20.04.2021 Fachübergreifend

IT-Sicherheits-Richtlinie der KBV

P. Kalbe

Finanzieller Aufwand muss von den Krankenkassen erstattet werden

Die Bundesregierung treibt die Digitalisierung im Gesundheitswesen (und nicht nur dort) mit erheblichem Druck voran. Der zwangsweise Anschluss aller Arztpraxen an die Telematik-Infrastruktur (TI) hat bei vielen Vertragsärzten zu großem Verdruss geführt, zumal die Ärzte dabei jahrelang nur als kostenlose Dienstleister für den Stammdatenabgleich der Krankenkassen fungiert haben. Für das Jahr 2021 sind nunmehr weitere Funktionen der TI in der Pipeline, die wenigstens für die Patientinnen und Patienten (Notfalldaten-Management) und hoffentlich im Verlauf des Jahres auch durch die verbesserte innerärztliche Kommunikation (KIM-Dienste) einen gewissen Benefit versprechen.

Allerdings hat die zwangsweise elektronische Vernetzung der Ärzteschaft in einzelnen Praxen auch gravierende Sicherheitslücken in der Infrastruktur und Sicherheit der EDV-Anlagen und deren Anbindung offengelegt, die es Hackern ermöglichen würden, in die Praxissysteme einzudringen und sensible Patientendaten zu entwenden.

Insofern ist es grundsätzlich zu begrüßen, dass die KBV nach einem langen Diskussionsprozess nunmehr eine IT-Sicherheitsrichtlinie verabschiedet hat, deren Vorgaben alle Arztpraxen nach einer Übergangsfrist einzuhalten haben. Der Autor war als Delegierter der KBV-Vertreterversammlung in diesen Prozess eingebunden und kann bestätigen, dass diese – zweifellos immer noch sehr umfänglichen – technischen Vorgaben den besterreichbaren Kompromiss darstellen und dass eine erhebliche Verschlankung und pragmatische Anpassung gegenüber den ursprünglichen Forderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) erreicht werden konnte.

Abstufung des Sicherheitsaufwandes

Es war der Ärzteschaft besonders wichtig, den Umfang der vorgeschriebenen Maßnahmen an die Praxisgröße anzupassen. Dies ist nunmehr gelungen, indem drei Stufen definiert und der IT-Sicherheitsaufwand daran angepasst wurde:

- Praxis: Praxis mit bis zu 5 ständig mit der Datenverarbeitung betrauten Personen

- Mittlere Praxis: Praxis mit 6-20 ständig der Datenverarbeitung betrauten Personen
- Großpraxis mit Datenverarbeitung im erheblichen Umfang: Praxis mit mehr als 20 ständig mit der Datenverarbeitung betrauten Personen oder mit komplexen EDV-Strukturen

Gestufte Umsetzung mit Fristen bis 2022

Darüber hinaus konnte eine gewisse zeitliche Streckung der Umsetzung bis zum 01.01.2022 erreicht werden. Trotzdem sollte man als Praxis-Inhaber ohne Verzögerung daran gehen, die Anbindung der Praxis an das Internet zu überprüfen und notwendige Änderungen/Ergänzungen in Auftrag zu geben, zumal zahlreiche Vorgaben schon bis zum 01.04.2021 umzusetzen sind. Dies dürfte in den meisten Fällen die Einbeziehung von IT-Experten erfordern, für welche die KBV darüber hinaus ein Zertifizierungsverfahren anbietet. Dies ist zwar nicht obligatorisch, bietet aber dem Auftraggeber eine gewisse Sicherheit, dass der externe Dienstleister zumindest weiß, worum es geht.

Bei aller verständlichen Unzufriedenheit über diese erneute zusätzliche Belastung der Praxen ist zu berücksichtigen, dass es sich um die Umsetzung einer gesetzlichen Verpflichtung (§ 75b SGB V) handelt und dass damit auch die Anforderungen der Datenschutzgrundverordnung gewährleistet werden.

Kosten und Refinanzierung

Es steht außer Frage, dass die Umsetzung der Vorgaben aus der IT-Sicherheitsrichtlinie mit erheblichen Investitionen und darüber hinaus mit laufenden Kosten für die Praxen verbunden ist. Deren Höhe ist abhängig von der Praxis-Größe und der bereits vorhandenen IT-Infrastruktur.

Bisher sind in der Refinanzierung der Telematik-Infrastruktur nur die zusätzlichen Kosten für den Konnektor, die Kartenlesegeräte und die Installation berücksichtigt. Die KBV und die Berufsverbände fordern einhellig, dass den Praxen auch die zusätzlichen Kosten für die in der Richtlinie vorgeschriebenen Sicherheitsmaßnahmen von den Krankenkassen erstattet werden müssen. Diese Forderung wird von der KBV in den Bewertungsausschuss eingebracht.

Konsequenzen für die niedergelassenen Chirurgen

Alle chirurgischen Praxen sollten Kontakt mit ihrem IT-Dienstleister aufnehmen und gemeinsam die IT-Sicherheitsrichtlinie als Checkliste abarbeiten. Sofern bestimmte dort empfohlene Maßnahmen unter Bezug auf die individuelle Praxisstruktur für nicht erforderlich gehalten werden, sollte dies mit einer Begründung schriftlich fixiert werden. Eine Beratung bieten neben den Softwareherstellern oft auch lokale IT-Dienstleister. Die Angebote sollten nach Leistungsumfang und Kosten verglichen werden.

Eine kompetente Beratung zur IT-Sicherheit und zu speziellen Versicherungslösungen bietet auch unser Kooperationspartner Ecclesia-med: https://www.ecclesiamed.de/news/news-details/news/cyberrisiken/

Darüber rät Ihnen Ihr Berufsverband dringend, Ihren elektronischen Arztausweis zu beantragen, sofern dies noch nicht geschehen ist. Dazu rufen Sie bitte die entsprechende Homepage einer der bisher zugelassenen Dienstleister auf:

- Bundesdruckerei
- Medisign
- T – Systems
- SHC Stolle & Heinz Consultants

Bei weiteren Fragen wenden Sie sich bitte an die IT-Beratung Ihrer kassenärztlichen Vereinigung oder an Ihren Berufsverband.

Kalbe P: IT-Sicherheits-Richtlinie der KBV. Passion Chirurgie. 2021 Mai; 11(05): Artikel 03_04.

Autor des Artikels

Dr. med. Peter Kalbe

Vizepräsident des BDC
Gelenkzentrum Schaumburg
Stükenstraße 3
31737 Rinteln
› kontaktieren