DSB im niedergelassenen Umfeld

IT-Sicherheitsrichtlinie der KBV

Umgang mit Mobilgeräten (BYOD)

DSFA in der Arztpraxis

MVZ in Trägerschaft eines Krankenhauses, Zusammenarbeit mit DSB des Krankenhauses

1

Letters Avatar

Kontakt info@letter-consulting.de

www.5medical-management.de

Tel: 02131 1331166

- Auszug Vita Michael Letter
- Studium Betriebswirtschaft GH Duisburg
- Gründung der 5medical management GmbH 1996
- Seit 15 Jahren im Bereich Datenschutz spezialisiert
- Mitautor der GDD Praxishilfen und der GMDS – Ratgeber
- Referent zum Thema DSFA

2

Aufgaben eines DSB im niedergelassenen Umfeld

- Beratung und Kontrolle
- Hilfestellung z. B. bei der Erstellung des VVT und einer Datenschutzrichtlinie (Datenschutzkonzept)
- Oft - die erforderlichen Unterweisungen durchführen
- Auskunfts- Löschbegehren begleiten bzw. beantworten und Prozess kontrollieren
- Ansprechpartner der Landesdatenschutzbehörden - Beschwerden / Datenpannen / Auskünften
- Und, und, und.....

3

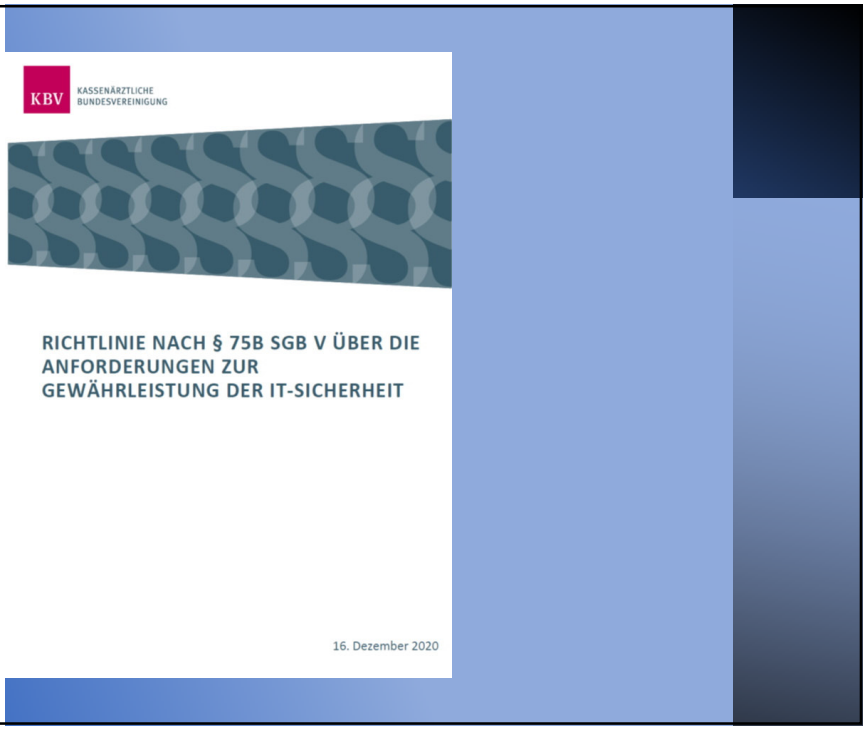
Aufbau der Richtlinie

Aufteilung nach Praxisgröße

und

Differenzierung nach medizinischen Großgeräten

(z. B. Computertomograph oder Linearbeschleuniger etc.)



4

§75B SGB V

IT-Sicherheitsrichtlinie war bis zum 30.06.2020 durch die KBV vorzulegen

Die Umsetzung in den Praxen startete am 01.04.2021

5

Zielsetzung

Die Richtlinie legt Anforderungen nach dem Stand der Technik zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung fest.

Sie umfasst auch Anforderungen an die Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur.

Es sollen die Ziele Verfügbarkeit, Integrität und Vertraulichkeit erreicht werden.

Die KBV muss die Zertifizierung von Anbietern regeln.

6

Status Quo

FAQ veröffentlicht: https://mio.kbv.de/display/itsrl/FAQ

IT-Dienstleister sind nicht verpflichtet sich von der KBV zertifizieren zu lassen.

Praxen sind nicht verpflichtet (zertifizierte) IT-Dienstleister zu beauftragen.

Nur die KBV ist verpflichtet die Personen-Zertifizierungen nach § 75b Abs. 5 SGB V für IT-Dienstleister anzubieten.

7

Unterscheidung nach Praxisgrößen und zeitlichem Rahmen

	Praxis bis 5 Beschäftigte		Praxis von 6 bis 20 Beschäftigte		Praxis mit mehr als 20 Beschäftigte		Praxis mit Großgeräten		Gilt ab
Anlage 1	X		X		X				01.04.2021
Anlage 2			X		X				01.04.2021 01.07.2022
Anlage 3					X				01.01.2022 01.04.2022 01.07.2022
Anlage 4 Großgeräte							X		01.07.2021 01.01.2022
a	X		X		X		X		01.01.2022

Beschäftigte = pro Person, nicht Vollzeitstellenäquivalent

8

Checkliste zur Umsetzung der BBV Richtlinie IT-Sicherheit in Praxen

https://www.kbv.de/media/sp/RiLi_75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf

Mit jedem zusätzlichen „NEIN“ steigt die Notwendigkeit zur Anpassung der Praxis IT an die gültigen Sicherheitsanforderungen.

Nr.	Frage	Hinweis in KBV-Richtline	Ja	Nein
1	Kommen Sie ohne Microsoft Office Produkte aus?	Anlage 1 Nummer 5		
2	Ist das automatische Speichern in Word (und allen anderen MS-Produkten) deaktiviert?	Anlage 1 Nummer 5		
3	Sind die IT-Systeme und Server vor unbefugten Zugriffen gesichert?	Artikel 32 DSGVO		
4	Werden starke Passwörter genutzt und regelmäßig verändert?	DSGVO technische und organisatorische Maßnahmen		
5	Kommen Sie ohne Unterstützung bei der Umsetzung der technischen und organisatorischen Maßnahmen aus?	Anlage 1, Nummer 5, 6, 7, 8, 10, 13, 16,18,20, 25, 29, 30, 31, 33, 34		
6	Ist eine Firewall im Einsatz?	Anlage 1 Nummer 9		
7	Wird eine Hardware-Firewall nach aktuellem Stand der Technik genutzt?	Artikel 32 DSGVO/Schutz vor Vernichtung, Veränderung oder Verlust personenbezogener Daten		
8	Werden die ein- und ausgehenden Verbindungen in dem Praxis-Netzwerk auf Schadsoftware geprüft?	Anlage 1 Nummer 9 und 32		
9	Gibt es eine Trennung der internen Netze?	Anlage 1 Nummer 32		
10	Ist das interne Netzwerk anhand eines Netzplanes dokumentiert?	Anlage 1 Nummer 33		

9

Bedeutung der Vorgaben nach &75B SGB V für die vertragsärztliche Praxis

- Nicht allumfassend
  - Bauliche Sicherheit nicht berücksichtigt
  - Analoge Anforderungen zum Schutz von Patientendaten nicht berücksichtigt
- Es werden erstmals Anforderungen an die Einrichtung der Telematik definiert
- Es ist ein Überwachungsprozess erforderlich, da sich die Anforderungen jährlich ändern können
- Eine Nachweispflicht ist nicht gesetzlich vorgeschrieben
- Regelung ist ein Mindestmaß („Stand der Technik“)
- Dokumentierte Umsetzung wirkt ggf. bußgeldmindernd bei Datenschutzvorfällen und ggf. Schadensersatzansprüchen

10

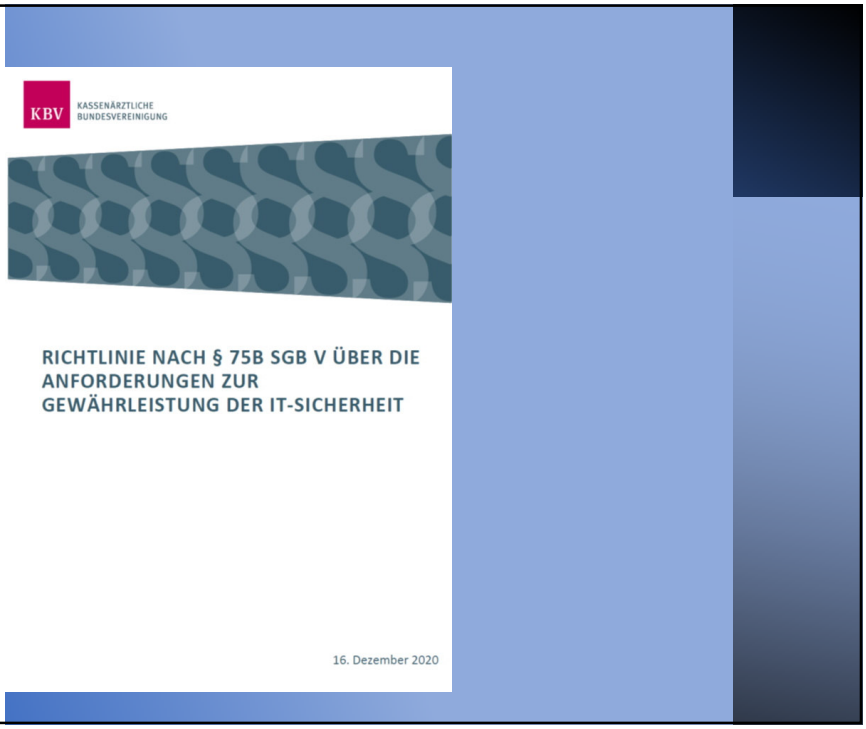
Stauts Quo

Umsetzung bis heute

???????

Sanktionen

keine bekannt



11

BYOD

- Umgang mit Mobilgeräten (BYOD)
- Empfehlung – Grundsätzlich untersagen (z. B. Datenschutzrichtlinie / Arbeitsanweisung)
- Eigene Geräte dürfen in den Pausen genutzt werden
- Patientendaten als Kontakte übernehmen ist untersagt
- Auf die Messenger Problematik (z. B. WhatsApp) eingehen
- Sofern ein Gastzugang (WLAN) besteht ggf. diese zur Nutzung erlauben (Pausen und außerhalb der Arbeitszeit)
- Konsequenzen aufzeigen

12

DSFA in der Arztpraxis

- Muss Kriterien beachten, z. B. MVZ mit gemeinsamer Patientenverwaltung
- Drei und mehr Behandler mit entsprechendem Patientenaufkommen
- Frage, warum nicht generell auch bei kleineren Einheiten (kein Muss aber ein Kann)

13

14