Mit Sicherheit gut behandelt.

Datenschutz in der Praxis # 10

Cloud-Computing

Immer häufiger werden einzelne Dienste oder gar ganze Praxisverwaltungssysteme (PVS) inkl. darin enthaltener Patientendaten als cloudbasierte Versionen angeboten. Dies bedeutet, dass in den Betrieb des PVS und der Datenverarbeitung Dienstleister eingebunden sind. Das klingt praktikabel, müssen doch nicht selbst Updates eingespielt oder andere Komponenten gepflegt werden. Im Vorfeld ist ein solcher Schritt allerdings gut vorzubereiten. Insbesondere die rechtlichen Voraussetzungen sind einzuhalten.

Was ist bei der Nutzung cloudbasierter Dienste zu beachten?
Die Inanspruchnahme von Cloud-Diensten durch Heilberufspraxen ist nach den Vorgaben des § 393 SGB V grundsätzlich zulässig. Der Maßstab ist dabei unabhängig von einer Kassenzulassung heranzuziehen (s.u.). Zudem gelten die bekannten Anforderungen der DS-GVO an eine Auftragsverarbeitung durch Dritte (siehe auch https://www.mit-sicherheit-gut-behandelt.de/digitale-arztpraxis/einsatz-von-dienstleistern)

Kommt jeder Anbieter in Betracht?
§ 393 SGB V stellt konkrete Anforderungen, die eingehalten werden müssen. Die Datenverarbeitung muss im Inland, in einem Mitgliedstaat der EU oder in einem diesem nach § 35 Absatz 7 SGB I gleichgestellten Staat stattfinden. Die datenverarbeitende Stelle muss über eine Niederlassung im Inland verfügen. Die von dem Dienstleister zum Schutz der Daten ergriffenen technisch-organisatorischen Maßnahmen müssen dem Stand der Technik entsprechen. Insbesondere verlangt das Gesetz das Vorliegen eines aktuellen C5-Testats (Typ-2) oder eines vergleichbaren Testats oder Zertifikats. Das C5-Testat ist ein unabhängiger Prüfbericht des BSI mit verbindlichen Anforderungen zu Informationssicherheit, Datenschutz und Compliance.

Weitere angemessene technische und organisatorische Maßnahmen sind insbesondere der Einsatz von Verschlüsselungstechnologien sowie das sog. Confidential Cloud-Computing. Die Datenschutzkonferenz hat im Jahr 2025 hierzu eine Entschließung veröffentlicht.

Chancen und Risiken
Die neue Rechtsgrundlage bietet insbesondere kleineren Praxen eine rechtssichere Möglichkeit, mit geringem technischen Aufwand ein modernes PVS betreiben zu können. Sind die rechtlichen und technischen Voraussetzungen auf beiden Seiten erfüllt, müssen noch die Vor- und Nachteile der hohen Abhängigkeit vom Anbieter und der Internetanbindung für die eigene Praxis in Erwägung gezogen werden.

Nützliche Links

https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Confidential_Cloud_Computing.pdf

Rechtsgrundlage

§ 393 Abs. 1 SGB V

(1) Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege eines Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind.

Art. 28 DS-GVO

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische u. organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags, (…) in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, (…) und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Eine Initiative von
Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz
KV RLP KASSENÄRZTLICHE VEREINIGUNG RHEINLAND-PFALZ
Landesärztekammer Rheinland-Pfalz
LPK RLP LandesPsychotherapeutenKammer Rheinland-Pfalz