



AUSGABE 4/2021

PRAXIS-NEWSLETTER FÜR ALLE PEGAMED-ANWENDER

HRSGBR. BASTIAN KELLNER – JOSEF-ADLER-STR. 8 – 93049 REGENSBURG

LIEBE PEGAMED-ANWENDER/INNEN,

heute erhalten Sie unseren letzten Newsletter für dieses Jahr mit aktuellen Informationen rund um PegaMed und EDV. Sie können **alle Ausgaben** des Newsletters auch aus unserem **Archiv unter www.bytekontrol.de** herunterladen.

EAU, KIM, EHBA

Die meisten von Ihnen sind schon in das „Vergnügen“ der Digitalisierungsbemühungen vorgedrungen und haben Ihre ersten Erfahrungen gemacht. Als Zwischenbericht können wir folgendes aus unserem Blickwinkel mitteilen:

- der Weg zur eAU ist lang und steinig
- es gibt viele technischen Hürden außerhalb von PegaMed
- leider sind sehr häufig fremde Ansprechpartner involviert und die Absprache läuft nur suboptimal

Denn für die TI, den TI-Dienstleister, den Herausgeber des eHBA, die Lesegeräte, den KIM-Anbieter usw. sind wir in erster Linie gar nicht verantwortlich. Deswegen sind uns oft die Hände gebunden und wir müssen Sie leider wieder an diese externen Firmen verweisen. Teilweise fehlen **Lizenzierungen** oder **bestimmte Einstellungen im Konnektor**, manchmal ist der eHBA gar nicht **Komfortsignatur-fähig**. So manche Fernwartungen mit externen Firmen laufen nach dem Motto „Jugend forscht“, wie Sie z.T. selbst schon miterleben konnten.

Allerdings scheitert es oft auch an nicht vorhandenen **Passwörtern/PINs**. Deswegen möchten wir nochmal an Sie appellieren, solche Dinge ordentlich, aber vor unbefugtem Zugriff geschützt, zu dokumentieren (genaue Bezeichnung, Benutzername, Passwort, PIN, Datum wann festgelegt/geändert etc.) und bereitzuhalten.

Trotz allem: ist wenigstens KIM funktionsfähig, wird es von zahlreichen Praxen bereits intensiv für den Empfang und Versand von Arztbriefen genutzt. Dabei zeigt sich, dass **KIM dem klassischen Fax haushoch überlegen** ist!

- Briefe werden **bekanntem Patient:innen automatisch zugeordnet**. Bei unbekanntem sind sie leicht per Rechtsklick zuzuordnen
- Briefe kommen in **besten Qualität**, teils in Farbe mit Logos, Befund-Bilder aus z.B. Gastro-/Endoskopie oder Ultraschall an
- Der Versand geht ruckzuck und wird – sofern mit eHBA signiert – auch vergütet

Sollten Sie bis jetzt noch keine KIM-Adresse registriert haben, so tun Sie das bitte baldmöglichst. Wir empfehlen nach wie vor kv.dox von der KBV.

Sollten Sie noch keinen eHBA haben, so kümmern Sie sich bitte auch darum! Dieser muss meistens im Online-Portal des Herstellers noch aktiviert werden und die Transport-PINs (welche Ihnen in einem Extra-Brief zugesandt werden) müssen in eigene PINs geändert werden (geht im PegaMed).

Auch wenn die Fristen für den Einsatz der eAU und des eRezepts wieder einmal aufgeschoben wurden (bis 30.06.22): es ist nicht „eEgal“! **“Es müssen die technischen Voraussetzungen in den Praxen geschaffen werden”** – so Dr. Kriedel, Vorstandsmitglied der KBV. Und wir empfehlen, frühzeitig vor Ablauf von Übergangsfristen alles in die Wege zu leiten.

Übrigens: im Zuge dieser ganzen Komplikationen welche aus der „Verantwortungsdiffusion“ entstehen, erwacht sehr häufig der Wunsch seitens der Praxen, endlich „einen“ Ansprechpartner „für alles“ zu haben. Dies ist aus verschiedensten Gründen leider nicht ohne Weiteres möglich. Allein für die TI haben alle Praxen üblicherweise 5-Jahres-Verträge geschlossen und werden darum von TI-Firmen betreut, welche direkte Konkurrenz zu PegaMed darstellen (oft die Betreuer des Vorgängerprogramms, von welchem gewechselt wurde). Und selbst wenn jemand verspricht, wirklich „alles“ zu machen: auch in jener Firma gibt es oft wieder Subunternehmer oder Mitarbeiter für Spezialgebiete wie z.B. Telefonanlagen, Zeiterfassung, Praxissoftware, TI usw. Ist jemand krank oder im Urlaub, wissen die Kolleg:innen oftmals auch nicht weiter. IT ist umfangreich, IT ist komplex – niemand kann alles wissen.

An dieser Stelle noch ein Wort zum eHBA und der “Qualifizierten elektronischen Signatur” QES:

Die QES ist gleichbedeutend mit der Unterschrift der ÄrztInnen. Darum darf nur der Arzt bzw. die Ärztin **persönlich** die PIN des eHBA wissen und am Lesegerät eingeben. Ebenso das Passwort der Komfortsignatur (Eingabe im PegaMed statt am Kartenleser). Auf die **Vertraulichkeit dieser PINs** werden Sie bei der Bestellung und bei Erhalt des eHBA hingewiesen. Es darf daher eigentlich nicht sein, dass uns z.B. Auszubildende am Telefon die PIN durchsagen und vom Chef bzw. der Chefin mit der Einrichtung des eHBA betraut wurden! Als Arzt/Ärztin haften Sie vollumfänglich für die Signatur! Und auch die Mitarbeiterin, die mit dem eHBA und dessen PIN signiert begeht Unterschriftenfälschung!

Wir wissen, dass das neue Vorgehen erstmal ungewohnt ist. Aber es gibt mehrere Möglichkeiten, die neuen Vorgaben in die Praxis umzusetzen. Überlegen Sie sich, was für Sie am praktikabelsten ist:

Entweder Sie als Arzt oder Ärztin erstellen die eAU (und später das eRezept) selbst. Dann können Sie bei der Signaturabfrage **direkt signieren** (am besten mit Komfortsignatur oder per PIN-Eingabe an einem Kartenleser im Sprechzimmer). Der Versand an die Krankenkasse erfolgt dann sofort im Anschluss. Die Exemplare für die Arbeitgeber und die Patient:innen werden vorerst noch weiter gedruckt, d.h. dort müssen Sie auch weiterhin händisch unterschreiben.

Wenn die MFAs die eAUs schon vorab ausstellen möchten, müssen diese bei der Signaturabfrage auf „Abbruch“ gehen. So werden die Exemplare für Arbeitgeber und Patient:in bereits ausgedruckt. Sie als Arzt bzw. Ärztin müssen dann **nachträglich signieren** und versenden. Sie können alle ausgestellten eAUs nochmal aufrufen über Praxis – Allgemeine Dokumente – eAU. Dort können Sie auch mehrere eAUs markieren und klicken zum Signieren und Verschicken oben auf das Briefsymbol. Einziges Problem dabei ist, dass die Patient:innen dann u.U. schon weg sind. Wenn nun ein Problem beim Versand auftritt, müssen Sie die eAU ausdrucken und per Post an die Krankenkasse schicken (oder die Patient:innen nochmal einbestellen, damit diese das selbst erledigen).

Soweit die Theorie. In wieweit die Übermittlung an die Krankenkassen tatsächlich reibungslos klappt, dazu erreichen uns unterschiedliche Rückmeldungen. Auch der Versand von Arztbriefen per KIM verläuft nicht immer erfolgreich, was verschiedene Ursachen haben kann. Derzeit befinden sich alle Beteiligten in der Erprobungsphase.

NEUE KV-SICHERHEITSRICHTLINIE, LOG4J, MEDATIXX-„HACK“

Täglich erreichen uns Nachfragen zu einem Schreiben der KVB bzgl. der neuen Sicherheitsrichtlinie. Hier möchten wir ganz kurz unsere persönliche Meinung wiedergeben: solange die KBV nicht exakt definiert, um welche Geräte oder Programme es sich handelt, erfüllen Sie die Formalien auf dem Papier. Jede Fritzbox, jeder Telekom-Router verfügt laut Hersteller über eine integrierte **Firewall**. Solange die Art der Firewall, die Ausprägung, technische Merkmale usw. nicht definiert werden, genügt uns das. Wir schützen Sie mit unserem **Panda AD360** (die meisten Kunden sind umgestellt auf den „grauen“ Pandakopf, einige wenige folgen demnächst). Dieser enthält auch eine „Application Layer Firewall“, welche bereits direkt auf dem PC und nicht erst im Netzwerk greift. Damit sind Sie m.M.n. besser geschützt, als in der Sicherheitsrichtlinie gefordert.

Gleichwohl gibt es Kolleg:innen, die komplexe Appliances, Hardwarefirewalls etc. in die Praxen stellen. Hier werden schnell 150,- und mehr pro Monat fällig (Angebote liegen uns und Ihnen vereinzelt vor). Wenn diese Geräte/Softwares allerdings nicht adäquat eingestellt und regelmäßig gewartet werden (und da haben wir in letzter Zeit so einige Negativbeispiele zu Gesicht bekommen), erfüllen sie nicht ihren Zweck. Und selbst dann: 100% Sicherheit wird es nie geben! Viel wichtiger ist, dass alle Praxismitarbeiter:innen sich der Gefahren bewusst sind, die bspw. von Emailanhängen fragwürdiger Absender ausgehen (s.u.).

Sie haben bestimmt auch aus den Medien von der gravierenden Schwachstelle **Log4J** gehört, welche weltweit in verschiedenster Software enthalten sein kann. Auch die Prüfmodule der KBV nutzen Log4J zur Protokollierung bei der Abrechnung. Hierbei ist es aber wichtig, nicht in Panik zu verfallen - es gab übereifrige IT-Betreuer, die die Prüfmodule gleich mal gelöscht haben! Die KBV hat bereits mit einem Update für die kommenden Prüfmodule reagiert, welches von PegaMed selbstverständlich ausgeliefert werden muss (wie vor jeder Quartalsabrechnung). **Ganz wichtig:** das Prüfmodul ist ja nicht einmal vom Internet, also von außen, erreichbar und stellt deshalb absolut keine Gefahr dar. Ja, jemand kann von innerhalb des Praxisnetzwerkes theoretisch darauf zugreifen. Dann ist der „Angreifer“ aber bereits drinnen und Sie haben ganz andere Probleme als ein **Log4J**.

Kritisch anzusehen sind alle sogenannten „Dienste“, welche vom Internet erreichbar sind und z.B. mit Handy-Apps aufgerufen werden können: Kameras, Heizungssteuerung, Smarte Türklingeln, Waschmaschinen und Staubsaugerroboter usw. Alles Geräte, welche mit der Praxissoftware bzw. dem Praxisnetzwerk nichts zu tun haben (sollten). Alle diese Geräte müssen geupdatet werden!

Auch die gesamte **Telematik-Infrastruktur** war **zeitweilig betroffen**, konnte jedoch sehr schnell geupdatet und wieder in Betrieb genommen werden. Auch hier gilt: Sinn der TI ist, dass die neuralgischen Dienste wie Chipkarten-Daten, KIM, Impfausweise usw. eben **nicht direkt vom Internet erreichbar** sind, sondern nur innerhalb der TI.

Dass wirklich niemand sicher ist, zeigt auch der „**Hack**“ der **medatixx AG**, unserem Mitbewerber. Die Kolleg:innen haben sich einen **Krypto-Trojaner** eingefangen, welcher alle Daten verschlüsselt hat und eine Lösegeldforderung nach sich zog. Wir kennen keine Details, aber üblicherweise ist das Einfallstor eine Email mit einer Aufforderung, irgendetwas anzuklicken, wie z.B. „Ihr Paket ist da, hier Sendungsverfolgung“ oder direkt mit der Schadsoftware im Anhang in Form einer Bewerbung o.ä. Darum fällt es mir so schwer, von „Hack“ zu sprechen, denn das ist eigentlich kein Hack, sondern das Ausnutzen der **ältesten Schwachstelle der Geschichte: des Menschen**. Sicherlich hat sich die medatixx auch mit Firewalls und Antivirensoftware geschützt und trotzdem kam es zum IT-Supergau. Laut den offiziellen Informationen wurden sämtliche Server, Systeme und PCs heruntergefahren, da sie als kompromittiert angesehen werden mussten. Das hatte zur Folge: keine und dann nur eingeschränkte Erreichbarkeit der Hotline, keine Updates für die Software in den Praxen, Störungen bei diversen Onlinediensten wie Terminvergabe oder auch dem bloßen Starten der Software in den Praxen....

NOTFALLDATENSATZ NFDN UND VERGÜTUNGSMÖGLICHKEIT

Da sich jetzt viele Praxen mit den einzelnen Funktionen des eHBA auseinandersetzen, möchten wir auch noch auf das (bereits seit langem) enthaltene Notfalldatenmanagement hinweisen. Innerhalb der **Karteikarte** können Sie über den Punkt „**Telematik**“ das NFDN aufrufen, die Bearbeitung aktivieren, das Patienteneinverständnis vermerken und z.B. die Nummer einer/s Angehörigen oder auch ein Dauermedikament hinterlegen. Hierfür gibt es ca. 8,70 €, die Abrechnung erfolgt nach Abrechnungsvorschlag, sobald Sie die Daten auf die eGK speichern. Hiefür ist in den meisten Fällen **keine PIN** seitens der Patient:innen notwendig, - werksseitig ist jedenfalls auf der eGK die PIN für Arztzugriffe deaktiviert. Sie als Arzt müssen mittels Ihres eHBA und Komfortsignatur das Beschreiben der Karte „absegnen“. Idealerweise haben Sie einen Chipkartenleser im Sprechzimmer für diesen Vorgang. Eine Anleitung hierzu gibt es auch unter Hilfe – PegaMed – Telematikinfrastruktur (S. 11-13).

EINLESEN MITGEBRACHTER BMP-VERORDNUNGSPLÄNE

Aus aktuellen Anlass wollen wir nochmal an die Möglichkeit erinnern, mitgebrachte Verordnungspläne mittels des aufgedruckten Matrix-Codes per Handscanner einzulesen. Damit entfällt das Abtippen der Medikation in den PegaMed-eigenen Medikamentenplan. Derlei Handscanner gibt es für wenig Geld, aber **Achtung:** nach Kauf müssen diese erst auf den Verwendungszweck „BMP“ programmiert werden! D.h. frisch aus der Packung funktionieren die meisten Scanner nicht! Gerne schicken wir Ihnen einen geeigneten Scanner zu. Derzeit prüfen wir verschiedene Modelle und können darum noch keine Preise nennen. Wir gehen aber von unter 100,- € aus.

So, viel Text ohne Bilder diesmal. Wir hoffen, Ihnen raucht nun nicht noch mehr der Kopf als sowieso schon. Falls doch: glauben Sie's uns, uns geht es nicht anders. Alles zum eRezept, das ab 01.01.2022 eingeführt wird, folgt im nächsten Newsletter bzw. im Neuerungsschreiben zum PegaMed-Quartalsupdate.

Für Fragen, Anregungen oder Kritik rufen Sie uns gern an oder senden Sie uns eine Email an buero@bytekontrol.de. Vielen Dank.

Nach diesem für Sie und uns alle erneut sehr anstrengenden Jahr wünschen wir Ihnen nun eine schöne Advents- und Weihnachtszeit, erholsame Feiertage und einen guten Jahreswechsel. Und vor allem kommen Sie gesund durch diesen Winter!

Mit den besten Grüßen aus Regensburg

Bastian und Magdalena Kellner

Rechtliche Hinweise: die in diesem Newsletter dargestellten Tipps, Tricks, Produkte und Meinungen spiegeln allein die Meinung des Herausgebers wieder und nicht die der Firma Pega Elektronik GmbH bzw. deren Mitarbeiter. Sollten wir Sie mit der Art des Newsletters, der Übermittlungsform oder der darin enthaltenen Beiträge verärgern, so teilen Sie uns dies bitte umgehend mit. Die aufgezeigten Tricks und ggf. Veränderungen an Ihrem PegaMed oder Betriebssystem erfolgen auf eigene Gefahr. Wir empfehlen eine Datensicherung vor allen Änderungen. Bei Unsicherheiten dürfen Sie uns jederzeit vorab konsultieren.



So erreichen Sie uns

ByteKontrol
Bastian Kellner
Josef-Adler-Str. 8
93049 Regensburg
0941/78036544
buero@bytekontrol.de
www.bytekontrol.de
www.pegamed.de