Konformitätserklärung

zur IT-Sicherheitsrichtlinie § 75b SGB V

Was ist die § 75b SGB V?

Die Bestimmungen der IT-Sicherheitsrichtlinie gemäß § 75b SGB V legen die Standards für das Sicherheitsniveau der IT-Systeme in den Praxen von Medizinerinnen und Medizinern, Zahnärztinnen und Zahnärzten sowie Psychotherapeutinnen und Psychotherapeuten im Rahmen der gesetzlichen Versorgung fest.

Wozu bedarf es die § 75b SGB V?

Die Anforderungen dieser IT-Sicherheitsrichtlinie dienen dem Schutz der Patientendaten. Durch das stetige Fortschreiten der Digitalisierung stehen besonders Arztpraxen vor der Verantwortung, erhöhte Anforderung an die IT-Sicherheit zu gewährleisten. Insbesondere sensible Patientendaten und digitale Krankenakten sind vielfältigen Gefährdungen ausgesetzt. Damit Patientinnen und Patienten ihren Arztpraxen vertrauen können, müssen diese die Informationssicherheit vollumfänglich gewährleisten.

Wie setze ich die IT-Sicherheitsrichtlinie um?

Die Kassenärztlichen Bundesvereinigungen regelt die Anforderungen, welche in den Praxen erfüllt sein müssen, um die Verordnung § 75b SGB V umsetzen zu können. Dabei gelten einige Anforderungen für alle Praxen, andere Anforderungen richten sich nach Praxisgröße und Beschäftigungsanzahl. Die Anforderungen sind dabei nach Vorgabe des Gesetzestextes § 75b SGB V verbindlich durchzuführen, weshalb angeraten wird, die Erfüllung der Anforderungen in der Praxis zu dokumentieren. Im Falle von Haftungsfragen ist eine schriftliche Dokumentation der Vorgaben und Einhaltungen von großem Vorteil, um sich gegebenenfalls in einer juristischen Untersuchung entlasten zu können.

Für die grundlegende Umsetzung der Anforderungen sollte zunächst eine Bestandsaufnahme der vorhandenen IT-Komponenten (Hard- und Software) erfolgen inkl. der jeweiligen Zugangsberechtigungen. Darüber hinaus sollten alle wichtigen Prozesse dokumentiert werden, die im Praxisalltag Anwendung finden. Das hilft vor allen Dingen externen Dienstleistern, welche sich im Falle eines Notfalls schnell einlesen können, wie diese Geräte und Programme bedient werden und wo diese Daten gespeichert sind. Ebenfalls ist es wichtig, ein Rollen-, Rechtekonzept und Berechtigungskonzept zu erstellen und darin transparent festzulegen, welche Personen mit welchen Befugnissen auf bestimmte Systeme und Daten zugreifen dürfen.

Legen Sie für die grundlegende Umsetzung der Anforderungen in Voraus folgendes fest:

- Die Definition der Zuständigkeiten
- Die Abwägung, ob ein externer Dienstleister zur Unterstützung hinzugezogen werden soll
- Die zeitliche Organisation unter Berücksichtigung des laufenden Praxisbetriebs
- Die klare Zuteilung der Umsetzungsaufgaben und Ressourcenplanung (Zeit + Budget)
- Die Überlegung, ob zur Umsetzung notwendige Tools beschafft werden müssen
- Die Abstimmung mit externen Kontaktpersonen, die Verantwortlichkeiten im IT-Bereich tragen (z. B. die Pflege der Praxis-IT oder der Praxisverwaltungssysteme)

Generell gilt der Grundsatz, je aktueller die vorhandene Soft- und Hardware auf dem Stand der Technik ist, desto umfangreicher und besser ist der Schutz der Praxissysteme und Patientendaten.

Wir von OctoGate erklären hiermit, dass unsere Soft- und Hardware den aktuellen Sicherheitsanforderungen an die Telematikinfrastruktur entsprechen. Die von der Kassenärztlichen Bundesvereinigung gesetzten Anforderungen können folglich in Kombination mit den OctoGate Produkten in Arztpraxen umgesetzt und die IT-Sicherheitsrichtline § 75b SGB V somit gewährleistet werden.