Medical Cloud: Alle Daten werden bereits in der Praxis verschlüsselt und dann erst in der Cloud abgelegt.

Medical Cloud

Gibt es doch eine sichere Datenwolke für Praxen?

Ärzten wird eher davon abgeraten, Praxisdaten in so genannte Clouds zu stellen. Ein Health-IT-Anbieter arbeitet derzeit aber an einer Datenwolke, in der es keine Sicherheitsprobleme geben soll.

Cloud-Computing liegt im Trend, doch für Arztpraxen gilt es – zumindest wenn es um Patientendaten geht – als zu risikobehaftet. Trotzdem arbeitet der Health-IT-Anbieter CompuGroup Medical (CGM) derzeit an einer „Medical Cloud“ für Arztpraxen und Ärztenetze und will dabei ein ganz besonderes Sicherheitsnetz bieten.

Dr. Adrian Spalka, Head of IT-Security bei der CompuGroup, gehört zu jenen, die immer wieder darauf aufmerksam machen, dass Ärzte in Sachen Online-Dienste und Auslagerung von Daten nicht nur an strengere Datenschutzregeln gebunden sind, sondern sich auch strafrechtlich verantworten müssen, wenn Patientendaten in falsche Hände geraten. „§ 203 des Strafgesetzbuches ist der große Spielverderber beim Outsourcen von Daten“, sagt Spalka. Der Paragraph ahndet die Verletzung von Privatgeheimnissen und besagt dabei auch ganz eindeutig, dass Ärzte, die persönliche Informationen von Patienten weitergeben mit einer Geldstrafe oder sogar einer Freiheitsstrafe von bis zu einem Jahr

rechnen müssen. Und die Cloud ist ja gerade dafür gedacht, Elemente der Praxis-IT outzusourcen, denn Cloud-Anbieter machen nichts anderes, als der Praxis IT-Ressourcen via Netzwerk zur Verfügung zu stellen. Programme, Rechenleistung, aber auch ganze Betriebssysteme ebenso wie Speicherplatz werden über solche Online-Netzwerke bereitgestellt. Die Daten liegen irgendwo auf Zentralservern und werden via Web abgelegt und aufgerufen.

Auf die Verschlüsselung kommt es an

Die Zusicherung von Rechenzentren, dass rein technisch Unbefugte keinen Zugriff auf die Daten hätten, reicht nach Ansicht von Spalka nicht, um die Anforderungen von § 203 „hinreichend zu erfüllen“. Alle Praxisdaten, die auf den Servern der Rechenzentren lagern, müssten auch so verschlüsselt werden, dass sie nur von einer Stelle einsehbar sind: dem Arzt oder zugriffsberechtigten Medizinischen Fachangestellten (MFA). Genau hier setzt das Konzept der Medi-

cal Cloud an. Alle Daten werden bereits in der Praxis verschlüsselt und dann erst in der Cloud abgelegt. CGM versichert dabei, dass die Verschlüsselung auch alle Anforderungen des Beschlagschutzes erfüllt – will heißen, dass sich die Daten nur mit dem Schlüssel des Arztes wieder in lesbare Form umwandeln lassen. Das Besondere dabei: Obwohl die Daten nicht in Klartext vorliegen, werden sie dennoch mit einem In-

Datenschutzregeln für Praxen

- **Bundesdatenschutzgesetz:** Werden Patientendaten anderen zugänglich, verstößt der Arzt damit gegen § 28 (Datenerhebung und -speicherung für eigene Geschäftszwecke)
- **Strafgesetzbuch:** Noch wichtiger ist § 203 StGB. Werden sensible Patienteninfos offengelegt, ist das eine Verletzung des Privatgeheimnisses. Und wird mit einer Geld- oder Freiheitsstrafe geahndet.

Rebekka Höhl