TÜV SÜD Management Service

Mehr Sicherheit. Mehr Wert.

ISO/IEC 27001 im Gesundheitswesen

IT- und Informationssicherheit mit System

Die Zeiten von Karteikarten und Krankenakten aus Papier sind auch im Gesundheitswesen vorbei – sollten sie zumindest. Die hohen Anforderungen an die Dokumentation und Prozesssteuerung sind mit den alten Mitteln nicht zu bewältigen. Die Digitalisierung verspricht hohe Effizienzsteigerungen etwa bei der elektronischen Übermittlung von Befunden und Laborergebnissen innerhalb des Unternehmens oder auch an weiterbehandelnde Einrichtungen. Für die Prozess-Steuerung im Krankenhaus oder der Arztpraxis ist es unabdingbar, alle relevanten Informationen datenschutzkonform zur richtigen Zeit am richtigen Ort zugänglich zu haben. Die Digitalisierung ist – auch im Gesundheitswesen – nicht aufzuhalten. Veraltete IT-Systeme stellen die Branche jedoch vor besondere Herausforderungen, denn Prozess- und Datensicherheit müssen stets gewährleistet sein. Andernfalls drohen nicht nur Haftungsrisiken, sondern auch Gefahren für Patienten. Ein zertifiziertes Informationssicherheits-Managementsystem (ISMS) auf Basis der ISO/IEC 27001 schafft die nötige Stabilität.

Gesundheitswesen rückt ins Visier von Cyberkriminellen

Krankenhäuser, Arztpraxen, Labore und Reha-Einrichtungen müssen Unmengen an Daten empfangen, verarbeiten, weiterleiten und langfristig speichern. Bei den meisten Daten handelt es sich um hochsensible Patientendaten, die erhöhten gesetzlichen Anforderungen an den Datenschutz gemäß Bundesdatenschutzgesetz (§§ 4a, 4d u. 28 BDSG) und die Datensicherheit unterliegen. Für Hacker sind solche Daten bares Geld wert. Das zeigen zahlreiche erpresserische Angriffe auf die IT-Systeme von Krankenhäusern, zum Beispiel auf ein städtisches Krankenhaus mit über 500 Betten in Nordrhein-Westfalen. Dort verschlüsselte ein als Anhang einer E-Mail verschickter Virus alle Daten. Ergebnis: Verschiebungen im OP-Plan sowie kostspielige Bereinigungsmaßnahmen. Immerhin waren die Patientendaten in einem sicheren Back-up gespeichert und wieder herstellbar. Ein Krankenhaus in Los Angeles sah sich hingegen gezwungen, Lösegeld zu zahlen, um eine Entschlüsselung seiner

Daten zu erreichen. Schädlinge, die sich in IT-Systeme einschleichen und Daten erst – wenn überhaupt – gegen ein Lösegeld wieder freigeben, werden fachsprachlich als Ransomware bezeichnet. Sie können einen geregelten Betrieb empfindlich stören oder sogar völlig lahmlegen.

Die Vorteile der ISO/IEC 27001

Als einer der Sektoren, in dem laut IT-Sicherheitsgesetz kritische Infrastrukturen betrieben werden, muss die Gesundheitsbranche hohe Sicherheitsmaßnahmen für ihre Informations- und Kommunikationsstrukturen umsetzen. Besonders geeignet: ein ISMS nach ISO/IEC 27001.
Die ISO/IEC 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme. Sie definiert die Forderungen für die Einführung, Umsetzung, Überwachung und Verbesserung eines Informationssicherheits-Managementsystems. Der Standard bietet einen systematischen und strukturierten Ansatz, der vertrauliche Daten schützt, die Integrität betrieblicher Daten sicherstellt und die Verfügbarkeit der IT-Systeme erhöht. Dank kontinuierlicher Überarbeitung auf Basis neuer Erkenntnisse und Entwicklungen wird die IT-Sicherheit laufend verbessert.

Die ISO/IEC 27001 sorgt in Unternehmen des Gesundheitswesens für:

- **Minimierte Risiken** – durch ein strukturiertes und weltweit anerkanntes Informationssicherheits-Managementsystem, das dabei unterstützt, Bedrohungen zu erkennen und Störungen zu reduzieren
- **Sicherheit der Daten** – durch Schutz vor Hackerangriffen, Datenverlust und Missbrauch vertraulicher Daten sowie Gewährleistung einer schnelleren Wiederherstellung nach Angriffen
- **Businesscontinuity** – durch ein geplantes Vorgehen im Schadensfall, damit Gesundheitseinrichtungen trotzdem weiterhin ihren Aufgaben nachkommen können

Warum TÜV SÜD?

Die erfahrenen, hoch qualifizierten Auditoren von TÜV SÜD verfügen über große Fachkenntnis und bewerten Informationssicherheits-Managementsysteme und andere Managementsysteme für die verschiedensten Branchen. Unser globales Expertennetzwerk bietet Ihnen weltweit Zertifizierungsdienstleistungen. Unsere Experten bieten Ihnen IT-Tests und Zertifizierungen nach den verschiedensten internationalen Normen und verfolgen dabei stets einen ganzheitlichen Ansatz. TÜV SÜD steht weltweit für Unabhängigkeit und Neutralität. Unser Prüfzeichen ist international anerkannt und geachtet und dadurch ein wichtiges Kommunikationsinstrument, das Ihr Unternehmen von der Konkurrenz abhebt.

Mehr Sicherheit. Mehr Wert.

TÜV SÜD ist ein Dienstleister in den Bereichen Prüfung, Begutachtung, Auditierung, Zertifizierung und Schulung und steht für Qualität, Sicherheit und Nachhaltigkeit. Wir sind an über 800 Standorten weltweit vertreten und verfügen über Akkreditierungen in Europa, Amerika, dem Nahen Osten, Asien und Afrika. Mit unseren neutralen und unabhängigen Lösungen schaffen wir echten Mehrwert für Unternehmen, Verbraucher und die Umwelt.

TÜV SÜD Management Service GmbH Ridlerstraße 65, 80339 München, Deutschland
Tel.: 0800 5791-5000 info@tms.tuev-sued.de www.tuev-sued.de/ms/iso-27001