

IT-Sicherheit: Neue Vorgaben im Anmarsch



Die zunehmende Vernetzung macht den Einsatz von IT-Systemen in den Arztpraxen schon lange erforderlich. Dabei steigen, auch durch die immer ernster werdende Bedrohungslage durch Cyber-Kriminelle, die Anforderungen an die IT-Sicherheit. Doch welche Anforderungen an die IT-Sicherheit sollte eine Arztpraxis erfüllen, um ihre Patienten- und Geschäftsdaten ausreichend zu sichern? Hierzu gab es bisher keine klaren Vorgaben und demnach viel Raum für Diskussionen.

Geschlossen werden soll diese Lücke nun durch eine neue Richtlinie der Kassenärztlichen Bundesvereinigung (KBV) zur IT-Sicherheit. Der durch das Digitale-Versorgung-Gesetz neu eingeführte § 75b SGB V verpflichtet Sie dazu. Hierbei muss der sogenannte „Stand der Technik“ umgesetzt werden. Diesen wiederum definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem IT-Grundschutz-Kompendium, einem Dokument von 820 Seiten Umfang, das jährlich neu editiert wird. Konsequenterweise muss die KBV deshalb ihre Richtlinie für die Vertragsärztinnen und -ärzte im Einvernehmen mit dem BSI erstellen. Dabei geht es nicht nur um technische Vorgaben, sondern auch um Dokumentationen, organisatorische Fragen und die Prozesse in der Praxis. Ziel ist es, die IT-Sicherheit kontinuierlich zu verbessern, wozu ein sogenanntes Informationssicherheitsmanagementsystem etabliert wird. Zur Zielerreichung arbeitet dieses in einem wiederkehrenden PDCA-Zyklus (Plan – Do – Check – Act). Neben der Richtlinie wird die KBV ferner Dienstleister zertifizieren, sodass eine einheitliche und verlässliche Qualifikation der IT-Berater gewährleistet werden kann.

HOHER ZUSATZAUFWAND IN DEN PRAXEN ABSEHBAR

So wichtig und sinnvoll die einzelnen Maßnahmen in den BSI IT-Grundschutzkatalogen sein mögen, so unklar ist, wie mit den absehbar daraus resultierenden Zusatzaufwänden bei Ihnen in der Praxis vor

Ort umgegangen werden soll. Auch sind die Formulierungen für fachliche Laien oft eher abstrakt und schwer zu verstehen. Die KBV versucht zurzeit, intern einen Kompromiss mit dem BMG und dem BSI zu finden. Es ist zu hoffen, dass die KBV-intern diskutierte Variante durchgesetzt werden kann. Allerdings steht zu befürchten, dass das BSI an seiner apodiktischen Position festhält. In diesem Fall wird der Praxisinhaber die Richtlinie nur unter fachkundiger Beratung eines (zertifizierten) IT-Dienstleisters umsetzen können. Ferner dürften oftmals auch Investitionen in Hard- und Software erforderlich sein. Aus Sicht der KV Hessen und der anderen KVen ist es unabdingbar, die Finanzierung dieser Vorgaben zu regeln und für einen Kostenausgleich zu sorgen. Beispiele für neue zusätzliche Kosten sind: Bestellung eines Informationssicherheitsbeauftragten, gegebenenfalls Umsetzung der baulichen Anforderungen und, falls IT-Systeme aus dem Consumerbereich eingesetzt werden (Fritzbox o. Ä.), müssten diese ergänzt oder ersetzt werden.

WIE GEHT ES NUN WEITER?

Nach dem Gesetz hätte die Richtlinie durch die KBV am 30. Juni 2020 in Kraft gesetzt werden müssen. Aufgrund der ungeklärten Finanzierungssituation und auch inhaltlich hat die KBV-Vertreterversammlung die Zustimmung zur Richtlinie verweigert und sämtliche KV-Vorstände haben sich in einem offenen Brief an das Bundesministerium für Gesundheit (BMG) gewandt (siehe S. 18), um eine praktikable

Regelung zu fordern. Das BMG hat in einer ersten Reaktion wenig Diskussionsbereitschaft erkennen lassen. Letztlich gibt es nun drei Szenarien:

1. Das BMG passt die gesetzliche Regelung nochmal an. Dies kann im Hinblick auf die Einbindung des BSI, aber auch in der Frage der Finanzierung erfolgen.
2. Das BMG schreitet zur Ersatzvornahme.
3. Es gibt noch einmal eine weitere Runde mit dem BMG und dem BSI auf der Basis eines neuen Entwurfs, der vorher von der KBV-VV abgesegnet werden müsste, für den beide, also BMG und BSI, erheblich zurückrudern müssten.

Sobald klar ist, wie es hier weitergeht, werden wir Sie natürlich umfassend informieren. ■

Markus Fritsch

Neue Vorgaben beachten

Lesen Sie auch den Artikel „IT sicher betreiben“ von Markus Fritsch in Heft 5/2018. Das IT-Grundschutzkompendium finden Sie unter

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

Infobox

Baustelle DMP Herzinsuffizienz

Kann das Disease-Management-Programm (DMP) Herzinsuffizienz abgerechnet werden? Wir informieren hier über den aktuellen Sachstand.

Zum jetzigen Zeitpunkt (Stand: 30. September 2020) ist eine Abrechnung des DMP Herzinsuffizienz (DMP HI) in Hessen noch nicht möglich, da es dazu keine vertragliche Vereinbarung gibt. Gemäß Anlage 13 der DMP-Anforderungs-Richtlinie für einen eventuellen Vertragsabschluss des DMP HI zwischen KV und den Verbänden der Krankenkassen und Ersatzkassen muss eine verpflichtende Patientenschulung konzipiert sein, die auch evaluiert und publiziert wird. So eine Patientenschulung liegt aber noch nicht vor. Am 18. Juni 2020 hat deshalb der Gemeinsame Bundesausschuss (G-BA) eine Änderung der Anlage 13 der DMP-Anforderungs-Richtlinie beschlossen. Fortan soll die Formulierung in „in der Regel evaluiert“ angepasst werden. Den Beschluss und die tragenden Gründe dafür finden Sie unter www.g-ba.de/beschluesse/4354

Durch diese Änderung kann das DMP HI auch mit einem noch nicht evaluierten Schulungsprogramm

geschlossen werden. In diesem Fall ist dem Bundesamt für Soziale Sicherung (BAS) ein entsprechendes Evaluationskonzept vorzulegen. Die Evaluation muss nach spätestens fünfeneinhalb Jahren in publizierter Form vorliegen. Der Beschluss wurde zwischenzeitlich vom Bundesgesundheitsministerium geprüft und nicht beanstandet und tritt somit zum 1. Oktober 2020 in Kraft. Zur weiteren Umsetzung steht die KV Hessen in Kontakt mit den hessischen Krankenkassenverbänden. ■



Sebastian Göbel