KBV ändert Vorgaben für Arzneidatenbanken

Seit Juli gelten umfangreiche neue Vorgaben der KBV an die Verordnungssoftware beziehungsweise Arzneimitteldatenbanken der Praxissoftware-Systeme. In der Regel werden die neuen Anforderungen von allen von der KBV zertifizierten EDV-Anbietern automatisch umgesetzt. Ärzte sollten aber darauf achten, dass neue Updates diese Änderungen auch tatsächlich beinhalten beziehungsweise dies mit ihrem Software-Anbieter klären. Das Software-Haus TurboMed hat zum Beispiel angekündigt, dass mit dem Q3-Update Ärzten eine neue Generation der ifap-Medikamentendatenbank zur Verfügung steht, die die neuen Vorgaben abdeckt.

Rebeka Höhl

Thinkpad nun auch im Tablet-Format

Mit dem Lenovo Thinkpad Tablet ist ein neuer Tablet-PC auf dem Markt, der sich durch sein robustes Gehäuse auch für den Praxisalltag eignet. Zwar ist das Thinkpad mit seinen 753 Gramm eher ein Schwergewicht unter den Tablets, aber dafür bietet es eine Abdeckung aus Gorilla-Glas und eine rutschhemmend beschichtete Rückseite. Für einfache Bedienung sorgen der mitgelieferte Digitalstift, der sich im Gehäuse versenken lässt, und die vier Hardkeys auf der Frontseite, über die man etwa den Browser schnell öffnen kann. Das Gerät kostet laut Hersteller allerdings um die 690 €, bietet dafür aber HDMI- und USB-Anschluss.

Rebeka Höhl

Social Media mausern sich zum Marketinginstrument

Fast die Hälfte (47%) aller Unternehmen in Deutschland setzt soziale Medien ein. Weitere 15 % haben bereits konkrete Pläne, damit in Kürze zu beginnen – so das Ergebnis einer repräsentativen Umfrage des Branchenverbands BITKOM, für die 723 Unternehmen aller Branchen befragt wurden. Als wichtigstes Ziel für den Einsatz der Sozialen Medien nennen 82 % der Unternehmen, die Social Media bereits einsetzen, die Steigerung ihres Bekanntheitsgrades. Für 72 % steht die Gewinnung neuer Kunden im Vordergrund und für 68 % die Pflege von Kundenbeziehungen. 42 % der Befragten wollen ihr Image verbessern, 23 % neue Mitarbeiter gewinnen.

red

Strenge Datenschutzregeln für Praxen

In einer „Cloud“ (Rechnerwolke) werden die Daten über ein Verschlüsselungsverfahren in unlesbare Kleinteile zerlegt und so gespeichert. Erst wenn sich der Nutzer mit seinen Zugangsdaten in das Programm oder auf dem Server einloggt, werden sie wieder über ein spezielles Programm zusammengeführt. Ärzte müssen, zumindest wenn es um Praxis- und Patientendaten geht, ganz besonders auf das Thema Datenschutz achten. Und hier wird Cloud-Computing heikel. Entscheidend sei, dass personenbezogene Gesundheitsdaten nicht Dritten zugänglich gemacht werden, erklärt Fachanwalt für Medizin- und Sozialrecht Professor Christian Dierks aus Berlin. Das heißt, Ärzte können auch Patientendaten auf webbasierten Servern ablegen, sie müssten aber auf „eine sichere Verschlüsselung oder eine Anonymisierung“ der Daten achten. Die Zuordnung zu Personen müsse faktisch ausgeschlossen sein.

„Die Verantwortung für die Patientendaten trägt letztlich der Arzt“, so Dierks. „Er verstößt gegen § 28 Bundesdatenschutzgesetz (Datenerhebung und -speicherung für eigene Geschäftszwecke), wenn die Daten anderen zugänglich werden. Zwar gibt es die Möglichkeit der Auftragsdatenverarbeitung, nach der eine Übermittlung personenbezogener Gesundheitsdaten an einen Cloud-Anbieter möglich wäre. Aber es ist unklar, ob darin nicht noch ein Verstoß gegen § 203 Strafgesetzbuch (Verletzung von Privatheimnissen) vorliegt.“ Deshalb müsse durch eine clientseitige Verschlüsselung, wie etwa durch TeamDrive, die Identität der Patienten geschützt werden. Der Cloud-Anbieter sei dann nicht in der Lage, einen Personenbezug herzustellen. Aber auch, wenn es um verschlüsselte Praxisdaten geht, sollte der Anbieter gründlich ausgewählt werden. Zudem sollte der Arzt prüfen, in welche Länder Daten transferiert werden, denn auch das hat Auswirkungen auf den Datenschutz, erklärt Dierks.

Im schriftlichen Vertrag mit dem Cloud-Service-Anbieter sollte neben dem Nutzungsumfang des Services laut Dierks Folgendes geregelt sein: die technische Datensicherung, der Datenschutz (diese Klausel sollte den Schutz der Integrität beinhalten und den Zugriff des Anbieters auf Personenidentitäten ausschließen), die Dokumentationspflichten des Cloud-Anbieters, die Verfügbarkeit der Daten und eventuell Vertragsstrafen, wenn Leistungsvereinbarungen nicht eingehalten werden.

Alternative Privat-Cloud

Für Ärzte, die in einem Ärztenetz zusammenarbeiten wollen, besteht die Möglichkeit, sich eine eigene „private cloud“ aufzubauen. Dann steht der gemeinsame Datenserver in einem abgesicherten Raum entweder in einer der Praxen oder bei der Managementgesellschaft des Netzes. Denkbar ist auch, die private Cloud an einen Dienstleister auszulagern. Aber auch dann sollte der Server in einem bestimmten, speziell gesicherten Rechenzentrum stehen. Die Patientendaten bleiben trotzdem in den einzelnen Praxen. Durch die Cloud kann aber übergreifend auf Fallakten oder Terminkalender zugegriffen werden oder der gesicherte Austausch von Daten erfolgen. IBM bietet beispielsweise solche Private-Cloud-Modelle an, mit denen auch Gesundheitsinformationen datenschutzkonform verarbeitet und gespeichert werden können, da die Infos weiterhin unter ärztlicher Hoheit und damit unter Beschlagschutz stehen, wie IBM erklärt. „Solche Modelle sind aber in Deutschland sehr selten, da es für sektoral organisierte Leistungserbringer bisher wenig Anreize gibt,

Patienteninformationen auszutauschen und eine sektorenübergreifende, integrierte Patientenversorgung effizienter zu koordinieren“, sagt Manuela Müller-Gerndt, bei IBM Deutschland für den Bereich Healthcare verantwortlich.

Sicherheit hört vor der Praxistür nicht auf

Auch Microsoft erprobt derzeit ähnliche Plattformlösungen. Ein Beispiel ist das Gesundheitsbuch von gnf Mediber, hinter dem die Microsoft-Cloud-Lösung HealthVault liegt. Hierüber können Senioren Zuhause wichtige Vitalparameter erfassen und dem Arzt über ein Zugriffsrechtssystem via Cloud zur Verfügung stellen. Doch es sind nicht nur die Anbieter, die eine Cloud sicher oder unsicher machen. „Solange mein Ende der Leitung nicht sicher ist, ist auch die Cloud nicht sicher“, betont Beckenbach. Das heißt, der Internetzugang und der Rechner in der Praxis sollten ebenfalls vor Zugriffen Dritter und vor Malware geschützt werden. Nicht nur mit aktuellen Virenschutzscannern, dazu gehört laut Beckenbach in jedem Fall auch eine Firewall.

Rebeka Höhl