

Arztbriefe

Das häufigste ärztliche Dokument, der Arztbrief, gelangt derzeit noch meist per Post vom Krankenhaus oder Facharzt zum Hausarzt. Gefaltet und verpackt in einen Briefumschlag, immerhin mit Fenster (so entfällt wenigstens das doppelte Adressieren), frankiert und zugeklebt, wandert der Brief über Briefkasten und Post zum Hausarzt. Nach ein bis zwei Tagen trifft er beim Empfänger ein. Die Praxismitarbeiterin muss ihn aus dem Briefkasten holen, öffnen und ins Sprechzimmer des Arztes transportieren. Dort wird er gelesen, anschließend wieder aus dem Arztzimmer geholt, um in Schrank, Schublade und Karteikarte einsortiert zu werden – hoffentlich beim richtigen Patienten. Das ist teuer, langsam und mit viel Arbeit und Fehlerfällen verbunden.

Interne Prozessoptimierung vorausgesetzt (siehe „Papierlose Arztpraxis, Teil 1“ in PRAxiS 1/2011), lässt sich auch die externe Kommunikation optimieren. Praktisch jeder Arztbrief entsteht heute computergestützt, und jeder Empfänger hat einen Rechner. Somit besteht die Möglichkeit, den im PC entstandenen Brief ohne Medienbruch statt auf Papier auf elektronischem Weg in den Rechner des Empfängers zu befördern. Das ist preiswert, fast kostenfrei, schnell und mit wenig Arbeit verbunden. Allerdings: Wer als Hausarzt diese Kommunikationsform nutzen möchte, muss in seinem Facharztumfeld meist erst einmal dafür werben. Er muss versuchen, die Kollegen zu überzeugen, dass von der Abschaffung des Postbriefes alle profitieren können.

Per Fax

Faxgeräte werden mittlerweile flächendeckend in den Praxen der niedergelassenen Ärzte genutzt. Bemerkenswert ist, dass der Versand von

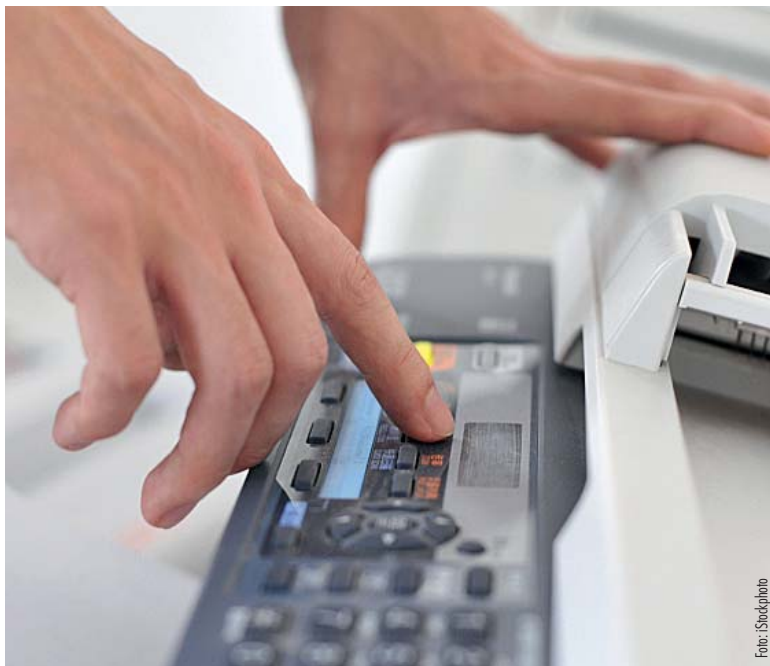
Papierlose Arztpraxis, Teil 2

Sichere Kommunikation und Datenhaltung

Wie lässt sich die elektronische Kommunikation mit externen Partnern gestalten, und was ist hinsichtlich der Datensicherheit zu beachten?

Mehr Effizienz durch optimalen Einsatz der Praxis-EDV – das lässt sich auch und gerade in der externen Kommunikation erreichen. Manches, das technisch möglich wäre, wird allerdings heute noch wegen datenschutzrechtlicher Probleme gebremst. Im Folgenden geht es um die Möglichkeiten und Grenzen der papierlosen externen Kommunikation in der Arztpraxis. In diesem Zusammenhang spielen auch Datensicherheit und Datensicherung eine Rolle. Dem Datenschutz kommt in der Arztpraxis

ein besonders hoher Stellenwert zu. Ebenso wichtig ist die Datensicherung im Hinblick auf die rechtssichere Dokumentation. Die hierfür geltenden Grundsätze haben Bundesärztekammer und Kassenärztliche Bundesvereinigung 2008 in ihren „Empfehlungen zur ärztlichen Schweigepflicht, zu Datenschutz und Datenverarbeitung in der Arztpraxis“ zusammengefasst (siehe www.aerzteblatt.de/v4/archiv/pdf.asp?id=60114 und die Technische Anlage unter www.aerzteblatt.de/v4/plus/download.asp?typ=PDF&id=2316).



Das herkömmliche Faxgerät ist derzeit in Praxen noch stark verbreitet, es wird jedoch zunehmend durch das elektronische Fax per Computer ersetzt.

Arztbriefen mittels Faxgeräten trotz der noch andauernden datenschutzrechtlichen Diskussion allgemein üblich ist. Es wird noch lange dauern, bis eine einheitliche software- und sektorenübergreifende Technologie für die sichere elektronische Beförderung des Arztbriefes eingeführt ist und von allen Ärztinnen und Ärzten angewandt wird. Daher sollte die derzeitige Faxlösung als nützlicher Übergang betrachtet werden.

Ein geringer Teil der Praxen hat schon auf elektronische Faxprogramme umgestellt und das Faxgerät abgeschafft. Dadurch entfallen hohe Betriebs-, Wartungs- und Wiederbeschaffungskosten. Empfang und Versand erledigt nun eine Steckkarte im Rechner. Wichtig ist dabei, dass das dazugehörige Programm ein Empfänger-Telefonbuch verwaltet, damit es nicht zu Wählfehlern und Fehlläuferten kommt. Der Arztbrief verlässt die Praxis in sauberer und leserlicher Form und kommt genauso beim Empfänger an. Das Programm arbeitet im Hintergrund, wodurch der Versand keinerlei Zeit beansprucht und kein Personal benötigt wird. Per Elektronikfax ange-

kommen, wird der Brief gelesen und mit einigen Klicks patientenbezogen im elektronischen Praxisarchiv abgespeichert und bei Bedarf gelesen.

Per E-Mail

Arztbriefe können im Prinzip auch als E-Mail-Text oder als E-Mail-Anhang (Attachment) versendet werden. Dabei muss die Mail jedoch verschlüsselt sein, und der Empfänger muss sie entschlüsseln können. Eine von allen Ärzten benutzte Kommunikationsplattform, die die Erfordernisse des Datenschutzes und der Datensicherheit erfüllt, steht nicht zur Verfügung. Wahrscheinlich könnten viele Ärzte mangels Übung damit auch noch nicht umgehen.

Seit zwei Jahrzehnten versuchen verschiedene Anbieter, entsprechende Plattformen zu etablieren. Bisher sind solche Ansätze aber an der fehlenden Akzeptanz der Ärzte gescheitert. Einige Softwarehäuser bieten bereits kostenfreie Plattformen, die sämtlichen Anforderungen an Datenschutz und technische Sicherheit genügen. Arztbriefe wandern dort vom Versen-

der in Millisekunden in die Karteikarte des Patienten beim Empfänger. Es ist und bleibt ein Rätsel, warum dies innerhalb der Ärzteschaft noch so wenig Anklang findet. Nach dem jetzigen Stand der Dinge gibt es lediglich einige gut funktionierende Insellösungen für die interne Kommunikation in Praxisnetzen sowie für die Kommunikation zwischen niedergelassenen Ärzten und Krankenhäusern. Auch von den Kassenärztlichen Vereinigungen gesteuerte Plattformen entstehen derzeit.

Der neue elektronische Arztausweis wird hier möglicherweise wegen der enthaltenen digitalen Signatur des Arztes einen Durchbruch bringen. Bis dahin ist es, von den genannten Insellösungen abgesehen, noch nicht möglich, die Effizienzvorteile der digitalen Kommunikation voll zu nutzen.

IT-Sicherheit

Sämtliche Patientendaten, die sich auf der Festplatte befinden, sind vor unberechtigtem Zugriff zu schützen. Das beginnt an der Rezeption, wo die Monitore so zu positionieren oder mit Sichtschutz zu versehen sind, dass kein Außenstehender die Daten lesen kann. Darüber hinaus unterliegen auch die Praxisangestellten der Schweigepflicht und tragen große Verantwortung für den Datenschutz und die Datensicherheit. Je nach Aufgabengebiet müssen daher auch die Zugriffsberechtigungen der Mitarbeiter und Mitarbeiterinnen individuell definiert und gesetzt werden.

Praxisrechner müssen prinzipiell gegen Diebstahl geschützt werden. Zu entsprechenden Schutzmaßnahmen zählen beispielsweise Tür- und Fenstersicherungen. Besonderes Augenmerk ist auch auf den Umgang mit den Praxissschlüsseln zu legen. Schlüsselberechtigte Personen, einschließlich der Reinigungskraft, müssen besonders vertrauenswürdig sein. Die Rechner selbst sollten mit alphanumerischen Passwörtern vor unberechtigtem Zugriff geschützt sein.

Datensicherung

Praxiscomputer und Praxissoftware werden zwar immer zuverlässiger, dennoch können jederzeit Störungen oder Ausfälle auftreten. Außerdem können sie gestohlen, durch Wasser oder Feuer beschädigt oder auch mutwillig zerstört werden. Für diesen Fall sind regelmäßig Festplattenkopien anzufertigen. Ein Teil- oder gar Totalverlust der Daten ist unter allen Umständen zu vermeiden.

Es gibt verschiedene Formen der Datensicherung je nach dem Kopiermedium: über eine interne zweite Festplatte, über eine externe Festplatte (meist USB), mittels Bandsicherungsgerät, CD, DVD, Bluray-Disc oder Auslagerung. Der Ablauf ist stets derselbe: Eine Spezialsoftware kopiert die Daten von der Festplatte auf das Kopiermedium und kontrolliert anschließend die Kopie durch Vergleich mit der Ausgangsdatei.

Dieser Vorgang nimmt je nach Programm, technischer Ausrüstung und Datenmenge mehr oder weniger Zeit in Anspruch. Daher kann abhängig vom Betrieb der Zeitpunkt der täglichen Datensicherung unterschiedlich festgelegt werden: Die einen machen

sie in der Mittagspause, die anderen lassen sie nachts laufen.

Man benötigt in der Regel einen oder zwei Sätze à fünf externe Speichermedien, um sie der Reihe nach einzusetzen. So hat man immer bis zu einer oder zwei Wochen alte Datensicherungen. Im schlimmsten Falle können dann die externen Kopien für die Rekonstruktion der Festplatte verwendet werden. Es ist unbedingt notwendig, die Sicherungsmedien in regelmäßigen Abständen durch die Softwarefirma überprüfen zu lassen. Deren Techniker prüft, ob die gesicherten Daten die für eine Rekonstruktion nötige Qualität aufweisen. Heute sind externe USB-Festplatten ein beliebtes Sicherungsmedium. Sie sind preiswert, klein, leicht, schnell und zuverlässig. Die externen Sicherungskopien sind unter allen Umständen



Der elektronische Arztausweis ermöglicht das digitale Signieren und Verschlüsseln von Dokumenten.

Foto: MedSign

den außerhalb der Praxis aufzubewahren. Es empfiehlt sich, während des Urlaubs eine zusätzliche Kopie im Banksafe aufzubewahren.

Beweissicherheit

Ärzte genießen das rechtliche Privileg, dass ihrer Dokumentation eine hohe Glaubwürdigkeit zugeschrieben wird. Anders verhält es sich, wenn es Anzeichen dafür gibt,

dass die Dokumentation nachträglich geändert wurde. Somit muss auch für die digitale Dokumentation der Nachweis geführt werden, dass sie gegen nachträgliche Änderungen gesichert ist. Einfache Kopien auf einer externen Festplatte genügen nicht.

Die Beweissicherheit einer Datenkopie lässt sich mit einfachen Mitteln herstellen. Das deutsche Recht gestattet eine zertifizierte digitale Signatur. Diese befindet sich üblicherweise auf dem Chip einer Signaturkarte, die man von einem der hierfür zugelassenen Unternehmen – unter anderem Post und Telekom – bezieht. Mit dieser Karte, einem Lesegerät und entsprechender Software wird die Kopie der Praxisdaten vom Arzt digital unterschrieben oder signiert. Danach holt sich die Software bei dem die Signaturkarte ausstellenden Unternehmen Uhrzeit und Datum und setzt diese in die Kopie ein. Jeder Versuch, die auf dem Kopiermedium gespeicherten Daten zu verändern, zerstört die Unterschrift und die Zeitangabe unwiderruflich. Mit digitaler Signatur und externem Zeitstempel versehene Praxisdatenkopien haben einen sehr hohen Beweiswert vor Gericht. **Zlatko Prister**

Tipps zur Auswahl von Hard- und Software

Für den Betrieb einer Arztpraxis benötigt man sichere und für einen Dauerbetrieb technisch ausgelegte Rechner. Hinzu kommt der Bedarf an guter Peripherie, darunter Netzwerk, Drucker, Kartenlesegeräte, medizintechnische Geräte wie EKG, Lungenfunktionsmessgerät, Sonographie, digitale Kamera, Laborgeräte, Telefonanlage, ISDN-Karte, Internetanschluss mit Router und Firewall. Bei der Investition in die Hardware – Rechner und Peripherie – sollte nicht gespart werden. Softwarehäuser und ihre Vertriebspartner haben hierfür entsprechende Berater. Bei der Auswahl der Monitore sollte die Ergonomie im Vordergrund stehen.

Die richtige Wahl der Praxissoftware dürfte oft schwieriger sein. Eine Demonstration wichtiger Funktionen reicht nicht, um einen echten Einblick in die Funktionalitäten des Programms zu gewinnen. Das gesamte Angebot anzusehen, ist schlicht nicht möglich. Hier können Empfehlungen von Kollegen und Anwenderberichte hilfreich sein. Hastige Entscheidungen können sich rächen – ein späterer Systemwechsel ist eine mühsame Angelegenheit. Darüber hinaus ist es jedem zu empfehlen, die IT-Beratungsstellen der Kassenärztlichen Vereinigungen in Anspruch zu nehmen.

Anschrift des Verfassers

Dr. Univ. Zagreb Zlatko Prister, Hausarzt
Zeil 111, 60313 Frankfurt/M.
www.prister.de, praxis@prister.de

Siehe auch „Papierlose Praxis (Teil 1): Interne Prozesse optimieren“, www.aerzteblatt.de/epaper/PRAXIS/2011/2/?startpage=12