KVB
Kassenärztliche Vereinigung Bayerns

FAQs - IT-Sicherheitsrichtlinie

Version 2.0, Stand: 07.04.2025

Inhalt

I. IT-Sicherheitsrichtlinie

1. Warum bedarf es der Richtlinie?

Zur Konkretisierung der abstrakten Europäischen Datenschutzgrundverordnung (DSGVO) hat der Gesetzgeber einheitliche und verbindliche Vorgaben für Praxen in einer Richtlinie gefordert. Deshalb wurde die Kassenärztliche Bundesvereinigung nach § 390 SGB V (ehemals § 75b SGB V) beauftragt, die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln.

2. Welchen Nutzen hat meine Praxis durch die Erfüllung der Maßnahmen?

In der IT-Sicherheitsrichtlinie werden Mindestmaßnahmen genannt, die Ihrer Praxis dabei helfen sollen, Risiken der IT-Sicherheit zu minimieren und IT-Systeme und sensible Praxisdaten bestmöglich zu schützen. Durch die klaren Vorgaben zur sicheren Verwaltung von Patientendaten und zur Risikominimierung kann die Sicherheit Ihrer sensiblen Daten gewährleistet werden.

3. Gilt die IT-Sicherheitsrichtlinie nur für diejenigen Praxen, die an die Telematikinfrastruktur (TI) angebunden sind?

Nein. Die Richtlinie ist unabhängig davon, ob eine Praxis an die TI angebunden ist oder nicht, verbindlich für alle Einrichtungen im ambulanten Sektor.

4. Sind Praxen dazu verpflichtet, einen externen Dienstleister zur Unterstützung bei der Umsetzung der IT-Sicherheitsrichtlinie zu beauftragen?

Praxen sind nicht verpflichtet, einen zertifizierten IT-Dienstleister zur Unterstützung bei der Umsetzung der IT-Sicherheitsrichtlinie zu beauftragen. Sollten sie die Richtlinien-Erfüllung auch ohne externe Unterstützung umsetzen können, ist ihnen das freigestellt; ebenso können sie einen externen Dienstleister einsetzen, der keine Zertifizierung gemäß § 390 Abs. 7 SGB V (ehemals § 75b Abs. 5 SGB V) hat.
Bitte beauftragen Sie dann einen (zertifizierten) Anbieter, wenn Sie Zweifel haben, ob Sie die Anforderungen allein bzw. mit Ihren vorhandenen Fachkräften (z.B. Systemadministratoren) erfüllen können.

5. Wo und wie finde ich einen zertifizierten Dienstleister?

Sollten Sie einen zertifizierten IT-Dienstleister zur Umsetzung der IT-Sicherheitsanforderungen in Ihrer Praxis beauftragen wollen, finden Sie eine Liste der erfolgreich Zertifizierten auf der Homepage der KBV. Auf unserer Themenseite finden Sie den entsprechenden Link dazu (Themenseite "IT-Sicherheitsrichtlinie" der KVB-Website).

6. Können sich Praxen zertifizieren/verifizieren und prüfen lassen, ob sie alle Anforderungen zur IT-Sicherheitsrichtlinie erfüllt haben?

Jeder Praxisinhaber ist für die Einhaltung der Anforderungen selbst verantwortlich. Derzeit sind seitens der KBV keine Zertifizierungen oder Verifizierungen zur Einhaltung der IT-Sicherheitsrichtlinie in Praxen geplant.

7. Muss ich der KV gegenüber nachweisen, dass ich die Anforderungen erfüllt habe?

Eine Nachweispflicht ist gesetzlich nicht vorgesehen. Es empfiehlt sich, zumindest eine interne Dokumentation über die Maßnahmenumsetzung und -kontrolle zu führen.

8. Was passiert, wenn ich gewisse Anforderungen nicht erfülle?

Die Anforderungen zur Gewährleistung der IT-Sicherheit schützen die sensiblen Daten Ihrer Praxis. Sollten Sie gewisse Anforderungen nicht erfüllen, ist kein vollständiger Schutz mehr in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit Ihrer IT-Systeme gewährleistet.

9. Wie ist die Definition "ständig mit der Datenverarbeitung betraute Person" zu verstehen? Müssen Auszubildende in die Anzahl eingerechnet werden?

Die Ausgestaltung der Regelung liegt im Ermessen der jeweiligen Arztpraxis. Sie wurde bewusst nicht abschließend definiert. Die Passage ist angelehnt an die entsprechenden Regelungen des Bundesdatenschutzgesetzes.

10. Können Praxisgemeinschaften, die ein Netzwerk gemeinsam nutzen, gewisse Anforderungen zusammen erfüllen?

Eine Praxisgemeinschaft gilt im Sinne der IT-Sicherheitsrichtlinie nicht als Einheit. Jede Praxis mit eigener Betriebsstättennummer ist für die Einhaltung und Dokumentation der Richtlinie selbst zuständig.
Hintergrund: Die IT-Sicherheitsrichtlinie enthält Anforderungen zu unterschiedlichen Aspekten der IT-Sicherheit – hier geht es also weit über reine Netzwerk-Komponenten hinaus. Beispielsweise werden Maßnahmen in Bezug auf Sensibilisierung von Mitarbeitenden, Office-Produkte, Internet-Anwendungen und mobile Anwendungen (Apps) ebenso adressiert wie Mobiltelefone, Smartphones und Endgeräte.
Da es bei der gemeinsamen Nutzung einer einheitlichen technischen Infrastruktur für jeden „Mandanten“ möglich und sinnvoll ist, eigene Festlegungen für konkrete IT-Sicherheitsvorkehrungen zu treffen, muss die IT-Sicherheitsrichtlinie auch von jeder Praxiseinheit persönlich angewendet und erfüllt werden.

11. Was ist mit „Dienstleistern vor Ort" gemeint?

Laut herkömmlicher Definition sind Dienstleister vor Ort (DVOs) „natürliche Personen.“ Es handelt sich also um externe Dienstleister, die Praxen unterstützen – nicht um interne System- oder Netzwerkadministratoren.

12. Können die Kosten zur Erfüllung der Anforderungen an die IT-Sicherheitsrichtlinie erstattet werden?

Viele der in der IT-Sicherheitsrichtlinie aufgeführten Anforderungen werden im Praxisalltag bereits angewendet, da sie durch die seit längerer Zeit geltenden Hinweise und Empfehlungen oder auch durch die DSGVO vorgegeben sind. Zur Erfüllung der Vorgaben gemäß DSGVO und der „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ wurde auch keine Erstattung anfallender Kosten vereinbart. Die Erfüllung der Anforderungen aus der IT-Sicherheitsrichtlinie dient der Gewährleistung der eigenen Praxis-IT-Sicherheit.

13. Ist eine Hardware-Firewall (UTM Firewall, etc.) nach der "Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit" verpflichtend vorgeschrieben?

In Anlage 5 Nr. 4 in Verbindung mit Anlage 1 Nr. 11 wird gefordert, die Praxis bzw. das Praxisnetz auf Netzebene zu schützen. Die KBV empfiehlt dies mittels einer korrekt installierten, konfigurierten und gewarteten Hardware-Firewall oder mittels eines Konnektors im Reihenbetrieb umzusetzen.

14. Müssen Netzwerkadministratoren die Anforderungen zur IT-Sicherheitsrichtlinie erfüllen?

Externe Dienstleister können die Zertifizierung gemäß § 390 Abs. 7 SGB V (ehemals § 75b Abs. 5 SGB V) erlangen – sie müssen es aber nicht zwingend tun. Interne Netzwerkadministratoren müssen sich nicht zertifizieren lassen.

15. Oft gibt es kein Diensthandy, aber die Mitarbeitenden nutzen ihre privaten Handys im Praxisnetz. Welche Maßnahmen sind hierfür empfehlenswert?

Es empfiehlt sich als technische Maßnahmen eine Netztrennung, durch welche die Privatgeräte (von z. B. Mitarbeitenden oder Patienten) einen vom vertraulichen Praxisnetz getrennten Zugriff zum Internet erhalten. Als organisatorische Maßnahmen empfehlen sich zudem Nutzungsbedingungen und eine entsprechende Datenschutzerklärung.

16. Warum wurde die Verschlüsselung von Speichermedien nicht schon in der Anlage 1 festgelegt?

Es ist jeder Praxis(größe) freigestellt, Anforderungen umzusetzen, die gemäß der Richtlinie größeren Praxen zugeordnet sind.

17. Wer erstellt den in der IT-Sicherheitsrichtlinie geforderten Netzwerkplan?

Der Praxisinhaber ist für die Erstellung verantwortlich, kann diese jedoch auch delegieren.

18. Sind Ultraschallgeräte auch medizinische Großgeräte?

Aktuell ist dieser Begriff bewusst offen formuliert. Hierdurch verbleibt dem Praxisinhaber Interpretationsspielraum. (IT-) Sicherheitsmaßnahmen können auch unabhängig von der Einstufung als "medizinisches Großgerät" umgesetzt werden.

19. Ist die Revisionssicherheit (bspw. Im Kontext eines Praxisarchivs) verpflichtend?

In der IT-Sicherheitsrichtlinie werden dazu keine Anforderungen festgelegt, dies geschieht an anderer Stelle.
Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht (vgl. § 10 Abs. 3 MBO-Ä, § 630f Abs. 3 BGB sowie für den vertragsärztlichen Bereich § 57 Abs. 2 BMV-Ä). Bewahrt der Arzt die Patientenakte nicht bis zum Ende der Aufbewahrungsfrist auf, trifft ihn in einem möglichen Arzthaftungsprozess gegebenenfalls die Pflicht zu beweisen, die medizinisch gebotenen Maßnahmen tatsächlich getroffen zu haben. Zu beachten sind zudem die zivilrechtlichen Verjährungsfristen, die etwa für einen Schadensersatzanspruch eines Patienten wegen eines Behandlungsfehlers des Arztes gelten.

20. Dürfen Patientendaten (Name, Tel. Nr.) auf dem Praxishandy in „Kontakten“ gespeichert werden, da sie zum Terminmanagement über SMS oder Apps (Signal) benötigt werden?

Jede Verwendung von personenbezogenen Daten muss begründet (Zweckbindung) und in einem "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Dies schließt auch die einzuhaltenden Löschfristen mit ein. Ein Beispiel für solch ein Verzeichnis und eine Ausfüllhilfe dazu gibt es auf den Seiten der KBV unter https://www.kbv.de/html/datensicherheit.php.
Im konkreten angesprochenen Fall sollte zudem darauf geachtet werden, dass die Praxishandys keine Kontaktsynchronisation in die Cloud vornehmen.