, wie der Dienstleister "Bitmark" welche die meisten BKKs technisch betreut. So kam es allein in 2023 zweimal zu einem Hacking der BKK Server mit weitreichenden Konsequenzen. Den Patienten wurde es selbst auf direkter Nachfrage bei ihrer BKK, hier einige Fälle der AUDI BKK, selbst erlebt, nicht die Wahrheit über die "technischen Störungen" kundgetan.

Auch die AOKs hat es in 2023 erwischt. Nach dem offiziellen Wortlaut konnten die Hacker "sinngemäß" keine wichtigen Daten (?) ergaunern?

Über den Inhalt solcher Meldungen kann man nur schmunzeln, meist wissen die Gehackten erst Monate nach dem Hack, dass sie gehackt wurden. Welche Daten bis dahin wirklich abgezogen wurden bleibt in den meisten Fällen komplett unbekannt.

Bei differenzierterer, ernsthafter Betrachtung muss die Frage nach der Sicherheit der intimsten persönlichen Daten erlaubt sein.

Die Antwort auf diese Frage kennen alle in der IT-Branche Tätigen, die ihre Verantwortung ernst nehmen. Es gibt keine 100%ige Datensicherheit im Internet.

Noch einige neue Bespiele hinsichtlich gehackter Betriebe, Verwaltungen oder Krankenhäuser, um sich die daraus entstandenen, desaströsen Folgen besser vorstellen zu können.

1. Cyber-Angreifer erbeuten E-Mails aus Microsofts Cybersicherheitsabteilung

Die kriminelle Gruppe Midnight Blizzard hat sich Zugang zu E-Mails von Microsoft-Mitarbeitern verschafft. Sie wollte wohl wissen, was Microsoft über sie weiß.

https://www.heise.de/news/Cyber-Angreifer-erbeuten-E-Mails-von-Microsoft-Mitarbeitern-9603710.html/

2. Europa - Virus im Covid-Testlabor

1,3 Millionen-Datensatzdatenbank des niederländischen COVID-19-Testlabors online ausgestellt
Eine Datenbank von Coronalab, einem COVID-19-Testlabor in den Niederlanden, wurde online offengelegt. Die Datenbank enthielt 1,3 Millionen Datensätze, darunter Testergebnisse, Namen, Geburtsdaten und Passnummern.

https://www.hipaajournal.com/1-3-million-record-database-netherlands-covid-19-testing-lab-exposed/

3. Netzwerkausfall an der Unimedizin in Mainz

An der Mainzer Universitätsmedizin funktionieren seit Freitagmorgen sämtliche Netzwerke nicht mehr - mit Folgen für Patientinnen und Patienten. Ein **Hackerangriff** ist es wohl nicht. (Redaktionelle Anmerkung: Was denn sonst!)

https://www.swr.de/swraktuell/rheinland-pfalz/mainz/netzwerkausfall-an-der-unimedizin-in-mainz-100.html

4. tagesspiegel.de

Hacker-Angriff auf Berliner Krankenhaus: Rettungsstelle in Reinickendorf abgemeldet
Die Caritas-Klinik Dominikus in Berlin-Hermsdorf ist Opfer eines **Hackerangriffes** geworden. Laut dem Betreiber läuft der Betrieb weitgehend normal weiter – bis auf die Notfallversorgung

https://www.tagesspiegel.de/berlin/berliner-wirtschaft/hacker-angriff-auf-berliner-krankenhaus-rettungsstelle-in-reinickendorf-abgemeldet-11146267.html

5. Hackerangriff auf die Bezirkskliniken Mittelfranken 30.01.2024 12:59 - Ärzte Zeitung

Die Bezirkskliniken Mittelfranken haben einen **Hackerangriff** gemeldet. Nach der Attacke auf die IT-Infrastruktur haben Angreifer wohl versucht, Kontakt mit dem bayerischen Klinikverbund aufzunehmen.

https://www.aerztezeitung.de/Wirtschaft/Hackerangriff-auf-die-Bezirkskliniken-Mittelfranken-446663.html

02.02.2024, 12:00 Uhr - Ärzte Zeitung
https://www.aerztezeitung.de/Wirtschaft/Hackerangriff-Kliniken-gehen-auf-Erpressungsversuch-nicht-ein-446816.html

6. Hackerangriffe auf Kliniken: 'Nur eine Frage der Zeit' 29.01.2024 10:11 - tagesschau.de

Krankenhäuser und Pflegeeinrichtungen werden immer häufiger zum Ziel von Cyberattacken. Ein großflächiger Angriff mit vielen Ausfällen ist ein denkbares Szenario.

Hackerangriffe auf *Kliniken* "*Nur* eine *Frage* der *Zeit*" ; Cyberangriffe auf IT-Dienstleister Finanzaufsicht warnt vor "virtuellem Bankraub".

https://www.tagesschau.de/inland/gesellschaft/cybersicherheit-krankenhaeuser-100.html

7. Auch aus Security-Sicht gibt es wenig Liebe für das E-Rezept

Kommentar: Sehr geehrter Herr Adler, sehr geehrte Kolleginnen und Kollegen,

Heise-Kommentatorin zur nicht-gewollten(?) Sicherheit in der Gesundheits-IT:

"Daten sammeln für … ja, für was eigentlich? Die primäre Zielsetzung ist hier ganz klar eine andere als der Datenschutz: die Vernetzung aller Informationen, um einen nicht näher definierten Mehrwert in der Forschung zu erreichen. Grundsätzlich ist es natürlich lobenswert, den medizinischen Fortschritt zu unterstützen. Bei den gesammelten medizinischen Daten eines Landes jedoch, sollte man meinen, wäre ein grundlegendes Konzept zur IT-Sicherheit drin gewesen. Das hat man sich – wohl aus gutem Grund – gescheut mitzuliefern. Das Frustrierende: Es wäre ja nicht einmal unbedingt technisch kompliziert gewesen. Die Daten könnten lokal je nach Anwendungsfall anonymisiert oder pseudonymisiert und auf jeden Fall verschlüsselt werden, bevor sie in die Cloud geschickt werden. Patientinnen und Patienten könnten ausgewählte Befunde gesondert verschlüsseln und den jeweiligen Ärztinnen und Ärzten wiederum einen Schlüssel für den Zugriff mitteilen – ob analog zum Beispiel über einen QR-Code oder über einen verschlüsselnden Messenger. Für die Forschung könnten Informationen ebenfalls von den Patienten freigegeben werden – als freiwillige Datenspende. Sicherlich, einen umfassenden Data Lake über die gesundheitlichen Probleme und Risiken ganz Deutschlands ohne Einwilligung der Betroffenen wird man so nicht erreichen, aber vielleicht ist das ganz gut so. Denn immerhin könnten nach längeren, erfolgreichen Tests des Systems, wenn bewiesen ist, dass nicht massenhaft Daten abhanden und in falsche Hände gekommen sind, schrittweise weitere Informationen geteilt oder der Opt-in weiter erleichtert werden. Hingegen alles auf die Karte "Wird schon gut gehen" zu setzen darf genau nullmal schiefgehen. Dafür sind wir nach aller Erfahrung der letzten Jahre noch nicht bereit."

Das Original:

Kommentar: Auch aus Security-Sicht gibt es wenig Liebe für das E-Rezept

Digitalisierung ja – aber nicht um den Preis einer gigantischen, dazu höchstwahrscheinlich schlecht gesicherten Datenzusammenführung, meint unsere Kolumnistin.

21.01.2024 07:16 Uhr - iX Magazin - Von Janis König

Ei, ei, ei, was seh ich da: Deutschland digitalisiert endlich!? Der Arztbesuch soll jetzt bequemer vonstattengehen, das E-Rezept beim Gang zur Apotheke Papier sparen? Wow! Geschehen etwa doch noch binäre Zeichen und digitale Wunder im Land der Faxe und blauen Passierscheine? Zu schön, um wahr zu sein.

Ganz so glatt läuft es natürlich nicht: Die AG Kritis, der Chaos Computer Club, das Zentrum für digitalen Fortschritt D64 e. V., der Verein Digitale Gesellschaft … – die Liste der Unterzeichnenden des offenen Briefes gegen das "Gesundheitsdatennutzungsgesetz" (GDNG) ist lang. Viele der Protestierenden kommen zwar aus dem Lager der häufig Nörgelnden, aber nicht unbedingt aus der Schublade der prinzipiell elektronisch Abgeneigten. Ihre Kritik ist ganz klar NICHT, dass sie einer Digitalisierung des Gesundheitssystems grundsätzlich immer entgegenständen: An der Ausformulierung und wahrscheinlich zu Recht befürchteten Umsetzung des Gesetzes hapert es aber nach Ansicht der Kritisierenden dafür umso mehr.

Vor allem schweigt sich der Gesetzesbeschluss darüber aus, wie genau die Sicherheit der Daten gewährleistet werden soll – "Confidential Computing" soll es im Wesentlichen richten, also eine aktuell wild beforschte Disziplin der Informatik, die erst in wenigen Anwendungsfällen langfristig ausgetestet wurde, und auch das noch nicht einmal im großen Maßstab. Es fehlte gerade noch der Verweis auf vollhorstomorphe Verschlüsselung auf der Quantenblockchain.

Daten sammeln für … ja, für was eigentlich?

Die primäre Zielsetzung ist hier ganz klar eine andere als der Datenschutz: die Vernetzung aller Informationen, um einen nicht näher definierten Mehrwert in der Forschung zu erreichen. Grundsätzlich ist es natürlich lobenswert, den medizinischen Fortschritt zu unterstützen. Bei den gesammelten medizinischen Daten eines Landes jedoch, sollte man meinen, wäre ein grundlegendes Konzept zur IT-Sicherheit drin gewesen. Das hat man sich – wohl aus gutem Grund – gescheut mitzuliefern.

Das Frustrierende: Es wäre ja nicht einmal unbedingt technisch kompliziert gewesen. Die Daten könnten lokal je nach Anwendungsfall anonymisiert oder pseudonymisiert und auf jeden Fall verschlüsselt werden, bevor sie in die Cloud geschickt werden. Patientinnen und Patienten könnten ausgewählte Befunde gesondert

verschlüsseln und den jeweiligen Ärztinnen und Ärzten wiederum einen Schlüssel für den Zugriff mitteilen – ob analog zum Beispiel über einen QR-Code oder über einen verschlüsselnden Messenger.

Für die Forschung könnten Informationen ebenfalls von den Patienten freigegeben werden – als freiwillige Datenspende. Sicherlich, einen umfassenden Data Lake über die gesundheitlichen Probleme und Risiken ganz Deutschlands ohne Einwilligung der Betroffenen wird man so nicht erreichen, aber vielleicht ist das ganz gut so. Denn immerhin könnten nach längeren, erfolgreichen Tests des Systems, wenn bewiesen ist, dass nicht massenhaft Daten abhanden und in falsche Hände gekommen sind, schrittweise weitere Informationen geteilt oder der Opt-in weiter erleichtert werden. Hingegen alles auf die Karte "Wird schon gut gehen" zu setzen darf genau nullmal schiefgehen. Dafür sind wir nach aller Erfahrung der letzten Jahre noch nicht bereit.

https://www.heise.de/meinung/Kommentar-elektronische-Patientenakte-ist-gut-fehlende-Datensicherheit-nicht-9602148.html

8. Datenlecks international

Europa holt auf: 33 Millionen Patientendaten gehackt
Paris – Mehr als 33 Millionen Menschen in Frankreich sind von einer Hackingattacke gegen zwei Dienstleister des Krankenversicherungswesens betroffen. Dabei gehe es um Name und Geburtsdatum, die Sozialversicherungsnummer sowie den Namen der gewählten Zusatzkrankenversicherung, teilte die Datenschutzbehörde CNIL mit. Weiterführende Informationen wie Kontodaten, Adressen oder medizinische Daten seien allerdings nicht in die Hände von Unbefugten gelangt. Die beiden Dienstleister hatten die Behörde über die Attacke vom Januar informiert. Die Krankenversicherungen, die mit den Dienstleistern zusammenarbeiteten, müssten betroffene Versicherte darüber informieren. Die Datenschutzbehörde rief die betroffenen Menschen zur Vorsicht bei allen Krankenversicherungsangelegenheiten auf. Außerdem sollten sie ihre Bankkonten im Blick behalten, denn möglich sei, dass Unbefugte die erlangten Daten mit weiteren Informationen kombinierten, die bei anderen Hacking-Attacken erlangt wurden."
Kommentar: Nun fehlen leider die Zahlen der -wie viele waren es noch- gehackten Krankenhäuser in Deutschland. Die Daten der Cafeteria wurden sicher nicht gestohlen.
Aber vielleicht ist das auch deutsche Bescheidenheit: man will nicht mit den Daten protzen.

Trotzdem "Chapeau!" an die französischen Hacker.

Das Jahr ist gerade 6 Wochen alt und schon werden alte Rekorde gebrochen.
Im Hackerwettcup zwischen den USA und Europa steht es kann 36 Millionen zu 33 Millionen.

Es wird spannend. Vor allem, wenn jetzt 73 Millionen elektronische Patientenakten bei uns hinzu kommen!

https://www.aerzteblatt.de/nachrichten/149181/Frankreich-Hackerangriff-auf-Gesundheitsdienstleister

Vereinigte Staaten der Datenlecks (USA) - 29% der Hackingopfer zahlen Lösegeld
Sicherheitsverletzungen im Gesundheitswesen im Jahr 2023
Sicherheitsverletzungen im Gesundheitswesen werden mit einer Rate von 2 pro Tag gemeldet. Im Jahr 2023 wurden 725 große Verstöße gemeldet und mehr als 133 Millionen Datensätze wurden aufgedeckt, als Hacking-Vorfälle ein Rekordhoch erreichten.
Kommentar: Da wurden einige Ransomangriffe bei der Zählung ausgelassen, die zahlen haben sich nach unseren Recherchen auf über 200 Millionen erhöht.

71% der Opfer von Ransomware-Angriffen weigern sich, das Lösegeld zu zahlen
Der Prozentsatz der Opfer von Ransomware-Angriffen, die ein Lösegeld zahlen, ist auf ein Rekordtief gesunken, von 85 % der Opfer im Jahr 2019 auf nur 29 % im 4. Quartal 2023.
Kommentar: Da werden sich wohl die Hackingzahlen erhöhen

Concentra bestätigt, dass fast 4 Millionen Patienten von einer PJ&A-Datenverletzung betroffen sind
Concentra, ein in Texas ansässiger Anbieter für körperliche und berufliche Gesundheit, hat bestätigt, dass die Daten von fast 4 Millionen Patienten bei der PJ&A-Datenverletzung kompromittiert wurde, wodurch sich die Gesamtzahl der betroffenen Personen auf 14 Millionen erhöht.

Die Datenverletzung Von Keenan & Associates Betrifft Mehr Als 1,5 Millionen Personen
Der in Torrance, CA, ansässige Versicherungsmakler Keenan & Associates hat kürzlich dem Generalstaatsanwalt von Maine einen Cybersicherheitsvorfall gemeldet, von dem 1.509.616 Personen betroffen war.

Plaza Radiology Datenverletzung betrifft bis zu 569.000 Patienten
Plaza Radiology, das als Chattanooga Imaging in Tennessee und North Georgia tätig ist, hat einen Cyberangriff und eine Datenschutzverletzung erlitten, von der 569.000 Patienten betroffen sind.

LockBit Ransomware Gang übernimmt die Verantwortung für den Angriff auf das Saint Anthony Hospital
Die LockBit-Ransomware-Gang hat das Saint Anthony Hospital in Chicago zu ihrer Datenleck-Website hinzugefügt und fordert eine Lösegeldzahlung von fast 900.000 Dollar vom gemeinnützigen Krankenhaus, um die Freigabe der gestohlenen Daten zu verhindern.

314.000 Patienten, die von Cyberangriff auf das CompleteCare Health Network betroffen sind
Das CompleteCare Health Network in New Jersey hat bestätigt, dass die geschützten Gesundheitsinformationen von 313.973 Patienten bei einem Cyberangriff im Oktober 2023 kompromittiert wurden.
Antwort: Aktueller Stand: 36 Millionen Patientenakten gehackt (im ersten Monat 2024 28 Millionen)
Wenn der Trend sich so hält, könnte dieses Jahr alle Rekorde brechen: 456 Millionen.
Wir drücken wie immer die Daumen.

Mussi denn, mussi denn ins Krankenhaus hinein - Einfältigkeit schlägt Dreifaltigkeit
... wenn I wieder wieder komm sind die Daten weg

Nach dem Hackerangriff auf das Dreifaltigkeits-Hospital in Lippstadt und die Krankenhäuser in Erwitte und Geseke wird weiter ermittelt. Wann der Krankenhaus-Alltag wieder nach Plan läuft, ist unklar.
Weite Teile des Computersystems liegen lahm. Neue Patienten können zur Zeit nicht aufgenommen werden, Operationen werden verschoben.
Nach ersten Erkenntnissen sind laut Polizei aber keine Bereiche betroffen, die die Versorgung der Patienten auf den Stationen gefährden. "Durch den Angriff besteht keine Gefahr für Leib oder Leben der derzeit im Krankenhaus befindlichen Patientinnen und Patienten, deren stationäre Versorgung gewährleistet ist", betonten die Behörden. Weitere Angaben könne man zunächst nicht machen.

Ermittlungen laufen
Wie die Dortmunder Polizei und die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) bei der Kölner Staatsanwaltschaft berichten, seien die Ermittlungen zur genauen Ursache und zum Ausmaß der Störung in vollem Gange. Von wem die drei Krankenhäuser gehackt wurden, ist nicht bekannt. Experten machten sich derzeit ein Bild vom Schadensausmaß des Angriffs, sagte Staatsanwältin Gianna Maria Graf am Samstag in Köln.
Ermittelt werde, was genau passiert sei und wie die Täter vorgegangen seien. Die Experten wollen auch herausfinden, ob der Angriff einer bereits bekannten Tätergruppierung zugeschrieben werden kann.

9. Petition gegen Handel mit Patientendaten

Die europäischen Staats- und Regierungschefs im Rat der Europäischen Union und Abgeordnete des Europäischen Parlaments

APPELL
Wir wollen das Recht auf Vertraulichkeit in Bezug auf unsere Krankenakten. Das bedeutet: Wie haben die Kontrolle über unsere persönlichen Gesundheitsdaten und darüber, wer Zugang zu ihnen hat und zu welchem Zweck.
Wir fordern Sie auf, den Europäische Raum für Gesundheitsdaten wie folgt zu ändern:
- die ausdrückliche Zustimmung der Patienten und Patientinnen ist erforderlich zur Weitergabe von Patientenakten für Zwecke, die nicht direkt mit der Behandlung zusammenhängen (auch bekannt als Sekundärnutzung)
- Begrenzung der umfangreichen Kategorien von "Gesundheitsdaten"

• Einschränkungen, wie diese Informationen verwendet werden können und wer Zugang zu ihnen hat.

Warum das wichtig ist

Die EU-Kommission denkt darüber nach, Unternehmen den Zugang zu unseren vertraulichen Patientenakten zu gewähren! Ein neues Gesetz sieht vor, den Austausch von Patientenakten und Informationen zu vereinfachen. So soll es zum Beispiel einfacher werden, eine MRT-Aufnahme von einer Urlaubsverletzung mit dem Hausarzt zu teilen. Aber als Teil desselben Gesetzes plant die EU, das Recht auf Datenschutz zu beeinträchtigen und das Vertrauen in unsere Ärzt*innen zu untergraben.

In der jetzigen Fassung würde das neue Gesetz Gesundheitsdienstleister dazu drängen, sensible Gesundheitsdaten an so ziemlich jeden weiterzugeben, der sie für "Forschungszwecke" benötigt. Dazu gehören Big Pharma, Big Tech und Versicherungsunternehmen. Noch schlimmer ist, dass sie für den Zugriff auf unsere Daten keine Erlaubnis benötigen und uns nicht über die Verwendung der Daten informieren müssen.

https://action.wemove.eu/sign/2023-05-european-health-data-space-petition-DE

Die Einführung der "EPA = Abschaffung der Ärztlichen Schweigepflicht"

Uns bleibt es ein Rätsel, warum Politiker sich nicht um die realen Probleme im Gesundheitwesen kümmern, sondern nun mittlerweile Milliarden von Versichertengeldern einer unausgegorenen Idee hinterherwerfen.

An dieser Stelle erlaube ich mir eine klare Forderung an die Politik, lernen Sie erst einmal, was es mit dem Wort "WANZ" auf sich hat, bevor Sie weiter die dringend benötigten Versicherungsgelder einer schier nimmer satten Computer- und Software-Industrie hinterher schmeißen.

Weiterer Sachvortrag bleibt explizit vorbehalten.

Bestätigen Sie uns bitte den Erhalt dieses Widerspruchs für das III. Quartal 2023 schriftlich.

Mit freundlichen Grüßen

Name/Stempel/Unterschrift