Neue Anforderungen im technischen Datenschutz für kleinere Krankenhäuser

Dortmund, 10.09.2021: Im September 2020 wurde der neue § 75c in das Sozialgesetzbuch 5 (SGB V) aufgenommen. Damit sind auch Krankenhäuser, die bisher nicht die Regelungen zum Schutz kritischer Infrastrukturen (KRITIS) nach § 8a BSI-Gesetz anwenden müssen, ab dem 1. Januar 2022 gemäß § 75c Abs. 1 SGB V verpflichtet, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind“. Die IT-Systeme sind gemäß dieser Regelung spätestens alle zwei Jahre dem aktuellen Stand der Technik anzupassen.

Für Krankenhäuser, die bisher schon den KRITIS-Regelungen nach § 8a BSI-Gesetz unterliegen, entstehen keine neuen Verpflichtungen (vgl. § 75c Abs. 3 SGB V).

Diese neue Verpflichtung können die Krankenhäuser gemäß § 75c Abs. 2 SGB V insbesondere dadurch umsetzen, dass sie einen branchenspezifischen Sicherheitsstandard (B3S) für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden. Bislang musste dieser B3S nur von solchen Krankenhäusern nachgewiesen werden, die zur kritischen Infrastruktur (KRITIS) gehören.

Zur Unterstützung der Krankenhäuser wurde durch die Deutsche Krankenhausgesellschaft ein eigener B3S-Sicherheitsstandard entwickelt und vom BSI Mitte 2019 anerkannt. Hierbei ist nach aktuellem Stand der B3S für die Krankenhäuser die Mindestanforderung. Alternativ können gleichwertige Managementsysteme für Informationssicherheit (ISMS) zur Erfüllung der Nachweispflicht verwendet werden. Der B3S-Standard für Krankenhäuser wird derzeit überarbeitet.

Die Neuregelung in § 75c SGB V hat auch Auswirkung auf die Beurteilung des technisch-organisatorischen Datenschutzes von Krankenhäusern. Wenn § 26 KDG unter den dort genannten Bedingungen fordert, „geeignete technische und organisatorische Maßnahmen zu treffen“, dann legt der Gesetzgeber mit § 75c SGB V fest, welche Maßnahmen geeignet sind.

Den gleichen Effekt hat die Erwähnung der geeigneten technischen und organisatorischen Maßnahmen in § 11 Abs. 4 KDG für die Verarbeitung besonderer Kategorien personenbezogener Daten, hier also z.B. Gesundheitsdaten im Sinne des § 4 Nr. 17 KDG. Auch hier werden die durch § 75c SGB V aufgestellten Vorgaben zukünftig zu berücksichtigen sein.