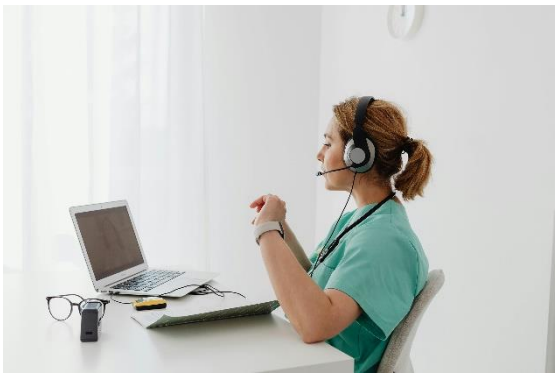
Consultix GmbH: Digitale Sprechstunde und internen Austausch im Gesundheitswesen sicher gestalten

Regelwerke wie der DSA (Digital Services Act) oder NIS2 (Network and Information Security 2) setzen die Gesundheitsbranche unter Druck. Die DSA ist bereits seit Mai 2024 in Kraft, NIS2 befindet sich in der finalen Phase. Beide Regelwerke stellen Einrichtungen im Gesundheitswesen vor regulatorische Veränderungen im IT- und Datenhandling. Online-Gesundheitsplattformen und -dienste, die Telemedizin und KRITIS-Einrichtungen wie Kliniken leiden besonders unter den neuen Standards für Datenschutz und Sicherheit. Dabei steht nicht nur der Schutz sensibler Patientendaten im Fokus, auch die eigenen Daten der Branchenteilnehmer – sprich die Gesamtheit ihrer Kommunikation.

Wie können Gesundheitsdienste also sicher kommunizieren? Muss dafür ein großer Aufwand erfolgen oder reicht für die Nutzung sicherer Tools ein kleiner Rechercheaufwand? Worauf müssen Health-Unternehmen Acht geben? Jörn Bittner, Senior Consultant bei Consultix, gibt Tipps.

Status quo

Krankenhäuser, Gesundheitszentren, Labore, Apotheken, Arztpraxen sowie Reha- und Pflegeeinrichtungen – sie alle kennen die schwierigen Bedingungen im Umgang mit Daten ihrer Branche. Doch bald schlägt mit NIS2 für Einrichtungen mit mindestens 50 Beschäftigten oder einem Jahresumsatz von mehr als 10 Mio. Euro die Stunde der aktuellen Cybersicherheit. „Zudem gilt weiterhin die DSGVO, wegen der viele Gesundheitseinrichtungen Sorge haben, gegen geltendes Recht zu verstoßen“, gibt Jörn Bittner, Senior Consultant bei Consultix, zu bedenken. Denn Gesundheitsdaten gehören zu der besonders geschützten Kategorie an Personendaten. Versorger im Health-Umfeld dürfen nur notwendige personenbezogene Daten erheben und verarbeiten, Mitarbeiter unterliegen der beruflichen Schweigepflicht und Akten von Patien:innen müssen vor unbefugtem Zugriff geschützt sein. Die Verarbeitung dieser Daten muss in einem nachvollziehbaren Verzeichnis erfolgen.



Dass diese zugegebenermaßen schwierigen Bedingungen tatsächlich zu horrenden Bußgeldern führen, zeigen immer wieder neue Beispiele aus Deutschland. 1 2024 verstieß beispielsweise ein Unternehmen der Gesundheitsbranche gegen Art. 6 Abs. 1 DSGVO, also die rechtmäßige Daten-verarbeitung, und wurde mit einem Bußgeld von

37.500 € belegt. Auch eine Apotheke erhielt einen Bußgeldbescheid von 6.500 € aufgrund von unsachgemäß entsorgten Daten in einem Raum, zu dem Fremde Zugriff hatten. Ärztinnen und Ärzte sowie Kliniken müssen immer wieder aufgrund solcher und ähnlicher Gegebenheiten enorme Summen zahlen.

Tools als Alltagshelfer

Die Digitalisierung kann helfen, rechtskonform mit Patient:innendaten umzugehen und auch die interne Kommunikation sicher zu gestalten. „Allerdings funktioniert das nicht mit den Platzhirschen am Markt – diese Anwendungen sind nicht DSGVO-konform und halten auch NIS2 nicht stand“, so Bittner. Einzelne Landesverwaltungen, wie die in Niedersachsen, gaben im vergangenen Jahr Microsoft-Anwendungen unter der Voraussetzung der EU-Boundary frei. Diese Vereinbarung sollte als Modell für andere Behörden oder Einrichtungen dienen, sofern eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt wird. Doch unter anderem Landesdatenschutzbehörden beäugen diese Entwicklung skeptisch. „Die EU-Boundary soll zwar Server in der EU bereitstellen, dennoch ist das Unternehmen immer noch in amerikanischer Hand und mit den jüngsten Entwicklungen auf der anderen Seite des Atlantiks entfernen sich Unternehmensstandards immer weiter von den Normen der EU“, fasst Bittner die aktuelle Situation zusammen. Zudem hatte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, abgekürzt DSK, bereits 2022 festgestellt, dass ein datenschutzkonformer Betrieb von Anwendungen dieser Unternehmen nicht möglich sei aufgrund mangelnder Transparenz und rechtswidriger Datenübermittlungen in Drittstaaten wie die USA. Diese Kritikpunkte wurden seither nicht vollständig ausgeräumt.

Von hier für hier

Die Wahl für oder gegen US-Software und IT-Strukturen der großen Hyperscaler betrifft auch das Gesundheitswesen. „Antwort auf die steigende Nachfrage nach DSGVO-konformem OnlineAustausch bieten europäische Lösungen wie Jitsi Meet oder Matrix Messenger Element, welche Videokonferenzen verschlüsseln, und Nextcloud für den Austausch von Dokumenten“, so der Kommunikationsexperte. Anbieter solcher Tools gehen auf individuelle Anforderungen von Gesundheitseinrichtungen ein und stellen dem Personal persönliche Berater zur Seite, die die Implementierung begleiten. Betrieben auf eigenen Servern in Deutschland, garantieren sie sichere digitale Meetings per Web-Browser oder Client auf allen Endgeräten – mit Lizenzverträgen von lokalen Dienstleistern sogar günstiger.

Über die Consultix GmbH

Die Consultix GmbH ist ein international agierender IT-Dienstleister mit Sitz in Bremen. Das inhabergeführte Unternehmen wurde 1994 gegründet, ist ISO 27001 zertifiziert und hat sich zum Technologieführer im Bereich Verwaltung und Management personenbezogener Daten entwickelt. Neben seinem Flaggschiff, dem Secure Customer Engagement Hub ProCampaign®, bietet die Consultix GmbH Dedicated Hosting, Private Cloud Services, Integration von Public Cloud Services, VMware-Services, Disaster-Recovery, Cyber-Sicherheit und DDoS Attack Mitigation an.
www.consultix.de