SECUREPOINT

KBV-KONFORME DIGITALISIERUNG

Patientendaten schützen

Wir schützen Ihre Daten und die Ihrer Patienten mit der Vielfalt von Unified Security.

Sichere KIM

Schützt Kanäle zur Kommunikation im Medizinwesen vor Viren, Phishing, Spy- und Malware.

Mobil- und Großgeräte sichern

Mit Unified-Security-Lösungen alle webfähigen Endgeräte zuverlässig schützen.

Verschiedene Bereiche

Schutz für alle Arten von Praxen, Laboren medizinischen Versorgungszentren und mehr.

SICHERE NETZWERKE FÜR MEHR PATIENTENSCHUTZ

CHECKLISTE FÜR MEHR IT-SICHERHEIT IM GESUNDHEITSWESEN

KBV-konforme Digitalisierung von Arztpraxen

In allen Lebensbereichen sind wir mit zunehmender Digitalisierung konfrontiert. Auch vor dem Gesundheitswesen macht diese nicht Halt.

Durch den Gesetzgeber werden immer mehr Verpflichtungen und Veränderungen verabschiedet, die der Verbesserung der Patientenversorgung, der Datensicherheit sowie dem Datenschutz dienen.
Auch die KBV macht neben dem digitalen Versorgungsgesetz (DVG), dem Patientendatenschutzgesetz (PDSG) und dem wohl bald gültigem digitalen Versorgungs- und Pflegemodernisierungsgesetz (DVPMG) immer mehr Vorgaben zur Wahrung der IT-Sicherheit.

Wir sind Ihr Partner für die Umsetzung

Die folgende Checkliste (angelehnt an die gültigen KBV-Richtlinien) ermöglicht es Ihnen, Handlungsbedarf in Ihrer Praxis zu erkennen. Wenn Sie auch nur eine oder gar mehrere Fragen mit „NEIN" beantworten, sollten Sie dringend in IT-Sicherheit investieren.

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

Nr.	Frage	Hinweis in KBV-Richtlinien	Ja	Nein
Allgemeine Sicherheitshinweise				
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		
Unterstützung bei der Umsetzung				
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		

Nr.	Frage	Hinweis in KBV-Richtlinien	Ja	Nein
Netzwerksicherheit (UTM-Firewall)				
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 im 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		
11	Wird ausschließlich auf verschlüsselten Internetseiten gesurft?	Anlage 1 Nummer 10		
12	Kommen Sie ohne Gästenetz aus?	Anlage 1		
Antivirus				
13	Wird eine aktuelle Antivirus-Software genutzt?	Anlage 1 Nummer 15		
14	Werden Wechseldatenträger/Speichermedien bei jeder Verwendung mit einer aktuellen Antivirussoftware überprüft?	Anlage 1 Nummer 28		
Mobile Device Management				
15	Kommen Sie ohne mobile Devices aus?	Anlage 1		
16	Ist es sichergestellt, dass die Mitarbeitenden keine Handys im Praxisnetzwerk nutzen?	Anlage 1		
17	Sind die mobilen Geräte verschlüsselt?	Anlage 1 Nummer 22		
18	Können die Geräte bei Verlust gesperrt, geortet oder gelöscht werden?	Anlage 1 Nummer 25 und DSGVO		
19	Wird das Verändern der Grundkonfiguration von Mitarbeitenden auf ihren Diensthandys verhindert?	Anlage 1 Nummer 21		
20	Sind die Smartphones und Tablets mit einem komplexen Gerätesperrcode geschützt?	Anlage 1 Nummer 22		
Backup				
21	Werden regelmäßig Backups der Daten erstellt?	Anlage 1 Nummer 14		

Handlungsbedarf ermittelt

Sie haben eine oder mehrere Fragen mit „NEIN“ beantwortet? Sprechen Sie uns an!