vision

CGM CompuGroup Medical

DAS MAGAZIN DER
CGM DEUTSCHLAND AG
NOVEMBER 2022

Editorial

„Niemand soll leiden oder sterben, nur weil einmal irgendwann, irgendwo eine medizinische Information fehlt.“

Frank Gotthardt, Gründer CompuGroup Medical

Liebe Leserinnen, liebe Leser!

wir haben es uns zur Aufgabe gemacht, medizinische Informationen für unsere Anwenderinnen und Anwender so einfach und effizient wie möglich nutzbar zu machen. Wir wollen dafür sorgen, dass Sie sich auf den Kern Ihres Berufes konzentrieren können: Menschen zu helfen und Menschen zu heilen.

Mit einer intelligenten IT möchten wir Brücken bauen zwischen Ärztinnen bzw. Ärzten, Apotheken, Kostenträgern, Laboren, Reha-Einrichtungen und Kliniken. Informationen rund um die Gesundheit sollen überall und schnellstmöglich abrufbar sein, um Pflege und Heilung voranzutreiben und mehr Zeit für das Wesentliche zu gewinnen: die Patientin bzw. den Patienten. Erst der zeitnahe und kontinuierliche Austausch zwischen allen, „die Gesundheit machen“, bringt uns dem medizinischen Fortschritt näher. Das ist unsere Aufgabe und Vision zugleich – in einer Zukunft, die mit all ihren digitalen Ausprägungen längst begonnen hat.

IT-Herausforderungen sollten nicht Ihre Aufgabe sein. In diesem Thema wollen wir der Partner sein, dem Sie vertrauen können. Mir ist es ein persönliches Anliegen, dass Sie in uns den vertrauensvollen und engagierten IT-Partner finden, der Ihnen den Rücken freihält.

Herzlichst,

Ihre Angela Mazza Teufer
Geschäftsführende Direktorin
Arztinformationssysteme & Telematikinfrastruktur

Inhalt.

04 | Digitale Patientenreise mit dem E-Rezept

Das E-Rezept bringt etliche Vorteile mit sich: für Patientinnen und Patienten, aber auch für die Arztpraxen. CLICKDOC ist der starke Partner bei allen Schritten der Patient Journey.

08 | Die TI erneuert sich So einfach geht´s:

Kundinnen und Kunden bekommen einen neuen Konnektor mit neuer Garantie und mehr Leistungsstärke bei voller Kostenerstattung.

11 | Bewusstsein für Sicherheit im Netz

Sicherheit im Netz ist kein Zufall. Wie der bewusste Umgang mit potenziellen Gefahrenquellen geht, erklären unsere IT-Sicherheitsexperten.

CGM CompuGroup Medical

Von A wie Arztsuche bis Z wie Zustellung

Digitale Patientenreise mit dem E-Rezept

Das E-Rezept ist da – und es bringt etliche Vorteile mit sich: für Patientinnen und Patienten, aber auch für die Arztpraxen. CLICKDOC ist der starke Partner bei allen Schritten der digitalen Patientenreise.

Menschen nutzen Online-Informationen in allen Bereichen ihres Lebens, auch bei Fragen rund um ihre Gesundheit. Studien zufolge recherchieren 72 Prozent der Befragten im Internet nach Symptomen, nach Diagnosen oder Therapien. Die medizinische Versorgung hat sich stark in den Online-Bereich verlagert und geht somit bereits ohne großes Zutun der Gesundheitsprofis auf digitalen Wegen. Warum diese nicht direkt mitgestalten?

Quellen: Capterra, apoBank, ABDA-Statistik.

1 Arzttermine vereinbaren – immer und überall

Krankheiten richten sich nicht nach der Uhr und viele Arztpraxen sind während ihrer Öffnungszeiten telefonisch schlecht zu erreichen, was für alle Beteiligten mehr als ärgerlich ist. Setzt die Praxis auf CLICKDOC, können Patientinnen und Patienten nicht nur nach Ärztinnen und Ärzten in ihrer Nähe suchen, sondern ihre Termine online buchen. Umfragen zeigen, wie groß das Interesse ist: 59 Prozent wünschen sich diesen Service, 79 Prozent schätzen, dies unabhängig von Telefonzeiten zu tun, und 83 Prozent finden gut, alle möglichen Termine direkt zu sehen. Die Technologie findet große Akzeptanz – und trägt dazu bei, dass die Versorgung der Patientinnen und Patienten verbessert wird.

2 Termine vor Ort oder per Videosprechstunde

Vielen Menschen fehlt die Zeit, zur Praxis zu fahren, einen Parkplatz zu suchen und dann vielleicht auch noch im Wartezimmer zu sitzen. Medizinisch sind persönliche Kontakte auch nicht immer notwendig. Mit CLICKDOC VIDEOSPRECHSTUNDE kommunizieren Ärztinnen und Ärzte mit Patientinnen und Patienten über moderne, sichere Technik. Die Praxis selbst kann weitere Fachärztinnen und Fachärzte hinzuziehen, beispielsweise, um Röntgenbilder, CTs oder MRTs zu besprechen. Von diesen Vorteilen sind Befragungen zufolge 91 Prozent aller Patientinnen und Patienten, die bereits Videokonsultationen hatten, überzeugt.

EINFACH FÜR ALLE

Das CLICKDOC E-REZEPT unterstützt die digitale Patientenreise bei sämtlichen Akteuren der medizinischen Versorgung.

Auf einen Blick:

CLICKDOC bildet alle Stationen der digitalen Patientenreise ab:

Arztsuche | Terminbuchung | Sprechstunde per Videokonferenz | Empfang des E-Rezepts | Apothekensuche | Bestellung und Lieferung von Medikamenten

3 E-Rezept – einfach digital ausstellen

Genau diesen Vorteil bietet CLICKDOC VIDEOSPRECHSTUNDE. Die Ärztin oder der Arzt stellt per Praxissoftware ein E-Rezept aus und legt es automatisch auf dem gematik-Server ab. Der Clou daran: CLICKDOC E-REZEPT schickt Patientinnen und Patienten eine SMS direkt auf ihr Smartphone. Sie brauchen nur noch den Link anzuklicken, um den Code des E-Rezepts zu öffnen. Patientinen und Patienten erhalten einen Link und können nach einer Sicherheitsabfrage das E-Rezept einsehen. Auch hier zeigen aktuelle Befragungen, was Patientinnen und Patienten denken. 70 Prozent erwarten, dass Arzneimittelverordnungen durch E-Rezepte einfacher werden. Und 75 Prozent verbinden das E-Rezept mit einem modernen, digitalen Gesundheitswesen.

4 E-Rezepte einlösen – bei der Apotheke vor Ort oder per Botendienst

Nutzen Patientinnen oder Patienten die CLICKDOC-App, haben sie nach dem Log-in mehrere Möglichkeiten. Sie können über die Suchfunktion eine Apotheke in ihrer Nähe finden, die Verordnung vorbestellen und sich auf Wunsch ihre Präparate per Botendienst liefern lassen. Sind Apotheken Mitglied bei IhreApotheken.de, profitieren Kundinnen und Kunden auch noch vom Online-Shop. Bekanntlich geben Deutschlands Bürgerinnen und Bürger ihren Apotheken Bestnoten: 93 Prozent sind mit den Dienstleistungen sehr zufrieden oder zufrieden. Und mit 300.000 Botenfahrten pro Tag kommen wichtige Arzneimittel schnell bis an die Haustür. Ärztinnen und Ärzte sowie Apothekerinnen und Apotheker ebnen mit der Nutzung von CLICKDOC E-REZEPT für Patientinnen und Patienten den Weg zur einfachen, digitalen medizinischen Versorgung.

CGM PROTECT – daran kommt keiner vorbei

Das Praxisnetzwerk abzusichern und hochsensible Patientendaten vor Angriffen zu schützen, ist insbesondere in diesen Zeiten im Gesundheitswesen wichtig.

Bereits seit Anfang 2021 gilt daher die IT-Sicherheitsrichtlinie gemäß §75b SGB V. Diese verpflichtet Arzt-, Zahnarzt- und Psychotherapiepraxen jeglicher Größenordnung dazu, Maßnahmen zur IT-Sicherheit, also zum Schutz von Hard- und Software, zu ergreifen, um Datenmissbrauch zu verhindern. Darunter fällt unter anderem der Einsatz einer Firewall sowie eines Virenschutzprogramms. Diese müssen für einen vollumfänglichen Schutz und einen reibungslosen Praxisbetrieb perfekt auf die Rahmenbedingungen in Ihrer Institution sowie Ihr Praxisnetzwerk abgestimmt sein. Die neue Produktlinie CGM PROTECT erfüllt alle genannten Anforderungen mithilfe der Produkte CGM Firewall und CGM Endpoint 360°. So sorgen Sie nicht nur für maximalen Schutz Ihrer Praxis-IT, sondern erhalten auch alles, was Sie brauchen, aus einer Hand.

CGM Firewall – der Türsteher für Ihre Netzwerk-IT

Die Wege, über welche sich Schadsoftware in Ihrem Praxisnetzwerk einnisten kann, sind ebenso vielfältig wie die Arten der Schadsoftware selbst (z. B. Viren, Trojaner oder Phishing-Mails). Umso wichtiger ist es, potenzielle Bedrohungen bereits „an der Schwelle" aufzuhalten. Genau dazu dient die Hardware-Lösung CGM Firewall: Dank ihrer Grundkonfiguration werden die Anforderungen der IT-Sicherheitsrichtlinie für Ihre Praxis optimal umgesetzt. Anhand individuell festgelegter Regeln, die auf die Bedürfnisse Ihrer Praxis abgestimmt sind, wehrt sie gezielt Netzwerkangriffe von außen ab. Dabei erlaubt sie nur Verbindungen, die im Vorfeld explizit freigeschaltet wurden. Der Eingangskanal zu Ihrer Praxis wird dadurch bestens geschützt und es entsteht eine kontrollierte „Türschwelle", an der freigeschaltete Verbindungen durch die automatische Sicherheitsfunktion der Firewall überprüft werden. Anpassungen in der Konfiguration und das Einspielen von Updates können dank des „Managed Firewall"-Konzepts remote erfolgen.

CGM Endpoint 360° – mehr als nur ein Virenschutz

CGM Endpoint 360° ist eine innovative IT-Sicherheitslösung für Computer, Laptops und Server, welche die Schutztechnologien eines klassischen Virenschutzes sowie eine Echtzeit-Überwachung vereint. Alle laufenden Anwendungen und Prozesse Ihres Computers oder Servers werden dabei überwacht und potenzielle Schadprogramme innerhalb Ihres Praxisnetzwerkes automatisch und in Echtzeit blockiert.

Perfekt aufeinander abgestimmt

CGM Firewall schützt Ihre IT vor allem vor dem, was von außen angreift. CGM Endpoint 360° schützt Ihre Computersysteme zusätzlich von innen. Die Kombination aus beiden Lösungen bietet Ihnen den perfekten Rundumschutz für Ihr Netzwerk und Ihre Patientendaten – richtlinienkonform und individuell anpassbar auf Ihre Bedürfnisse.

Alle Infos rund um CGM PROTECT und die Möglichkeit zur Kontaktaufnahme finden Sie auf unserer Website **cgm.com**/protect.

DIE TI ERNEUERT SICH

SO EINFACH GEHT'S

Mehr als 60.000 Institutionen arbeiten heute schon sicher mit CGM-Komponenten in der TI

Sicher haben Sie es auch schon gelesen oder gehört: Ihre Hardware für die Telematikinfrastruktur (TI) hat aus Sicherheitsgründen ein vorgegebenes Ablaufdatum. Und dies aus gutem Grund: In Deutschland ist mit der TI in den letzten Jahren in gemeinsamer Kraftanstrengung ein hochsicheres Gesundheitsnetz aufgebaut worden, das den sicheren Austausch von wichtigen, behandlungsrelevanten Patientendaten ermöglicht.
Ein wichtiger Bestandteil der Sicherheit sind die sogenannten Zertifikate in den TI-Komponenten. Diese sorgen dafür, dass sich nur zugelassene Komponenten mit der TI verbinden. Das bedeutet: ohne gültiges Zertifikat kein Zutritt zur TI. Die gematik hat Spezifikationen entwickelt, die diesen Zertifikaten ein Ablaufdatum mitgeben. Seit September 2022 laufen nun die ersten Zertifikate ab. Das bedeutet: Alle Praxen, deren Zertifikate dann ablaufen, müssen aktiv tätig werden, um nicht aus der TI ausgeschlossen zu werden. Vielleicht haben Sie es den Medien entnommen: In den letzten Wochen gab es endlich klare Aussagen zur Förderung des Hardwaretauschs, den diskutierten Alternativen, und darüber, wie dem Zertifikatsablauf zu begegnen ist.

Die Gesellschafter der gematik haben Ende Februar 2022 entschieden, die vorhandenen Konnektoren in den nächsten Jahren gegen neue Geräte auszutauschen. In der Gesellschafterversammlung der gematik Ende August 2022 wurden die zur Verfügung stehenden Alternativen zu einem Austausch der Konnektoren in den Praxen dann nochmals betrachtet. Das Ergebnis: Bei allen bis August 2023 ablaufenden Konnektoren ist der Austausch alternativlos und wurde als die „einzig sinnvolle Alternative" bestätigt. Für TI-Komponenten, deren Zertifikate ab September 2023 ablaufen, werden Wahlmöglichkeiten für den TI-Anschluss einer medizinischen Einrichtung denkbar – neben dem Konnektortausch könnte es dann die Möglichkeit einer Laufzeitverlängerung der TI-Gerätekarte oder einen Anschluss über eine Rechenzentrumslösung geben (siehe Newsroom der gematik unter gematik.de, Pressemitteilung vom 30.08.2022). Für die Kundinnen und Kunden, die jetzt den Konnektor tauschen werden, entsteht aber kein Nachteil: Unsere CGM-Kundinnen und -Kunden bekommen einen neuen Konnektor mit neuer Garantie und mehr Leistungsstärke bei voller Kostenerstattung.
Auch hinsichtlich der Förderung wurden im August und September 2022 Fakten geschaffen: KBV, KZBV und der GKV-Spitzenverband haben sich auf eine Förderung in Höhe von 2.300 Euro geeinigt. Die Förderung entspricht dem Angebot der CGM zum Hardwaretausch.

Aktuell bündeln wir in der CGM alle Kräfte, um den Anschluss unserer rund 60.000 Kundinnen und Kunden an die TI sicherzustellen. Es ist ein Projekt besonderer Größe, dessen Bedeutung uns für die Aufrechterhaltung der kritischen Infrastruktur bewusst ist. Wir werden, wie von den Gesellschaftern der gematik beschlossen, alle Konnektoren mit Zertifikatsablauf bis August 2023 tauschen und allen Praxen, die einen Zertifikatsablauf ab September 2023 planen müssen, sofort Informationen zukommen lassen, sobald weitere Alternativen beschlossen wurden.

Sollte eine Ihrer Komponenten von einem Zertifikatsablauf betroffen sein, wird Ihnen in Ihrem CGM-Arztsoftwaresystem eine Meldung angezeigt, die auf den Zertifikatsablauf und Handlungsbedarf hinweist. Daneben informieren wir betroffene Kundinnen und Kunden postalisch in einem mehrschrittigen Informationssystem. Parallel stellen wir Ihnen ein Prüfmodul bereit, das Sie nach Eingabe von Kundennummer und Postleitzahl über die Ablaufdaten der Zertifikate Ihrer Praxis informiert und Handlungsempfehlungen generiert.

„Jede Hardware, egal, ob man sie in der Praxis nutzt, oder auch privat, wird nach einiger Zeit getauscht – hier geht es meist um viel kürzere Nutzungszeiten und teilweise höhere Kosten als beim Konnektor und den anderen TI-Komponenten. Und man darf eines nicht vergessen: Beim Hardwaretausch geht es um die Sicherheit und die Daten der Patientinnen und Patienten. Für uns war es selbstverständlich, dass wir den neuen Konnektor in unserer Praxis einsetzen."

Alex Donner, HNO aus Solingen

Gut zu wissen:

Wann laufen die Zertifikate in meiner Praxis ab?

Wie kann ich einen Termin für den Konnektortausch erhalten?

Kostenfreie Online-Informationsveranstaltungen

In welcher Höhe wird der Konnektortausch refinanziert?

Alles rund um den Konnektortausch finden Sie auf unserer Website

#thinkb4uclick

Wie das eigene Bewusstsein die Sicherheit im Netz maßgeblich beeinflusst

E-Mail, QR-Code, Social Media oder die Nutzung von digitalen Endgeräten und dem Internet im Allgemeinen: Mögliche Tatorte für Cyberkriminalität besuchen wir alle beruflich wie privat mehrmals täglich. Das Risiko, in die Fänge von Cyberkriminellen zu geraten, steigt stetig. Doch die eigene Sicherheit im Netz ist nicht nur Zufall oder durch teure Tools zu beeinflussen – maßgeblich ist der bewusste Umgang mit potenziellen Gefahrenquellen. Wie dieser Umgang aussehen kann und was „Think bevor you click" damit zu tun hat, das erklären die CGM-IT-Sicherheitsexperten Jochen Klein und Matthias Limbach im Interview.

Das Thema Cybersecurity scheint immer wichtiger zu werden. Gibt es konkrete Anhaltspunkte dafür, dass die Kriminalität im Netz tatsächlich zunimmt?

Jochen Klein: Ja, da gibt es definitiv konkrete Anhaltspunkte. Im Großen und Ganzen beobachten wir, dass die Angriffsszenarien deutlich zunehmen und sich die Kriminellen, die dort angreifen, professionalisieren. Wir stellen fest, dass sich bestimmte Gruppen zusammenschließen, um kriminelle Organisationen zu bilden. Solche Angriffe werden inzwischen bereits als „as a Service" angeboten. Das heißt, ich kann mir im Darknet Kapazitäten mieten und darüber dann letzten Endes Firmen, Unternehmen und Institutionen angreifen. Und auch Privatpersonen natürlich.

Habt ihr konkrete Tipps, wie sich Anwenderinnen und Anwender gegen Cyberkriminalität schützen können? Beim Arbeiten oder in der Freizeit?

Matthias Limbach: In erster Linie durch Aufmerksamkeit. So banal sich das anhört, einfach überlegen, bevor ich auf einen Link in einer E-Mail klicke. Bevor ich am Telefon irgendjemandem eine Antwort gebe. Denn der größte Angriffsvektor ist nach wie vor das klassische Phishing und da gibt es unterschiedliche Varianten.

Jochen Klein: Genau. Also generell ist das auch eines der Mottos, die mit der Aktion Cybersecurity Month* einhergehen: **„Think before you click"**. Also denk nach, bevor du auf irgendwas draufklickst. Gerade beim Thema Phishing versuchen Cyberkriminelle, über gefälschte E-Mails die Anwenderin oder den Anwender dazu zu verleiten, auf einen bestimmten Link zu klicken oder einen Anhang zu öffnen und darüber dann beispielsweise die Zugangsdaten zu bestimmten Portalen im Internet abzugreifen. Oder aber auch die Computer des oder der Angegriffenen zu kompromittieren, dort entsprechende Schadsoftware zu installieren.

Das heißt in diesem speziellen Fall sollte ich schon misstrauisch werden, wenn ich eine E-Mail von einem Absender bekomme, den ich vielleicht gar nicht kenne?

Matthias Limbach: Vollkommen korrekt, ja. Da fällt mir der Satz ein, den meine Großmutter mir als Kind schon gesagt hat: „Trau, schau, wem!" Sobald ich nur irgendeinen Zweifel habe, lieber noch mal nachfragen und vergewissern. Dann bin ich eher auf der sicheren Seite. Vorsicht gilt übrigens auch bei QR-Codes. QR-Codes sind einfach nur zweidimensionale Codes, die Klartext – also beispielsweise auch Links – darstellen und die ich mit jedem Smartphone abfotografieren kann. Das Problem ist, ich sehe auf den ersten Blick nicht dahinter, also wohin mich dieser Link führt. Hier kann ich nur darauf hinweisen, dass es unterschiedliche Betriebssysteme bei Smartphones und anderen Endgeräten gibt, und die neuesten Versionen sind in der Regel so ausgelegt, dass sie **den Link bei Scan des QR-Codes erst anzeigen**. Aufgerufen wird er dann, indem man aktiv daraufklickt. Das kann man meistens in den Einstellungen des Smartphones festlegen.

Wie kann man sich noch schützen?

Matthias Limbach: Ein wichtiger Faktor ist ganz sicher auch, dass man seine Endgeräte, also Laptops, Computer, Mobiltelefone, immer auf dem **aktuellen Stand der Software** hält. Denn letztendlich werden mit jedem Update der Anbieter Sicherheitslücken geschlossen. Das heißt: Kommt ein Update raus, dann bitte installieren.

Jochen Klein: Ja, das Update-Thema ist extrem wichtig, weil das tatsächlich eines der größten Einfallstore ist. Es gibt natürlich auch ganz einfache Tipps, wie **Endgeräte sperren**. Also wenn ich meinen Computer irgendwo stehen lasse und weggehe, immer sperren. Auf Windows-Systemen einfach **Windows-Taste plus L** und das Gerät ist gesperrt. So ist kein Zugriff mehr möglich für Personen, die dieses Gerät so vorfinden.

Matthias Limbach: Das kann man sich auch relativ einfach merken: „Windows L geht schnell!" Also das ist eigentlich nicht das Problem. Das sind zwei Finger, zwei Tasten. Einmal drücken und der Rechner ist gesperrt.

Du hast gerade angesprochen, dass es leicht gehen soll. Nimmt man den privaten Bereich und den Arbeitsbereich zusammen, hat man oftmals gefühlt 150 Passwörter. Habt ihr einen Tipp, wie man da vorgehen kann? Gibt es vielleicht Techniken oder Unterstützung, die man bei der Passwortgenerierung und beim Verwalten der Passwörter nutzen könnte?

Jochen Klein: Da ist der Tipp ganz klar die Verwendung von sogenannten Passwort-Managern. Diese Tools sind in der Lage, sichere Passwörter zu generieren und diese dann auch zu verwalten. Der Vorteil dabei ist einfach, dass man letzten Endes einen zentralen Login zu dem Tool hat, und darüber alle anderen Passwörter verwendet werden können. Zum Schutz eines solchen **Passwort-Managers** sollte man sich natürlich auch ein sicheres Passwort überlegen.

Thema Social Media: Muss man da etwas Besonderes beachten?

Jochen Klein: Alles, was ich bei Social Media eingebe, ist per se erst mal mehr oder weniger öffentlich. Durch diese Daten können Rückschlüsse gezogen und gezielte Attacken per E-Mail oder Telefon ausgeübt werden. Es gibt im Darknet sogar Suchmaschinen, die darauf spezialisiert sind, verschiedene Informationen zu einer Person, zu einer E-Mail-Adresse zu konsolidieren.

Matthias Limbach: Ich höre auch im Privaten oft: „Das ist doch egal, die wissen doch eh alles über mich." Diese Resignation sollte man, glaube ich, überwinden. Sie werden wahrscheinlich viel wissen, aber sie müssen ja nicht wirklich alles wissen. Vielleicht ist genau dieser eine Punkt, den sie vielleicht noch nicht wissen, die entscheidende fehlende Information, um gegen mich einen Angriff starten zu können. Also auch da einfach: **„Bewusst sein, was ich poste"**. Ich habe auch die Möglichkeit, viele Sachen nur in geschlossenen Benutzergruppen oder unter Freunden, Bekannten und Familie zu teilen.

Jochen Klein: Man muss sich generell immer dessen bewusst sein: **„Nichts ist umsonst"**. Deswegen sollte ich nicht nur in sozialen Medien vorsichtig sein, sondern auch bei Gewinnspielen beispielsweise bewusst überlegen, ob oder welche Daten ich preisgebe. Man kann zum Beispiel alternativ eine separate E-Mail-Adresse anlegen, die keine Rückschlüsse auf die Person zulässt und die man dann vielleicht für so etwas verwendet.

Wussten Sie schon?

*Jedes Jahr im Oktober findet der Cybersecurity-Month mit verschiedenen Aktionen statt, um das Sicherheitsbewusstsein beim Thema Cyberkriminalität zu steigern. In Europa wird er maßgeblich durch die ENISA (Agentur der Europäischen Union für Cybersicherheit) gestaltet.

Die Telematikinfrastruktur (TI) wächst – immer mehr Heilberufler kommen dazu

Nachdem Arzt- und Zahnarztpraxen, Apotheken, Krankenhäuser und gesetzliche Krankenversicherungen an die Telematikinfrastruktur (TI) angebunden wurden, haben nun die nicht-verkammerten Heilberufe die Gelegenheit, Teil dieses großen und sicheren Netzwerks zu werden. Als führendes E-Health-Unternehmen ist die CompuGroup Medical (CGM) seit vielen Jahren maßgeblich an der Entwicklung und dem Aufbau der TI, dem digitalen Gesundheitsnetz für Deutschland, beteiligt. Mehr als 60.000 Institutionen arbeiten heute schon sicher mit CGM-Komponenten in der TI – und es werden täglich mehr. Von dieser Erfahrung können nun auch Einrichtungen aus dem Bereich der nicht-verkammerten Heilberufe wie Hebamme oder Physiotherapeutin und -therapeut profitieren. Der Anschluss an die TI bietet diesen Einrichtungen und ihren Mitarbeitenden den Zugang zum Kommunikationsnetz mit behandelnden Kolleginnen bzw. Kollegen und sorgt dafür, dass die Behandlungsqualität deutlich steigt, während der administrative Aufwand minimiert wird.

Die CGM kooperiert deshalb auch aktiv mit Softwareanbietern in den Berufsgruppen Hebamme, Heilmittelerbringer, Rehabilitations- und Pflegeeinrichtungen sowie dem Öffentlichen Gesundheitsdienst (ÖGD) und hat bereits die erste Physiotherapiepraxis und die erste Pflegeeinrichtung an die TI angeschlossen. Der Nutzerkreis wächst also und wird interdisziplinärer, was besonders relevant ist, denn: Damit die wichtigsten Patienteninformationen schnell und einfach verfügbar werden, müssen alle Leistungserbringer im Gesundheitswesen an einem Strang ziehen – und sich um die im Mittelpunkt stehenden Patientinnen und Patienten bestmöglich vernetzen. Das Vorantreiben der Digitalisierung ist dabei die zentrale Voraussetzung für die erfolgreiche Weiterentwicklung der Gesundheitsversorgung. Nur die Vernetzung aller Leistungserbringer untereinander sowie mit den Patientinnen und Patienten sorgt dafür, dass die Versorgung verbessert wird.

Beispielsweise wird die Krankheitsgeschichte einer Patientin bzw. eines Patienten durch die gemeinsame Nutzung der elektronischen Patientenakte (ePA) und die Sammlung von Befunden, Diagnosen, Therapiemaßnahmen, Behandlungsberichten sowie elektronischen Medikationsplänen transparenter und jeder berechtigte Leistungserbringer weiß, was der andere tut. Dies ist ein enormer Mehrwert für alle, die an der Versorgung beteiligt sind: Durch die gemeinsame Dokumentation in der ePA kann die Betreuung durch Ärztinnen und Ärzte, Hebammen, Therapeutinnen und Therapeuten etc. besser untereinander abgestimmt werden. Die interdisziplinäre Zusammenarbeit wird dadurch verbessert und die eigene Reflexion der Therapie erleichtert.

Dabei braucht es aber nicht nur für die Weiterentwicklung der ePA Menschen, die voranschreiten, sondern auch für die Kommunikation im Medizinwesen (KIM). Da die meisten Ärztinnen und Ärzte diesen Dienst bereits für den Versand der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) nutzen, können diese jetzt schon durch die aktive Nutzung von KIM für die Kommunikation mit anderen Leistungserbringern profitieren und so die Vernetzung innerhalb der Gesundheitsversorgung aktiv vorantreiben.

Alles rund um die TI finden Sie auf unserer Website

IMPRESSUM

HERAUSGEBER
CompuGroup Medical Deutschland AG
Maria Trost 21, 56010 Koblenz

REDAKTION
Nicola Böhler
Julia Girnus
Nicole Graf
Beata Luczkiewicz
Yannick Schmidt
Dr. Dorothée Zerwas

LEKTORAT
Sebastian Riechert

LAYOUT
Sina Huder

BILDNACHWEIS
gettyimages: S. 1, 15

DRUCK
KRMP Intermedia GmbH
Habsburgerring 1 | 50670 Köln

vision

CompuGroup Medical Deutschland AG
Maria Trost 21 | 56070 Koblenz
cgm.com/de

„Niemand soll leiden oder sterben, nur weil einmal irgendwann, irgendwo eine medizinische Information fehlt.“

Frank Gotthardt, Gründer CompuGroup Medical

CGMCOM_18796_VOR_1022_SWI