KBV
KASSENÄRZTLICHE
BUNDESVEREINIGUNG

IT-SICHERHEIT IN DER PRAXIS
SICHERHEITSRICHTLINIE NACH § 75 B SGB V

INFORMATIONSVERANSTALTUNG DER KV BERLIN AM 12.03.2021

Motivation für IT-Sicherheit in der Praxis

- Patienten vertrauen Praxen besonders schutzbedürftige Informationen an

- Bereits jetzt existieren empfindliche Strafen bei Datenschutzverstößen oder Verletzung der Schweigepflicht (§ 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, § 203 Strafgesetzbuch)

- Zur Konkretisierung der abstrakten Anforderungen der DSGVO hat der Gesetzgeber einheitliche und verbindliche Vorgaben für Praxen in einer zu erstellenden Richtlinie gefordert:
  → Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

- ↗ **EINLEITUNG**
- ↗ **§ 75B SGB V**
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
  - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ **ABSCHLUSS**

Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

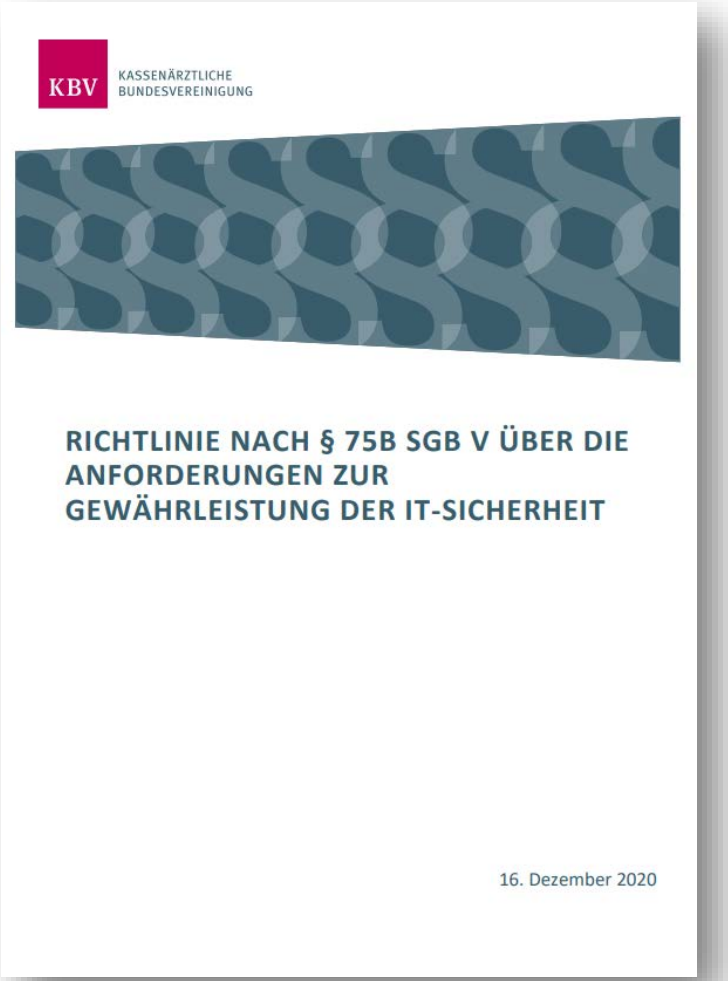
› Es gibt zwei Richtlinien für unterschiedliche Aspekte:

1. **Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit**
   Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich anzupassen. Die Richtlinie ist für die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich.

2. **Zertifizierung vertrauenswürdiger Dienstleister**
   IT-Dienstleister können sich auf Basis der o. g. Richtlinie bei der KBV zertifizieren lassen und ihre Kompetenz gegenüber Dritten mittels des ausgestellten Zertifikates vorweisen.

1. Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

- Beschreibt das Mindestmaß der zu ergreifenden Maßnahmen für IT-Sicherheit
- Gilt für vertragsärztliche bzw. vertragspsychotherapeutische Praxen
- Praxisinhaber sind für die Einhaltung der Anforderungen verantwortlich



Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit – Anlagen

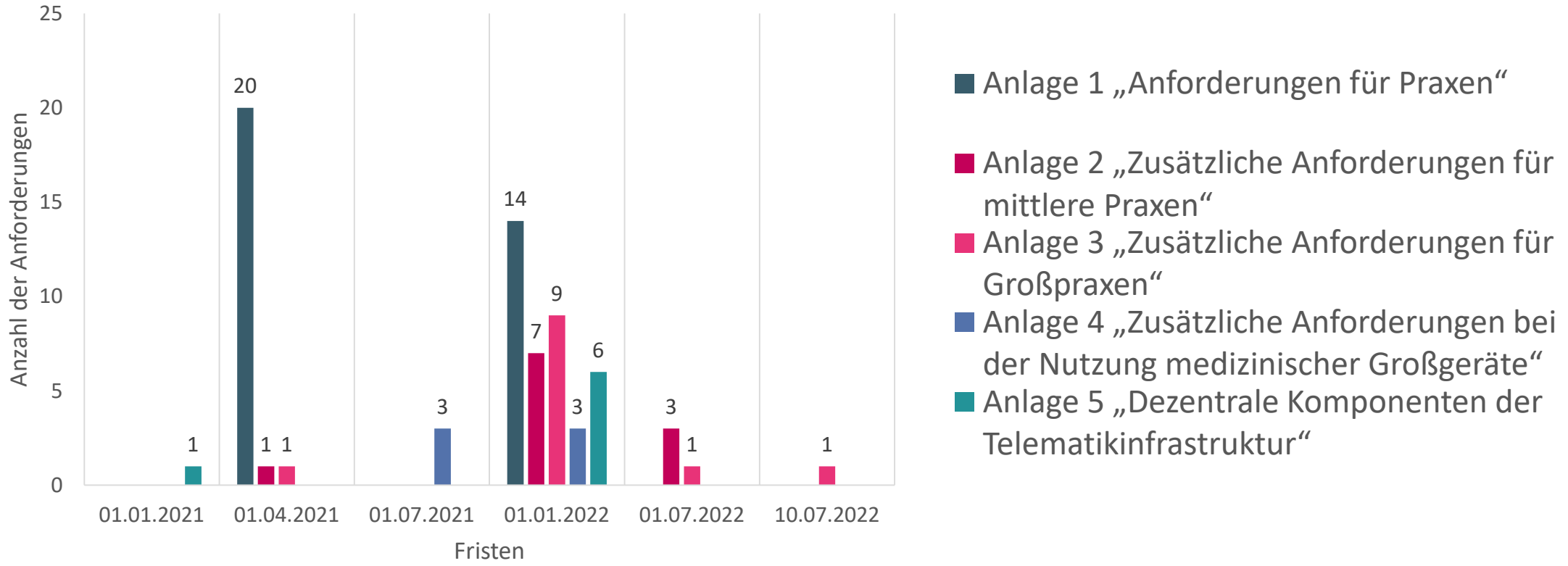
- Anforderungen sind gestaffelt nach stattfindender Datenverarbeitung bzw. Praxistyp:
  - Anlage 1 „Anforderungen für Praxen“
  - Anlage 2 „Zusätzliche Anforderungen für mittlere Praxen“
  - Anlage 3 „Zusätzliche Anforderungen für Großpraxen“
- Bei Einsatz medizinischer Großgeräte müssen (unabhängig vom Praxistyp) die Anforderungen der Anlage 4 „Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte“ erfüllt werden
- Anforderungen der Anlage 5 „Dezentrale Komponenten der Telematikinfrastruktur“ müssen immer (unabhängig vom Praxistyp) erfüllt werden

Tipp

→ Viele der Anforderungen können in den Vertragsbedingungen mit Dritten (z. B. IT-Dienstleistern, die den Betrieb von Software oder Infrastruktur übernehmen) genutzt werden.

Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit – Anlagen

› Pro Anforderung einer Anlage sind unterschiedliche Fristen zu beachten:



- ↗ **EINLEITUNG**
- ↗ **§ 75B SGB V**
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
  - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ **ABSCHLUSS**

Die Praxis als Patient

- **Idee**
  Die Praxis wird mit einem Patienten verglichen, dem mit Hilfe von IT-Sicherheitsmaßnahmen geholfen werden kann.

- **Beispielsituation**
  Die Praxis wird beim Arzt vorstellig: Ihr geht es nicht gut. Sie ist in absehbarer Lebensgefahr und ihr muss dringend geholfen werden. Nach einem ersten Gespräch stellt sich heraus, dass die akute Symptomatik auf einer chronischen Krankheit beruht. Der Praxis kann durch geeignete, dauerhafte Therapie ein Leben in Normalität ermöglicht werden.

Die Praxis als Patient – Umsetzung § 75b SGB V

1. **Anamnese:** Praxistyp festlegen
2. **Diagnose:** Anzuwendende Anlagen festlegen
3. **Behandlungsplan:** Anzuwendende Anforderungspunkte festlegen
4. **Therapie:** Maßnahmen festlegen und umsetzen
5. **Mitbehandlung:** Dienstleister beauftragen/anweisen
6. **Verlaufskontrolle:** Anforderungsumsetzung prüfen
7. **Folgetermin:** auf Änderungen reagieren

→ Die hier aufgelisteten Schritte werden auf den folgenden Seiten den Umsetzungsschritten der Richtlinie nach § 75b SGB V und mit dem Symbol rechts oben gekennzeichnet.

- ↗ **EINLEITUNG**
- ↗ **GESETZLICHE RAHMENBEDINGUNGEN**
  - ↗ ÄRZTLICHE SCHWEIGEPFLICHT
  - ↗ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)
- ↗ **§ 75B SGB V**
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
      - ↗ VORBEREITUNG
      - ↗ HILFESTELLUNGEN ZUR DURCHFÜHRUNG
      - ↗ NACHBEREITUNG
    - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ **ABSCHLUSS**

Praxistyp auswählen

Praxistyp	Definition
 Praxis	Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen
 Mittlere Praxis	Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen
 Großpraxis	Eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichem Umfang ist eine Praxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore).

Anlagen auswählen

› Anlagen 1, 2 und 3 korrelieren mit der Praxisgröße und bauen aufeinander auf

› Anlage 4 ist verpflichtend bei Einsatz von medizinischen Großgeräten (Computertomograph, Magnetresonanztomograph, Positronenemissionstomograph, Linearbeschleuniger, o. ä.)

› Anlage 5 ist für alle Praxen verpflichtend (und somit genauso anzuwenden wie Anlage 1)

Praxistyp	Ständig mit Datenverarbeitung betraute Personen	Anlage				
		1	2	3	4	5
Praxis	Weniger als 5	x			ggf.	x
Mittlere Praxis	Zwischen 6 und 20	x	x		ggf.	x
Großpraxis	über 20 ***– oder –*** Datenverarbeitung in erheblichem Umfang	x	x	x	ggf.	x

Anforderungsauswahl

› Anforderungen beziehen sich immer auf ein Zielobjekt

› Anforderungen von Zielobjekten, die in der Praxis nicht genutzt werden, **müssen nicht** umgesetzt werden

› Insgesamt werden 12 Zielobjekte in den fünf Anlagen referenziert:

Dezentrale Komponenten der TI	Mobile Device Management (MDM)
Endgeräte	Mobiltelefon
Endgeräte mit dem Betriebssystem Windows	**Netzwerksicherheit**
Internet-Anwendungen	Office-Produkte
Medizinische Großgeräte	Smartphone und Tablet
Mobile Anwendungen (Apps)	**Wechseldatenträger / Speichermedien**

- ↗ **EINLEITUNG**
- ↗ **GESETZLICHE RAHMENBEDINGUNGEN**
  - ↗ ÄRZTLICHE SCHWEIGEPFLICHT
  - ↗ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)
- ↗ **§ 75B SGB V**
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
      - ↗ VORBEREITUNG
      - ↗ HILFESTELLUNGEN ZUR DURCHFÜHRUNG
      - ↗ NACHBEREITUNG
    - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ **ABSCHLUSS**

Anforderungsumsetzung

- Hinweise und konkrete Maßnahmen zur Umsetzung der Anforderungen können von unterschiedlichen Stellen herausgegeben werden:
  - https://hub.kbv.de
  - Hersteller eines Produktes selbst
  - Verbände wie der Allianz für Cybersicherheit
  - Behörden wie dem BSI

- Auch eigenständig entwickelte technische und/oder organisatorische Maßnahmen können zur Erfüllung der Anforderungen genutzt werden

Tipp

→ Eine ständig aktualisierte Liste von Hilfsmitteln zur Umsetzung kann auf der Webseite der KBV gefunden werden.

Umzusetzen bis 01.01.2021

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	-	-	-	-	1	1
	-	-	-	-	1	1
	-	-	-	-	1	1

- Eine Anforderung der Anlage 5 muss bis 01.01.21 erfüllt sein
- Anforderung betrifft „Dezentrale Komponenten der TI“
- Muss von allen Praxistypen umgesetzt werden

Umzusetzen bis 01.01.2021 – Anlage 5

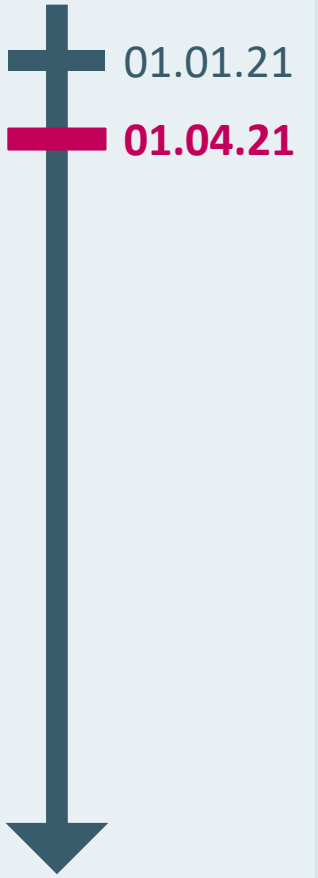
Anforderung Nr. 5

Zielobjekt	Anforderung	Erläuterung
Dezentrale Komponenten der TI	Geschützte Kommunikation mit dem Konnektor	Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.

- Clients sind die mit dem Konnektor verbundenen Systeme, z. B. Kartenterminals und Praxisverwaltungssystem (PVS)

- Schutz z. B. durch Aktivierung
  - der verschlüsselnden TLS-Verbindung vom PVS-System zum Konnektor
  - der Authentisierungsmöglichkeit am Konnektor

Umzusetzen bis 01.04.2021



	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	20	-	-	-	-	20
	20	1	-	-	-	21
	20	1	1	-	-	22

- Bis zu 22 Anforderungen müssen bis 01.04.21 erfüllt sein
- 20 Anforderungen müssen von allen Praxen umgesetzt werden
- Themengebiete sind vor allem:
  - Endgeräte, insbesondere mobile Geräte
  - Wechseldatenträger
  - Netzwerksicherheit

Umzusetzen bis 01.04.2021 – Anlage 1 (II)

Nr.	Zielobjekt	Anforderung	Erläuterung
7	Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.
8	Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.
10	Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.
12	Endgeräte	Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras	Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.
13	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder Abmelden.
15	Endgeräte	Einsatz von Viren-Schutzprogrammen	Setzen Sie aktuelle Virenschutzprogramme ein.

Umzusetzen bis 01.04.2021 – Anlage 1 (IV)

Nr.	Zielobjekt	Anforderung	Erläuterung
29	Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.
30	Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Versand-Anbieter mit sicherem Nachweis-System, Manipulationssichere Versandart und Verpackung.
32	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.
33	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.

Umzusetzen bis 01.04.2021 – Anlage 3

Anforderung Nr. 10

Zielobjekt	Anforderung	Erläuterung
Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.

› Sichere und nicht veraltete Verschlüsselungsverfahren einsetzten

› Das BSI beschreibt in der ständig aktualisierten Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1) sichere Verfahren.

Umzusetzen bis 01.07.2021

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	-	-	-	3	-	3
	-	-	-	3	-	3
	-	-	-	3	-	3

- Bis zu 3 Anforderungen müssen bis 01.07.21 erfüllt sein
- Nur bei der Nutzung medizinischer Großgeräte umzusetzen

Umzusetzen bis 01.07.2021 – Anlage 4

- Medizinische Großgeräte sind beispielweise:
  - Röntgengeräte, Computertomograph (CT), Magnetresonanztomograph (MRT), Positronenemissionstomograph (PET)
  - Linearbeschleuniger /Telecobalt-Gerät
  - Herzkatheter-Messplätze
  - Dialysegeräte
  - Gammakameras
  - Herz-Lungen-Maschinen

IT-Sicherheitssicht: Ein medizinisches Großgerät ist ein Computer mit Spezialfunktionen

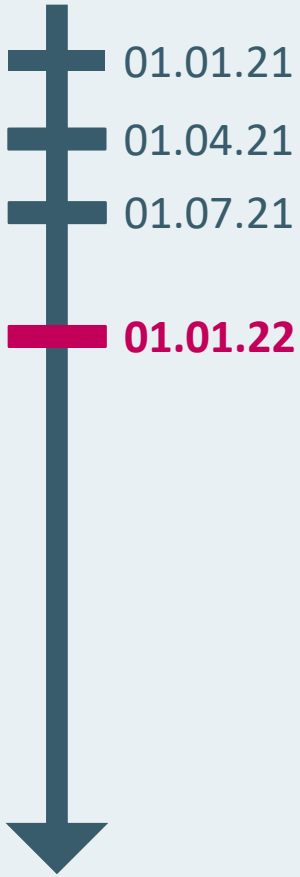
- Geltende gesetzliche Vorgaben für Medizinprodukte:
  - Medizinproduktegesetz (nach Richtlinie 93/42/EWG bzw. Verordnung (EU) 2017/745)
  - Datenschutzgrundverordnung (DSGVO)
  - Medizinprodukte-Betreiberverordnung (MPBetreibV)

Umzusetzen bis 01.07.2021 – Anlage 4

Anforderung Nr. 1, 2 & 5

Zielobjekt	Anforderung	Erläuterung
Medizinische Großgeräte	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten sollten gewechselt werden.
Medizinische Großgeräte	Nutzung sicherer Protokolle für die Konfiguration und Wartung	Für die Konfiguration und Wartung von medizinischen Großgeräte müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.
Medizinische Großgeräte	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.

Umzusetzen bis 01.01.2022

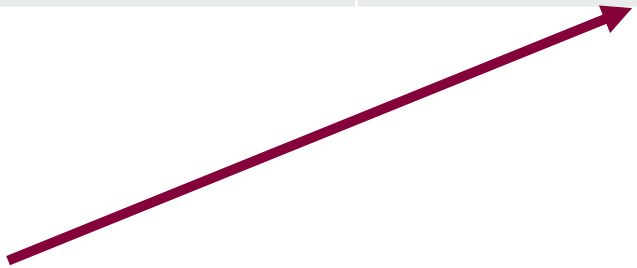


	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	14	-	-	3	6	23
	14	7	-	3	6	30
	14	7	9	3	6	39

- Bis zu 39 Anforderungen müssen bis 01.01.22 erfüllt sein
- Frist mit den meisten umzusetzenden Anforderungen
- Themengebiete sind vor allem:
  - Mobile Geräte bzw. Mobile Device Management
  - Netzwerkmanagement
  - Berechtigungsmanagement

Umzusetzen bis 01.01.2022 – Anlage 1 (I)

Nr.	Zielobjekt	Anforderung	Erläuterung
3	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.
9	Internet-Anwendungen	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.
11	Internet-Anwendungen	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.
14	Endgeräte	Regelmäßige Datensicherung	Sichern Sie regelmäßig Ihre Daten.



Umzusetzen bis 01.01.2022 – Anlage 1 (II)

Anforderung Nr. 14

Zielobjekt	Anforderung	Erläuterung
Endgeräte	Regelmäßige Datensicherung	Sichern Sie regelmäßig Ihre Daten.

- Datensicherungen („Backups“) helfen bei Hard- und Softwareausfällen sowie Verschlüsselungstrojanern
- Backup-Plan: welche Daten wann wie (vollständig oder inkrementell) gesichert werden
- Sowohl den Sicherungs- als auch den Wiederherstellungsprozess regelmäßige testen
- Backups schützen (z. B. vor Verlust oder versehentliches Überschreiben)
- 3-2-1-Regel erwägen (3 Kopien auf 2 unterschiedlichen Medien, davon 1 außer Haus)

Umzusetzen bis 01.01.2022 – Anlage 1 (III)

Nr	Zielobjekt	Anforderung	Erläuterung
16	Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.
17	Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.
18	Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	Verwenden Sie so wenige persönliche Daten wie möglich.
21	Smartphone und Tablet	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräte das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.
24	Smartphone und Tablet	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.

Umzusetzen bis 01.01.2022 – Anlage 1 (V)

Anforderung Nr. 34

Zielobjekt	Anforderung	Erläuterung
Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.

- Geeignete Authentisierung ist beispielsweise eine 2-Faktor-Authentifizierung mit Passwort (Wissen) und einem zugeschickten Code (Besitz)
- Default-Passwörter auf jeden Fall ändern
- Passwörter ausreichend stark gestalten:
  - mind. 3 verschiedene Zeichenarten (z. B. Buchstaben, Zahlen und Sonderzeichen)
  - mind. 12 Zeichen Länge

Umzusetzen bis 01.01.2022 – Anlage 2 (I)

Nr.	Zielobjekt	Anforderung	Erläuterung
2.	Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.
3.	Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.
4.	Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.
7.	Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.
9.	Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.
10.	Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.
11.	Netzwerksicherheit	Umfassende Protokollierung, Alarmierung und Logging von Ereignissen	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.

Umzusetzen bis 01.01.2022 – Anlage 4

Nr.	Zielobjekt	Anforderung	Erläuterung
3.	Medizinische Großgeräte	Protokollierung	Es muss festgelegt werden: • welche Daten und Ereignisse protokolliert werden sollen, • wie lange die Protokolldaten aufbewahrt werden und • wer diese einsehen darf. Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.
4.	Medizinische Großgeräte	Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen	Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden.
6.	Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden.

IT-Sicherheitssicht: Ein medizinisches Großgerät ist ein Computer mit Spezialfunktionen

Umzusetzen bis 01.01.2022 – Anlage 4 – Details

- Protokollfunktionalitäten der medizinischen Großgeräte richtig konfigurieren und auswerten um Fehlfunktionen und mögliche Sicherheitsvorfälle zu erkennen

- Verifizieren, dass der Zugriff auf die vernetzte Medizintechnik von außerhalb der Praxis nicht möglich ist
- Verhindern des Zugriffs durch Deaktivierung ungewollter Dienste und Konfiguration der Firewall

- Zum Schutz der medizinischen Großgeräte (z.B. bei ausbleibenden Sicherheitsupdates der Hersteller) Isolierung der Geräte von der weiteren IT durch Netzwerksegmente oder -Zonen
- Die erlaubten Kommunikationsverbindungen auf das notwendige Maß beschränken

- Trennung der medizinischen Großgeräte im Netzplan (vgl. Anlage 1 – Anforderung 33) nachvollziehbar dokumentieren

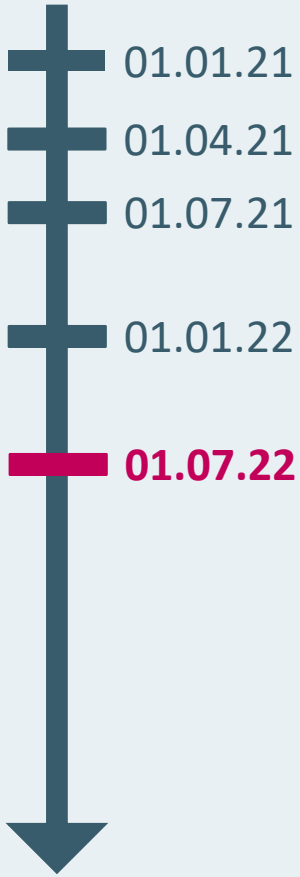
Umzusetzen bis 01.01.2022 – Anlage 5

Nr.	Zielobjekt	Anforderung	Erläuterung
1.	Dezentrale Komponenten der TI	Planung und Durchführung der Installation	Die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten müssen berücksichtigt werden.
2.	Dezentrale Komponenten der TI	Betrieb	Die Anwender- und Administrationsdokumentationen der gematik GmbH und der Hersteller der TI-Komponenten, insbesondere die Hinweise zum sicheren Betrieb der Komponenten, müssen berücksichtigt werden.
3.	Dezentrale Komponenten der TI	Schutz vor unberechtigtem physischem Zugriff	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.
4.	Dezentrale Komponenten der TI	Betriebsart „parallel“	Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungserbringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.
6.	Dezentrale Komponenten der TI	Zeitnahes Installieren verfügbarer Aktualisierungen	Die TI-Komponeten in der Praxis müssen regelmäßig auf verfügbare Aktualisierungen geprüft werden und verfügbare Aktualisierungen müssen zeitnah installiert werden. Bei Verfügbarkeit einer Funktion für automatische Updates sollte diese aktiviert werden.
7.	Dezentrale Komponenten der TI	Sicheres Aufbewahren von Administrationsdaten	Die im Zuge der Installation der TI-Komponenten eingerichteten Administrationsdaten, insbesondere auch Passwörter für den Administrator-Zugang, müssen sicher aufbewahrt werden. Jedoch muss gewährleistet sein, dass der Leistungserbringer auch ohne seinen Dienstleister die Daten kennt.

Umzusetzen bis 01.01.2022 – Anlage 5 – Details

- Informationen von der Webseite der gematik und von den Herstellern der TI-Komponenten nutzen
- Installationsprotokoll, die vom Dienstleister erstellten Dokumentation und ggf. weitere relevante Informationen wie Administrationsdaten aushändigen lassen und aufbewahren
- Konnektor an einem zutrittsgeschützten Ort aufstellen (z. B. (Server-)Raum oder abschließbarer Schrank)
- Bei **paralleler** Installation des Konnektors, ausreichende Funktionen (Firewall, UTM, etc.) anderer für die Internetanbindung zuständigen Geräte (Router, etc.) sicherstellen und konfigurieren
- Regelmäßig auf Updates der TI Komponenten prüfen und zeitnah installieren

Umzusetzen bis 01.07.2022



	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	-	-	-	-	-	0
	-	3	-	-	-	3
	-	3	1	-	-	4

- Bis zu 4 Anforderungen müssen bis 01.07.22 erfüllt sein
- Anforderungen greifen nur ab einer entsprechenden Praxisgröße
- Fokus liegt auf Anforderungen zu mobilen Geräten

Umzusetzen bis 01.07.2022 – Anlage 2

Nr.	Zielobjekt	Anforderung	Erläuterung
5.	Endgeräte mit dem Betriebssystem Windows	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.
6.	Smartphone und Tablet	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.
8.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.

- Veraltete Protokolle zur Authentisierung sollten blockiert werden
- Eine Nutzungs- und Sicherheitsrichtlinie für mobile Geräte:
  - Sollte Nutzungs-, Pflege-, Aufbewahrungs- und Verlustmeldungsvorgaben machen
  - Sollte Deinstallation von Verwaltungssoftware und Rooten von Geräts verbieten
  - Sollte Teil der Schulung zu Sicherheitsmaßnahmen sein
  - Muss jedem Benutzer ausgehändigt und regelmäßig auf Einhaltung überprüft werden

- ↗ EINLEITUNG
- ↗ GESETZLICHE RAHMENBEDINGUNGEN
  - ↗ ÄRZTLICHE SCHWEIGEPFLICHT
  - ↗ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)
- ↗ § 75B SGB V
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
      - ↗ VORBEREITUNG
      - ↗ HILFESTELLUNGEN ZUR DURCHFÜHRUNG
      - ↗ NACHBEREITUNG
    - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ ABSCHLUSS

Umsetzungsprozess: Maßnahmenkontrolle

- Regelmäßige Überprüfung der Maßnahmen auf:
  - **Umsetzungsstand**
    z. B.:
    „Können alle anwendbaren Anforderungen bis zum jeweiligen Fristtermin umgesetzt werden?“
  - **Wirksamkeit**
    z. B.:
    „Halten sich Angestellte an die Vorgaben und Richtlinien, z. B. den Regelungen zur Nutzung mobiler Geräte?“

Umsetzungsprozess: Gesamtkontrolle

- Regelmäßige Überprüfung der IT-Sicherheit der Praxis aufgrund:
  - **Richtlinienaktualisierung**

    „Bedarf es aufgrund der (jährlichen) Anpassung der Richtlinie für IT-Sicherheit in der Praxis einer Angleichung der Vorgaben oder Maßnahmen?“
  - **Umfeldwandel**

    „Bedarf es aufgrund von Änderungen im Praxisalltag, in der Praxis-IT, zusätzlichen Aufgaben oder einer geänderten Rechtslage einer Angleichung der Vorgaben oder Maßnahmen?“

- ↗ EINLEITUNG
- ↗ GESETZLICHE RAHMENBEDINGUNGEN
  - ↗ ÄRZTLICHE SCHWEIGEPFLICHT
  - ↗ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)
- ↗ § 75B SGB V
  - ↗ RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT
    - ↗ DIE PRAXIS ALS PATIENT
    - ↗ ANFORDERUNGSUMSETZUNG
  - ↗ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN
- ↗ ABSCHLUSS

2. Zertifizierung vertrauenswürdiger Dienstleistern (§ 75b Abs. 5 SGB V)

- Zweiter Aspekt des § 75b SGB V und in Absatz 5 von diesem geregelt
- Erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Erstellt im Benehmen mit maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen

→ Dank dieser Personenzertifizierung können qualifizierte Dienstleister zur Unterstützung der anforderungsgerechten Umsetzung der „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ in Anspruch genommen werden.

2. Zertifizierung vertrauenswürdiger Dienstleistern (§ 75b Abs. 5 SGB V)

„Richtlinie zur Zertifizierung nach § 75b Absatz 5 SGB V“

› Veröffentlichung zertifizierter Antragstellers von der KBV und der KZBV

Zertifikatsausstellung

› Bestehen einer Prüfung zur Umsetzung der Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

oder

› Anerkennung von Zertifikatsinhabern anderer IT-Sicherheitsstandards

Recap

Die Praxis als Patient - Durchführung

1. **Anamnese:** Praxistyp festlegen
2. **Diagnose:** Anzuwendende Anlagen festlegen
3. **Behandlungsplan:** Anzuwendende Anforderungspunkte festlegen
4. **Therapie:** Maßnahmen festlegen und umsetzen
5. **Mitbehandlung:** Dienstleister beauftragen/anweisen
6. **Verlaufskontrolle:** Maßnahmenwirksamkeit prüfen
7. **Folgetermin:** auf Änderungen reagieren; spätestens nach einem Jahr eine überarbeitete Richtlinie

Take-Home-Message Fortbildung „IT-Sicherheit in der Praxis“

1. Geltende Anforderungen aufgrund der Praxisgröße und den genutzten Systeme identifizieren

2. Umgesetzte Maßnahmen dokumentieren und fehlende Maßnahmen **bis zur entsprechenden Frist** umsetzen

3. Eine ständig aktualisierte Liste von Hilfsmitteln zur Umsetzung kann auf der Webseite der KBV gefunden werden.

Tipp

→ Beauftragen Sie einen qualifizierten Dienstleister, der Sie bei bestimmten Punkten unterstützt (z. B. der Aufstellung der erforderlichen Anforderungen und möglichen Maßnahmen) oder den kompletten Prozess für Sie übernimmt.

Autoren

↗ **Sarah Schuchardt, H.-Theo Rey**
Kassenärztliche Bundesvereinigung - Dezernat Digitalisierung und IT

↗ **Dr. med. Sören Holste**
mio42 GmbH

Kontakt
H.-Theo Rey
Kassenärztliche Bundesvereinigung
Dezernat Digitalisierung und IT
Herbert-Lewin-Platz 2
10623 Berlin

Vielen Dank!

Alle Informationen auch unter
https://www.kbv.de/html/it-sicherheit.php