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 in einem solchen Fall sollte der Server in einem bestimmten, speziell gesicherten Rechenzentrum stehen. Die Patientendaten bleiben trotzdem in den einzelnen Praxen. Mithilfe der Cloud kann aber übergreifend auf Fallakten oder Terminkalender zugegriffen werden oder der gesicherte Austausch von Daten stattfinden.

IBM bietet beispielsweise Privat-Cloud-Modelle an, mit denen auch Gesundheitsinformationen datenschutzkonform verarbeitet und gespeichert werden können, da die ausgelagerten Daten weiterhin unter ärztlicher Hoheit und damit unter Beschlagschutz stehen, wie IBM erklärt. „Solche Model-

KBV ändert Vorgaben für Arzneydatenbanken

Seit Juli gelten umfangreiche neue Vorgaben der KBV an die Verordnungssoftware beziehungsweise Arzneymitteldatenbanken 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 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.

reh

le 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 nicht vor der Praxistür 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 Se-

nieren zuhause wichtige Vitalparameter erfassen und dem Arzt über ein Zugriffssystem 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. Hierzu benötigt man nicht nur einen stets aktualisierten Virenschutz, sondern laut Beckenbach in jedem Fall auch eine gut funktionierende Firewall.

Rebeka Höhl

Anzeige