SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Checkliste zur Prüfung der Cybersicherheit in medizinischen Einrichtungen

Mit der Entschließung „Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten“ vom 6. November 2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung auf die Problematik der Sicherheit zum Schutz der Patientendaten hingewiesen (siehe https://lsaurl.de/DSKKrankenhaeuser). Dabei sind vor allem die Vertraulichkeit und die Integrität der Patientendaten zu gewährleisten, was unter anderem auch gegen interne Bedrohungen schützt. Entgegen den Bestrebungen, zur vermeintlichen Effizienzsteigerung oder aus Kostengründen möglichst Viele auf möglichst Vieles im System zugreifen zu lassen, ist es geboten, durch differenzierte Rollen- und Berechtigungskonzepte den Zugriff auf Patientendaten auf das Nötigste zu reduzieren (siehe Grundsätze der Datenminimierung sowie der Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit. c) und f) Datenschutz-Grundverordnung (DS-GVO)).

Von besonderer Bedeutung ist insbesondere bei Krankenhäusern, dass die gebotene Verfügbarkeit der Daten in Gefahr gerät, wenn das Informationssystem keine hinreichende Cybersicherheit aufweist. Die Praxis hat gezeigt, dass Gesundheitsdatensätze von über 10.000 Patientinnen und Patienten im Internet offengelegt wurden. Dies macht die Notwendigkeit deutlich, die zumeist vernetzten Informationssysteme medizinischer Einrichtungen in nach der DS-GVO hinreichendem Maß durch technische und organisatorische Maßnahmen gegen Cyberangriffe zu schützen. Der Verantwortliche ist verpflichtet, nach dem Stand der Technik Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten zu treffen (siehe Art. 5 Abs. 1 lit. f), Art. 24 Abs. 1 und 2, Art. 32 DS-GVO). Die Maßnahmen müssen in angemessenem Verhältnis zu den Verarbeitungstätigkeiten stehen, wobei die Sensibilität der in der Regel betroffenen Gesundheitsdaten (siehe Art. 9 Abs. 1 DS-GVO) hohe Anforderungen begründet.

Es ist daher sinnvoll, die getroffenen Maßnahmen dahingehend zu überprüfen, ob sie den jeweiligen Anforderungen genügen. Anhaltspunkte hierfür gibt eine Checkliste zur Prüfung der Cybersicherheit in medizinischen Einrichtungen. Die darin aufgeführten Maßnahmen betreffen vor allem die Verfügbarkeit der Daten und sind nicht als abschließend zu betrachten. Die Checkliste soll dazu dienen, den effektiven Schutz gegen aktuelle Cybersicherheitsbedrohungen zu unterstützen. Aufgrund der unterschiedlichen Gegebenheiten in den medizinischen Einrichtungen muss nicht jede der aufgeführten Maßnahmen zwingend umgesetzt werden. Vielmehr soll in Abhängigkeit vom Umfang und den jeweiligen Umständen der Verarbeitung von Patientendaten ein angemessenes Schutzniveau erreicht werden.

Impressum
Herausgeber:
Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstraße 9
39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de

Stand: Juli 2020