Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung (Richtlinie nach §75b SGBV)

Allgemein

Die Kassenärztliche Bundesvereinigung hat (entsprechend dem Auftrag nach § 75b SGB V) eine Richtlinie erstellt, um Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln.
Diese Richtlinie legt die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest.

Der/die Praxisinhaber ist/sind verantwortlich für die Einhaltung der Anforderungen dieser Richtlinie.

Untergliederung nach Praxisgröße

Die umzusetzenden Anforderungen sind nach Praxisgröße unterteilt:

1. Praxis: Eine Praxis ist eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen.

2. Mittlere Praxis: Eine mittlere Praxis ist eine vertragsärztliche Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen.

3. Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang: 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).

Anforderungskategorien

In der Richtlinie werden fünf Anforderungskategorien genannt:

Anforderungen für Praxen
Diese Anforderungen gelten für alle Praxen

Zusätzliche Anforderungen für mittlere Praxen
Diese Anforderungen gelten für Praxen mit Praxisgrößen 2 und 3

Zusätzliche Anforderungen für Großpraxen
Diese Anforderungen gelten für Praxen mit Praxisgrößen 3

Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte
Diese Anforderungen gelten für Praxen die medizinische Großgeräte, wie Computertomograph, Magnetresonanztomograph, Positronenemissionstomograph und Linearbeschleuniger, einsetzen

DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR
Diese Anforderungen gelten für alle Praxen

Unterteilung nach Geltungszeiträumen

Wir haben Ihnen die Anforderungen nach Geltungszeitraum gelistet:

Anforderungen ab dem 01.01.2021

DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR (ab dem 01.01.2021)

Zielobjekt	Anforderung	Erläuterung
Primärsysteme	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.

Anforderungen ab dem 01.04.2021

Anforderungen für alle Praxen (ab dem 01.04.2021)

Zielobjekt	Anforderung	Erläuterung
Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen.
Mobile Anwendungen (Apps)	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.
Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.
Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung der in Office-Produkte integrierte Cloud-Speicher zur Speicherung personenbezogener Informationen
Office-Produkte	Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.
Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.
Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.
Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.

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.
Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder Abmelden.
Endgeräte	Einsatz von Viren-Schutzprogrammen	Setzen Sie aktuelle Virenschutzprogramme ein.
Smartphone und Tablet	Schutz vor Phishing und Schadprogrammen im Browser	Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.
Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.
Smartphone und Tablet	Verwendung eines Zugriffschutzes	Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.
Smartphone und Tablet	Updates von Betriebssystem und Apps	Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.
Mobiltelefon	Updates von Mobiltelefonen	Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.
Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.
Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Versand-Anbieter mit sicherem Nachweis-System, Manipulationssichere Versandart und Verpackung.
Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.
Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.

Zusätzliche Anforderungen für mittlere Praxen (ab dem 01.04.2021)

Zielobjekt	Anforderung	Erläuterung
Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.

Zusätzliche Anforderungen für Großpraxen (ab dem 01.04.2021)

Zielobjekt	Anforderung	Erläuterung

Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.

Anforderungen ab dem 01.07.2021

Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte (ab dem 01.07.2021)

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.

Anforderungen ab dem 01.01.2022

DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR (ab dem 01.01.2022)

Zielobjekt	Anforderung	Erläuterung
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.
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.
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.
Konnektor	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.
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.
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.

Anforderungen für alle Praxen (ab dem 01.01.2022)

Zielobjekt	Anforderung	Erläuterung
Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.
Internet-Anwendungen	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.

Internet-Anwendungen	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.
Endgeräte	Regelmäßige Datensicherung	Sichern Sie regelmäßig Ihre Daten.
Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.
Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.
Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	Verwenden Sie so wenige persönliche Daten wie möglich.
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.
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.
Mobiltelefon	Sperrmaßnahmen bei Verlust eines Mobiltelefons	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.
Mobiltelefon	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.
Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.
Wechseldatenträger / Speichermedien	Sicheres Löschen der Datenträger vor und nach der Verwendung	Datenträger nach Verwendung immer sicher und vollständig Löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.
Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.

Zusätzliche Anforderungen für mittlere Praxen (ab dem 01.01.2022)

Zielobjekt	Anforderung	Erläuterung

Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.
Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.
Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.
Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.
Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.
Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.
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.

Zusätzliche Anforderungen für Großpraxen (ab dem 01.01.2022)

Zielobjekt	Anforderung	Erläuterung
Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.
Smartphone und Tablet	Definition der erlaubten Informationen und Applikationen auf mobilen Geräten	Die Praxis sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.
Mobile Device Management (MDM)	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden.
Mobile Device Management (MDM)	Berechtigungsmanagement im MDM	Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.
Mobile Device Management (MDM)	Verwaltung von Zertifikaten	Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.
Mobile Device Management (MDM)	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.

Mobile Device Management (MDM)	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.
Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.
Netzwerksicherheit	Absicherung von schützenswerten Informationen	Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.

Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte (ab dem 01.01.2022)

Zielobjekt	Anforderung	Erläuterung
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.
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.
Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden.

Anforderungen ab dem 01.07.2022

Zusätzliche Anforderungen für mittlere Praxen (ab dem 01.07.2022)

Zielobjekt	Anforderung	Erläuterung
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.
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.
Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.

Zusätzliche Anforderungen für Großpraxen (ab dem 01.07.2022)

Zielobjekt	Anforderung	Erläuterung
Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.
Mobile Device Management (MDM)*	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.

(* diese Anforderung wurde in dem uns vorliegenden Dokument zur Richtlinie mit dem Geltungsdatum 10.07.2020 angegeben)