

Neue KBV IT-Sicherheitsrichtlinie: Was Ärzt:innen und Praxen wissen müssen

Zum 1. Oktober 2025 müssen die neuen Anforderungen der aktualisierten KBV IT-Sicherheitsrichtlinie umgesetzt sein. Die Richtlinie trat bereits am 1. April 2025 in Kraft und soll Praxen noch besser vor Cyberbedrohungen schützen. Ziel der Überarbeitung ist es, sensible Patientendaten durch verstärkte Sicherheitsmaßnahmen und bessere Sensibilisierung des Praxispersonals zu schützen.

Wen betrifft die IT-Sicherheitsrichtlinie?

Die IT-Sicherheitsrichtlinie richtet sich an alle niedergelassenen Ärzt:innen und Psychotherapeuten in der vertragsärztlichen Versorgung. Dabei gelten unterschiedliche Anforderungen je nach Praxisgröße:

- **Kleine Praxen:** bis zu 5 Personen mit Datenverarbeitung
- **Mittlere Praxen:** 6 bis 20 Personen mit Datenverarbeitung
- **Große Praxen:** über 20 Personen oder bei besonderer Datenverarbeitung sowie Praxen mit Großgeräten: CT, MRT, PET, Linearbeschleuniger etc.

Wichtig: Ob Voll- oder Teilzeitmitarbeiter ist dabei irrelevant. Jeder Mitarbeiter zählt als eine Person.

FAQ: Ihre Fragen – unsere Antworten

1. Warum wurde die IT-Sicherheitsrichtlinie aktualisiert?

Medizinische Einrichtungen sind zunehmend Ziel von Hacker-Angriffen und die Bandbreite der Angriffsmethoden wächst stetig. Durch das Digital-Gesetz wurden außerdem neue gesetzliche Anforderungen eingeführt, insbesondere zur Sensibilisierung von Mitarbeitern für Informationssicherheit.

2. Was sind die wichtigsten Neuerungen?

Die Hauptneuerungen betreffen das Praxispersonal: Es muss regelmäßig zur IT-Sicherheit geschult und für Informationssicherheit sensibilisiert werden. Zusätzlich wurden Vorgaben für E-Mail-Sicherheit (z. B. Phishing), Patchmanagement (Software muss immer durch die aktuelle Version auf dem neuesten Stand sein) und Cloud-Anwendungen verschärft.

3. Bis wann müssen die neuen Vorgaben umgesetzt werden?

Die neuen Anforderungen sind spätestens ab 1. Oktober 2025 umzusetzen, ein halbes Jahr nach Inkrafttreten der aktualisierten Richtlinie. Alle bestehenden Anforderungen aus der Richtlinie von 2021 gelten weiterhin. Es gibt auch keine Übergangsfrist. Das bedeutet, dass Sie ab dem 1. Oktober alle technischen und organisatorischen Anforderungen erfüllen müssen. ABER: Sofern Sie ein Schulungskonzept haben, müssen noch nicht alle Schulungen zum 1. Oktober erfolgt sein. Hier können Sie die Schulungen entsprechend Ihres Konzeptes auch nach dem Stichtag durchführen.

4. Wie müssen Mitarbeiter geschult werden?

Das Praxispersonal muss regelmäßig zur Informationssicherheit geschult werden, soweit

dies für die Arbeit relevant ist. Die Form der Schulung bleibt der Praxisleitung überlassen – ob durch interne Schulungen, E-Learning oder externe Fortbildungen.

5. **Was gilt für E-Mail-Sicherheit?**

Die Richtlinie fordert klare Verhaltensregeln für den E-Mail-Umgang, insbesondere zum Schutz vor Phishing-Attacken und Spam. E-Mail-Clients und -Server müssen sicher konfiguriert werden.

6. **Was passiert bei Cloud-Anwendungen?**

Seit dem Digital-Gesetz 2024 dürfen Gesundheits- und Sozialdaten nur noch unter besonderen Sicherheitsanforderungen in der Cloud verarbeitet werden. Nur Cloud-Dienste von Anbietern mit C5-Testat des BSI sind zulässig. Hier müssen Sie als Arztpraxis prüfen, ob Ihre Dienstleister dies erfüllen.

7. **Was passiert bei Nichteinhaltung?**

Im § 390 SGB V werden keine möglichen Sanktionen thematisiert. Bei tatsächlichen Datenschutzvorfällen und einer Nichteinhaltung der IT-Sicherheitsrichtlinie können datenschutzrechtliche Konsequenzen im Sinne der DSGVO drohen. Honorarkürzungen oder Bußgelder der KV gehören hier allerdings nicht dazu.

8. **Was ändert sich sonst noch für kleine, mittlere oder große Praxen?**

Alle Praxen müssen folgende (neue) Anforderungen erfüllen:

- a. Mitarbeiterregelungen
- b. Patchmanagement
- c. Endgerätesicherheit/Datensicherungen
- d. E-Mail- und Serversicherheit
- e. Sicherheit der Website
- f. Cloudanwendungen nur bei C5-Testat
- g. Zusätzliche Schutzpflichten bei Internetzugang neben TI-Anbindung

Darüber hinaus treffen große Praxen noch folgende neuen Anforderungen:

- a. Lernerfolge der Mitarbeiterschulungen müssen ausgewertet werden
- b. Netzwerksicherheit muss erhöht werden
- c. Berechtigungskonzepte und Regelungen zu mobilen Geräten
- d. Erhöhte Regelungen zu E-Mail- und Serversicherheit

9. **Was müssen Mitarbeiter konkret erfüllen und worauf müssen sie geschult werden?**

- a. Die Pflichten zu Mitarbeitern treffen alle Praxisgrößen.
- b. Verschwiegenheitserklärungen unterzeichnen
- c. In die Praxis-IT sowie alle zugehörigen Sicherheitsrichtlinien einweisen
- d. Es muss ein Prozess für den Austritt von Mitarbeitern vorhanden sein (u. a. Entzug von Zugangsberechtigungen und Schlüsseln, ggf. Passwörter ändern bei gleichem Zugang für mehrere Personen).
- e. Es müssen betriebliche Regelungen eingeführt werden, um regelmäßige Schulungen zu gewährleisten.
- f. Es müssen Schulungen zum Umgang mit Phishing-Mails/Spam-Mails durchgeführt werden.

- g. Die Form der Schulung ist offen. Sie können Ihre Mitarbeiter selbst schulen, Online-Kurse buchen oder die teilweise kostenlosen Schulungen der KV/KBV nutzen.

10. Was muss Fremdpersonal erfüllen?

- a. Vertraulichkeitsverpflichtung wie Mitarbeiter unterzeichnen
- b. Einmalige Dienstleister nur unter Aufsicht in sensible Bereiche lassen
- c. Bei Beendigung zu Rückgabe aller Informationen und Unterlagen auffordern

11. Gibt es eine Fortbildung mit allen wichtigen Infos zur neuen Sicherheitsrichtlinie?

Ja. Das Institut für Hausärztliche Fortbildung (IHF) bietet am 10. September 2025 von 15:30 - 17:00 Uhr ein Online-Webseminar „Cyberangriffe & KV-Sicherheitsrichtlinie: Pflichtwissen“ an. Melden Sie sich zusammen mit Ihrem Praxisteam direkt an: aerzte.ihf-fortbildung.de

12. Ich kann an der IHF-Fortbildung nicht teilnehmen. Wo kann ich mich informieren und wie muss ich handeln?

Die KBV stellt auf ihrer Website Schulungsunterlagen für MFA und niedergelassene Ärzt:innen als PDF zur Verfügung (kbv.de). Gehen Sie mit allen inhaltlichen Rückfragen und zur Umsetzung der technischen Anforderungen direkt auf Ihren persönlichen IT-Dienstleister zu. Unten stellen wir Ihnen für weitere Informationen hilfreiche Quellen bereit.

13. Wo finde ich weiterführende Informationen oder Unterlagen?

- a. Allgemeines zur KBV IT-Sicherheitsrichtlinie: kbv.de
- b. KBV-Fortbildungsinhalte für MFA und Niedergelassene als PDF: kbv.de
- c. KBV-Hub mit Musterdokumenten und FAQs: kbv.de
- d. Übersicht zertifizierte IT-Dienstleister: kbv.de
- e. Bundesamt für Sicherheit in der Informationstechnik (BSI): bsi.bund.de