Wirksamer Schutz von Patientendaten in der Cloud: Das Bayerische Krankenhausgesetz braucht ein Update

10.02.2021 – München: In Bayern ticken die Uhren oft ein wenig anders als im Rest der Bundesrepublik. Die föderale Struktur Deutschlands ist auch der Grund, weshalb wir Bayern einen Sonderweg in Sachen Datenschutz eingeschlagen haben. Ein folgenreicher Unterschied ist im Bayerischen Krankenhausgesetz (BayKrG) zu beobachten. Artikel 27 limitiert die Cloudnutzung für Krankenhäuser durch besonders strenge Richtlinien, um medizinische Patientendaten vor unberechtigtem Fremdzugriff zu schützen. So dürfen Drittanbieter nur dann für die Datenverarbeitung herangezogen werden, sofern das Krankenhaus die Schlüsselgewalt für die Daten wahrt und Weisungsbefugnis über die datenverarbeitenden Mitarbeiter des externen Dienstleisters erhält.

Der Artikel 27 des BayKrG zum Gewahrsam des Klinikums wurde Anfang der 1990er Jahre konzipiert. Ziel des Artikels war es, den „Kreis der Personen, die mit sensiblen medizinischen Daten in Berührung kommen, möglichst eng und die Qualifikation der betreffenden Personen möglichst hoch zu halten." Demnach dürfen medizinische Patientendaten, wie Untersuchungsbefunde oder Daten aus bildgebenden Verfahren, nicht außerhalb der dem Krankenhaus zugehörigen Räumlichkeiten verarbeitet oder archiviert werden. So soll der unrechtmäßige Zugriff auf diese Daten verhindert werden. Um Krankenhäusern die Cloudnutzung dennoch zu ermöglichen, braucht es Kunstgriffe: So werden beispielsweise externe Serverräume zum Krankenhausgelände deklariert. Doch der Zwang zu bürokratischen Pirouetten ist weder zeitgemäß, noch dient er dem Datenschutz.

Guter Ansatz, falsche Konsequenz

Niemand kann bestreiten, dass medizinische Patientendaten zu den sensibelsten und intimsten Informationen eines Menschen gehören. Deshalb ist es nur richtig, solche Daten durch besonders strikte Regeln vor Missbrauch zu schützen. Doch ist zu bezweifeln, dass die im Art. 27 BayKrG festgelegten Regelungen dem Test der Zeit standhalten oder den stetigen Weiterentwicklungen der Digitalisierung Rechnung tragen können.

Wenn also das Ziel der Gewahrsamspflicht von Kliniken ist, maximalen Datenschutz für Patientendaten zu gewährleisten, dann müssen die Daten jederzeit so geschützt sein, dass unberechtigter Zugriff nicht möglich ist. Die sicherste Lösung ist also, jeglichen Fremdzugriff technisch auszuschließen. Dies ist der zentrale Ansatz des Confidential Computing.

Confidential Computing garantiert Schlüsselgewalt für das Krankenhaus

Confidential Computing stellt sicher, dass der Cloud-Anbieter zu keinem Zeitpunkt Zugriff auf die in der Cloud gespeichert Daten hat – selbst während ihrer Verarbeitung. Somit können beispielsweise Röntgenbilder oder schriftliche Befunde ohne Gefahr zwischen Krankenhaus und einer externen Arztpraxis ausgetauscht werden.

uniscons Confidential Computing-Ansatz stellt mit rein technischen Mitteln sicher, dass die Daten selbst während der Verarbeitung weder für den Betreiber noch für Cyberkriminelle oder unbefugtes Personal einsehbar sind. Denn die Datenverarbeitung erfolgt auf physisch versiegelten Servern in speziell abgekapselten Segmenten.

Auf diese Weise ermöglicht der Cloud-Dienst idgard® das einfache Verwalten und Austauschen von Dokumenten und Daten jeden Typs und schützt medizinische Patientendaten mindestens so sicher wie ein vom Krankenhaus betriebener Server.

Hochsichere Cloud bietet besten Datenschutz und spart Betriebskosten

Das Dogma, medizinische Patientendaten auf dem Krankenhausgelände speichern zu müssen, ist aus der Zeit gefallen. Angefangen bei hohen Kosten für Anschaffung, Modernisierung sowie für Betrieb und Wartung. Hauseigene Server sind weder günstiger, noch garantieren sie höhere Datensicherheit als eine hochsichere Cloud. Cyberkriminelle scheren sich nicht um den Serverstandort, solange dieser mit dem Internet verbunden ist.

Ein dedizierter Cloud-Experte hat die notwendige Expertise, um Daten vor Fremdzugriffen effektiv zu schützen – jederzeit und DSGVO-konform, selbst während der Datenverarbeitung.
Am 01. Januar 2021 hat der deutschlandweite Rollout der Elektronischen Patientenakte begonnen. Die ePA ist jedoch kaum mit dem veralteten Regelwerk des BayKrG zu vereinbaren. Es wird Zeit für ein Update!

Weitere Beiträge rund um die Themen Datenschutz und Datensicherheit finden Sie unter www.privacyblog.de.

uniscon – Ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons *Sealed Platform®* bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.

uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).

Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten *Sealed Cloud Technologie*, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design“ entwickelt.

Uniscon wurde 2009 gegründet und ist seit 2017 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Pressekontakt
uniscon GmbH, Wilhelm Würmseer
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20