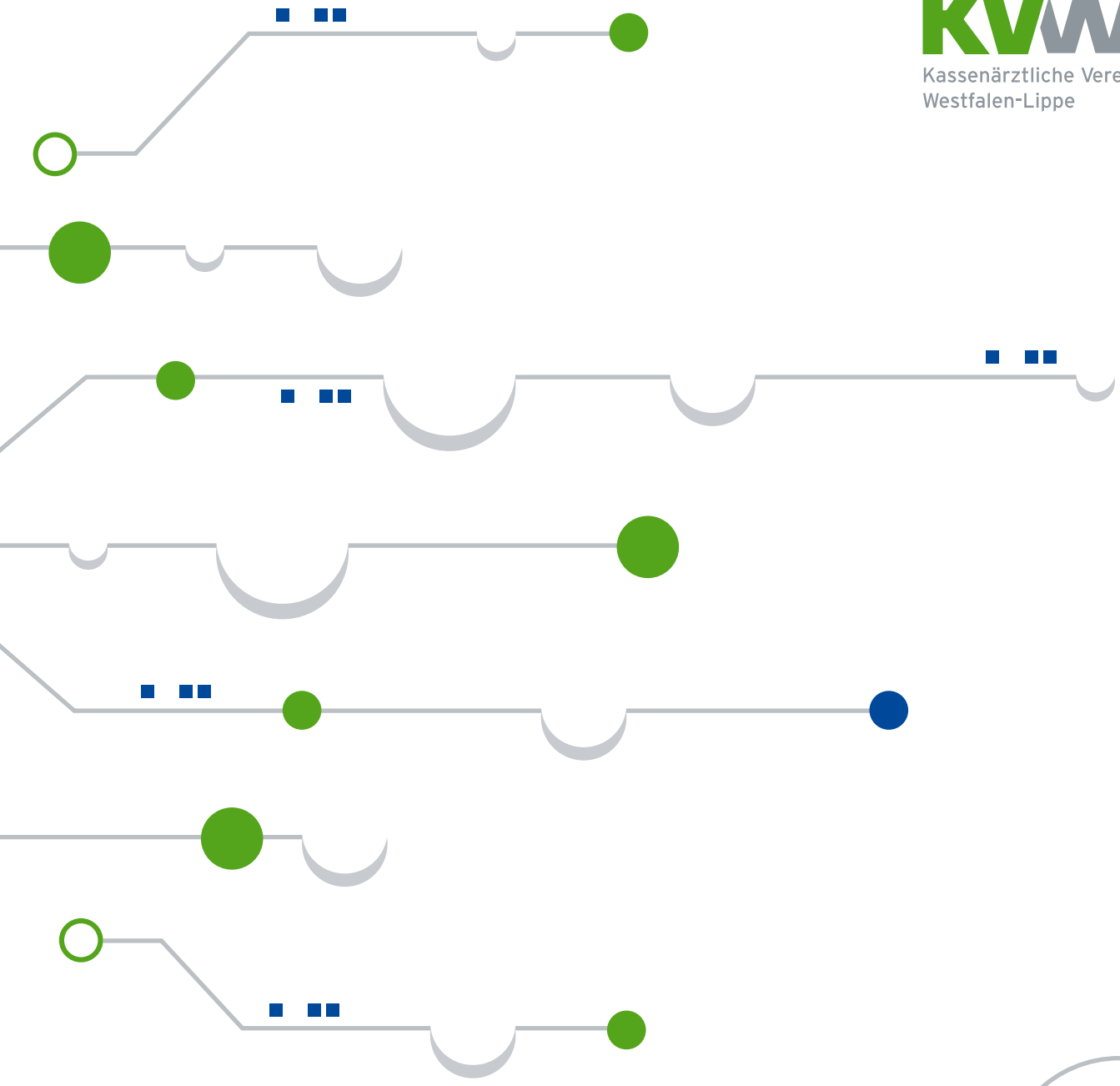


KVWL
Kassenärztliche Vereinigung
Westfalen-Lippe

2021
2022

Hinweise zur

IT-Sicherheitsrichtlinie

nach §75b SGB V

Inhalt

Sicherheit geht vor

Die Digitalisierung spielt in der heutigen Zeit eine bedeutende Rolle. So stehen auch in Ihrer Praxis digitale Prozesse und die Vernetzung mit anderen Leistungserbringern immer mehr im Fokus Ihrer ärztlichen Tätigkeit. Hierfür nutzen Sie bereits einige technische Komponenten wie die Telematikinfrastruktur (TI) und ihre Anwendungsmöglichkeiten. Da Sie in Ihrer Praxis besonders schützenswerte Gesundheitsdaten verarbeiten, ist Ihnen – genau wie der KVWL – die Sicherheit dieser Daten ein besonderes Anliegen. Vor diesem Hintergrund wurde eine gesetzliche Grundlage geschaffen, nach der die KBV im Einvernehmen mit dem Bundesamt für Informationstechnik (BSI) eine Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit (IT-Sicherheitsrichtlinie) erstellt hat. Die Richtlinie ist am 23.01.2021 in Kraft getreten und soll durch die Vorgaben zu IT-Systemen, der Nutzung mobiler Apps, der Telematikinfrastruktur sowie durch zusätzliche Anforderungen in Abhängigkeit von der Praxisgröße Rechtssicherheit schaffen.

Die KVWL möchte Sie, die niedergelassenen Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten, mit dieser Broschüre bei der Umsetzung der Anforderungen unterstützen. Dazu finden Sie hier ergänzende Hinweise und anschauliche Beispiele zu den in Ihrer Praxis zu implementierenden Maßnahmen, kategorisiert und gesondert unterteilt nach ihrer Umsetzungsfrist und unter Verweis auf die Grundlage in der Richtlinie. Die Inhalte werden regelmäßig an die aktuellen Anforderungen der Sicherheitsrichtlinie angepasst und veröffentlicht. Als weitere Hilfestellung enthält die Broschüre zusätzlich ein Glossar (Seite 37), um Ihnen bei den IT-Fachtermini Orientierungshilfen zu geben sowie grundlegende Handlungsempfehlungen der KVWL (Seite 30), die bereits im Januar 2020 in ähnlicher Form zum ersten Mal von der KVWL veröffentlicht wurden.

Diese Umsetzungshilfe der KVWL bietet damit eine Aufbereitung der weiteren Hinweise der KBV zur IT-Sicherheitsrichtlinie, die unter Praxishinweise – Richtlinie IT-Sicherheit in der Praxis – IT-Sicherheit in der Praxis veröffentlicht sind und ist als deren Ergänzung zu verstehen.

Thomas Müller, KVWL-Vorstand

Anlagen

Die Anforderungen der IT-Sicherheitsrichtlinie sind in fünf Anlagen unterteilt. Die nach Praxisgröße und gesonderten weiteren Anforderungen differenzierten Anlagen bauen aufeinander auf und sind gegebenenfalls kumulativ zu erfüllen:

Anlage 1: Anforderungen für Praxen – betrifft alle Praxistypen
Anlage 2: Zusätzliche Anforderungen für mittlere Praxen
Anlage 3: Zusätzliche Anforderungen für Großpraxen
Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte
Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur

Praxisgröße

Die Definition der Praxisgrößen ergibt sich aus Punkt A. III der IT-Sicherheitsrichtlinie. Danach gilt:

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).

Hinweise zur nach §75b SGB V

IT-Sicherheitsrichtlinie

mit Umsetzungsdatum ab

2021

Dezentrale Komponenten der TI

Geschützte Kommunikation mit dem Konnektor

Gültig ab 01.01.2021

Alle Praxen
Die Kommunikation zwischen Clients wie z. B. dem PVS und dem TI-Konnektor muss verschlüsselt erfolgen. Die Authentisierung erfolgt über X.509-Zertifikate oder Benutzername und Passwort. Hierzu müssen die Clients entsprechend konfiguriert werden. Falls Sie unsicher sind, informieren Sie sich bitte ggf. bei Ihrem Softwarehaus, ob die Verschlüsselung bereits bei Ihnen umgesetzt ist. Ist dies noch nicht der Fall, schalten Sie die Funktion frei oder bitten Sie das Softwarehaus, dies für Sie umzusetzen.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 5

Mobile Anwendungen (Apps)

Sichere Apps nutzen

Gültig ab 01.04.2021

Alle Praxen
Verwenden Sie nur Apps aus den offiziellen App Stores („Google Play" von Google und „App Store" von Apple). Deaktivieren Sie in den Sicherheitseinstellungen Ihres Smartphones die Möglichkeit, Applikationen unbekannter Herkunft zu installieren.

Anlage 1: Anforderungen für Praxen, Nr. 1

Aktuelle App-Versionen

Gültig ab 01.04.2021

Alle Praxen
Aktualisieren Sie die Apps auf Ihren Smartphones durch Nutzung der Option „Autoupdate". Dies können Sie in den Einstellungen des jeweiligen App Stores konfigurieren. So sind Sie immer auf dem neuesten Stand.

Anlage 1: Anforderungen für Praxen, Nr. 2

Verhinderung von Datenabfluss

Gültig ab 01.04.2021

Alle Praxen
Stellen Sie sicher, dass Ihre Apps keine Daten an unerwünschte Empfänger wie Facebook oder Google senden. Verwenden Sie für vertrauliche Informationen nur Apps von Organisationen, die Ihnen bekannt sind und die bestenfalls für den Einsatz im medizinischen Umfeld in Deutschland getestet und freigegeben sind (z. B. Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)).

Anlage 1: Anforderungen für Praxen, Nr. 4

Minimierung und Kontrolle von App-Berechtigungen

Gültig ab 01.04.2021

Mittlere und große Praxen
Jeder App dürfen nur die minimal notwendigen Berechtigungen zugewiesen werden. Hierbei geht es beispielsweise um den Zugriff auf Kamera, Mikrofon, Standort, Telefon, SMS, Kontaktlisten, Speicher etc.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 1

Office-Produkte

Verzicht auf Cloud-Speicherung

Gültig ab 01.04.2021

Alle Praxen
Verwenden Sie keine Cloud-Dienste wie iCloud, Google Docs oder OneDrive.

Anlage 1: Anforderungen für Praxen, Nr. 5

Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten

Gültig ab 01.04.2021

Alle Praxen
Verwenden Sie für den Datenaustausch möglichst PDF-Dokumente. Denken Sie bitte daran, dass bei der Wandlung von Office-Dokumenten Angaben zum Autor und zum Erstellungsdatum in das PDF-Dokument übernommen werden. Ist das nicht gewünscht, können Sie dies bei Office-Dokumenten in den Dateieigenschaften ändern.

Anlage 1: Anforderungen für Praxen, Nr. 6

Internet-Anwendungen

Authentisierung bei Webanwendungen

Gültig ab 01.04.2021

Alle Praxen
Nutzen Sie nur Internet-Anwendungen mit sicherer Authentisierung (mindestens Benutzername / Passwort, besser Zweifaktor-Authentisierung). Die Anwendung sollte Sie außerdem nach einer Inaktivitätszeit von z. B. zehn Minuten automatisch wieder abmelden. Nutzen Sie sichere Passwörter (acht oder mehr Zeichen zusammengesetzt aus Buchstaben, Zahlen und Sonderzeichen). Verwenden Sie für die sichere Speicherung Ihrer Zugangsdaten einen Passwortmanager wie KeePass, der für viele Betriebssysteme kostenlos verfügbar ist.

Anlage 1: Anforderungen für Praxen, Nr. 7

Schutz vertraulicher Daten

Gültig ab 01.04.2021

Alle Praxen
Um die langfristige Speicherung vertraulicher Daten in Ihrem Browser zu verhindern, sollten Sie die Passwortspeicherung und Formularvervollständigung im Browser abschalten.

Löschen Sie außerdem regelmäßig die im Browser gespeicherten Daten wie Browserverlauf, Cookies, zwischengespeicherte Daten etc. Dies ist in Chrome, Firefox und Edge z. B. mittels der Tastenkombination „Strg“ + „Umschalt“ + „Entf“ möglich oder stellen Sie ein, dass der Browser beim Schließen alle Daten automatisch löscht. Stellen Sie durch die Auto-Updatefunktion unbedingt sicher, dass Ihr Browser immer auf dem aktuellen Stand ist.

Anlage 1: Anforderungen für Praxen, Nr. 8

Kryptographische Sicherung vertraulicher Daten

Gültig ab 01.04.2021

Alle Praxen
Achten Sie bitte unbedingt darauf, dass alle genutzten Internetverbindungen das sichere Protokoll HTTPS verwenden. Dies erkennen Sie z. B. an dem Schloss, das bei sicheren Verbindungen im Adressfeld des Webbrowsers angezeigt wird. Prüfen Sie ggf. auch den Herausgeber und den Inhaber des Zertifikats durch Klicken auf das Schlosssymbol. Die URLs beginnen dann auch mit https:// statt mit http://. Viele Browser versuchen sogar automatisch das Protokoll HTTPS zu verwenden.

Anlage 1: Anforderungen für Praxen, Nr. 10

Endgeräte

Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras

Gültig ab 01.04.2021

Alle Praxen
Deaktivieren Sie Mikrofone und Kameras an Ihren Rechnern, wenn sie – auch temporär – nicht verwendet werden. Diese können üblicherweise im Betriebssystem unter den Datenschutzeinstellungen abgeschaltet werden. Kameras können zusätzlich durch eine Abdeckung geschützt werden. Achten Sie auf evtl. vorhandene LED-Indikatoren, die einen möglicherweise nicht erwünschten Zugriff auf Kamera oder Mikrofon anzeigen.

Anlage 1: Anforderungen für Praxen, Nr. 12

Abmeldung nach Aufgabenerfüllung

Gültig ab 01.04.2021

Alle Praxen
Melden Sie sich nach Ende der Nutzung von Ihrem Endgerät ab oder sperren Sie den Bildschirm. Eine automatische Bildschirmsperre, die den Bildschirm nach z. B. zehn Minuten Inaktivität sperrt, sollte zusätzlich eingerichtet werden.

Anlage 1: Anforderungen für Praxen, Nr. 13

Einsatz von Virenschutzprogrammen

Gültig ab 01.04.2021

Alle Praxen
Setzen Sie ein aktuelles Virenschutzprogramm ein und halten Sie die Erkennungsdateien aktuell. Eine Übersicht über geeignete Produkte finden Sie z. B. auf www.av-test.org. Bei Windows 10 wird das Schutzprogramm „Windows Defender“ bereits mitgeliefert.

Anlage 1: Anforderungen für Praxen, Nr. 15

Smartphone und Tablet

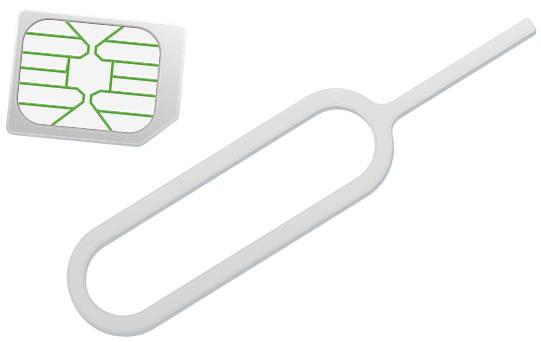
Schutz vor Phishing und Schadprogrammen im Browser

Gültig ab 01.04.2021

Alle Praxen
Klären Sie im Zweifel z. B. durch telefonische Nachfrage die Authentizität von Nachrichten, die Ihnen verdächtig erscheinen. Folgen Sie niemals irgendwelchen in einer Nachricht enthaltenen Links, wenn Sie sich nicht sicher sind, dass die Nachricht vertrauenswürdig ist. Geben Sie in keinem Fall Anmeldedaten preis, wenn Sie dazu aufgefordert werden. Sensibilisieren Sie Ihre Mitarbeiter.

Im Browser können Sie sich durch Schutzfunktionen wie „Safe Browsing“ (Android) ggfs. vor Schadprogrammen schützen.

Anlage 1: Anforderungen für Praxen, Nr. 19



Verwendung der SIM-Karten-PIN

Gültig ab 01.04.2021

Alle Praxen
Schützen Sie Ihre SIM-Karten durch eine individuelle PIN. Die zugehörige PUK sollte nur einem für die Geräte zuständigen Mitarbeiterkreis bekannt sein.

Anlage 1: Anforderungen für Praxen, Nr. 20

Verwendung eines Zugriffsschutzes

Gültig ab 01.04.2021

Alle Praxen
Verwenden Sie für die mobilen Geräte einen angemessen komplexen Sperrcode und aktivieren Sie die Bildschirmsperre. Schalten Sie alle Benachrichtigungen ab, die ggfs. auf dem Sperrbildschirm angezeigt werden. Aktivieren Sie die Verschlüsselungsoptionen für eine möglicherweise vorhandene SD-Karte (nur Android). Aktivieren Sie das automatische Löschen von Daten („Auto Factory Reset“ unter Android) nach z. B. zehn in Folge fehlgeschlagenen Anmeldeversuchen. Diese Option steht Ihnen unter Android und iOS zur Verfügung.

Anlage 1: Anforderungen für Praxen, Nr. 22

Updates von Betriebssytem und Apps

Gültig ab 01.04.2021

Alle Praxen
Wir empfehlen Ihnen, auf Ihren mobilen Geräten die Auto-Updatefunktion für das Betriebssystem und die installierten Apps einzuschalten.

Anlage 1: Anforderungen für Praxen, Nr. 23

Mobiltelefon

Update von Mobiltelefonen

Gültig ab 01.04.2021

Alle Praxen
Bitte prüfen Sie regelmäßig, ob es für Ihre Mobiltelefone Softwareupdates gibt, und installieren Sie diese.

Anlage 1: Anforderungen für Praxen, Nr. 27

Wechsel-datenträger/ Speicher-medien

Angemessene Kennzeichnung der Datenträger beim Versand

Gültig ab 01.04.2021

Alle Praxen
Kennzeichnen Sie die zu versendenden Datenträger so, dass die Bezeichnung für Dritte keinen Rückschluss auf betroffene Patienten, Diagnosen, Fachgebiete etc. zulässt.

Anlage 1: Anforderungen für Praxen, Nr. 29

Sichere Versandart und Verpackung

Gültig ab 01.04.2021

Alle Praxen
Bitte informieren Sie sich bei Ihrem Versand-Dienstleister über entsprechende Angebote. Versenden Sie keine USB-Sticks per Geschäftsbrief.

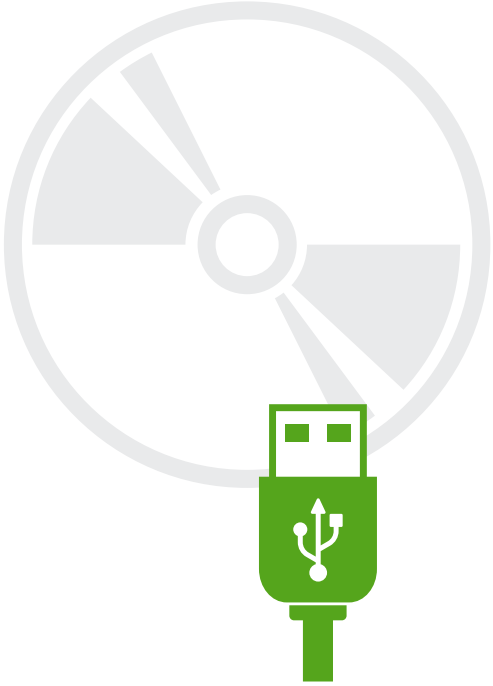
Anlage 1: Anforderungen für Praxen, Nr. 30

Datenträgerverschlüsselung

Gültig ab 01.04.2021

Große Praxen
Wechseldatenträger **sollten** vollständig verschlüsselt werden. Es sollte ein sicheres Verschlüsselungsverfahren eingesetzt werden. Empfehlungen zu geeigneten Algorithmen und Schlüssellängen bieten die Technischen Richtlinien des BSI (TR-02102). Mittels Open-Source-Lösungen wie VeraCrypt können entsprechend verschlüsselte Container angelegt werden.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 10



Netzwerk-sicherheit

Absicherung der Netzübergangspunkte

Gültig ab 01.04.2021

Alle Praxen
Trennen Sie bei größeren Praxis-Netzwerken die sensiblen Bereiche (PVS-Server, medizinische Geräte) von unkritischen bzw. öffentlichen Bereichen (Webserver) durch eine oder mehrere Hardware-Firewalls.
Erfolgt Ihre Anbindung an die Telematikinfrastruktur im sog. Reihenbetrieb, kann der Übergang ins Internet über den Konnektor erfolgen. Hierzu benötigen Sie den optionalen sicheren Internet-Service SIS. In diesem Fall nutzen Sie die im Konnektor integrierte Firewall.
Im Fall des Parallelbetriebs erfolgt die Internetanbindung über eine separate Firewall.
Sie sollten sich bei den Firewallregeln von der Maßgabe „Alles ist verboten, außer es wird explizit erlaubt" leiten lassen. Wenn keine Dienste nach außen angeboten werden sollen, können alle eingehenden Verbindungen von der Firewall geblockt werden. Dies ist in der Regel die Standardeinstellung.

Lassen Sie sich bei komplexeren Netzwerken von Ihrem IT-Dienstleister unterstützen.

Anlage 1: Anforderungen für Praxen, Nr. 32

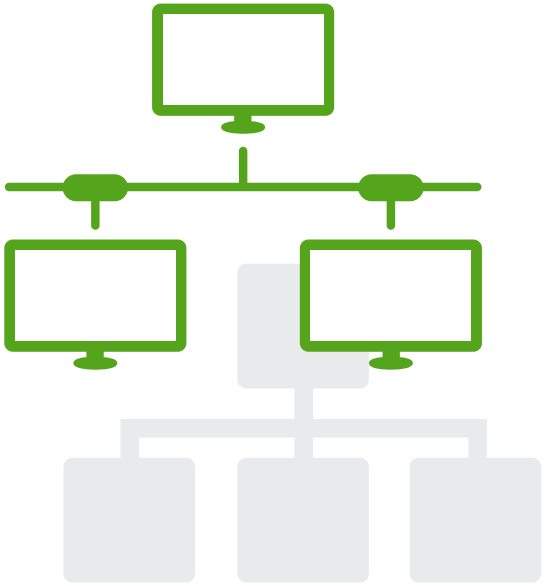
Dokumentation des Netzes

Gültig ab 01.04.2021

Alle Praxen
Für Ihr Praxisnetz muss eine Dokumentation vorliegen, die den aktuellen Status Ihres Netzes wiedergibt. Dies schließt einen Netzplan mit allen an das Netzwerk angeschlossenen Geräten wie PCs, Server, Router, Switches, medizinischen Geräten, Bürogeräten etc. mit ein. Zusätzlich müssen alle für die Netzwerkkommunikation wesentlichen Einstellungen erfasst werden (Routen, IP-Adressen, Firewallregeln etc.). Siehe Musterdokument „Netzplan" der KBV.

Lassen Sie sich bei komplexeren Netzwerken von Ihrem IT-Dienstleister unterstützen.

Anlage 1: Anforderungen für Praxen, Nr. 33



Medizinische Großgeräte

Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen

Gültig ab 01.07.2021

Bei Nutzung medizinischer Großgeräte
Der Zugriff auf Konfigurations- und Wartungsschnittstellen muss auf einen festgelegten Kreis von dazu autorisierten Mitarbeitern beschränkt werden, damit niemand im Netzwerk an medizinische Daten gelangen kann. Standardkonten müssen gelöscht oder mit einem neuen Passwort geschützt werden. Alle Zugangsdaten müssen sicher aufbewahrt und jederzeit verfügbar sein.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 1

Nutzung sicherer Protokolle für die Konfiguration und Wartung

Gültig ab 01.07.2021

Bei Nutzung medizinischer Großgeräte
Benutzen Sie für Konfiguration und Wartung von medizinischen Großgeräten ausschließlich sichere Protokolle wie HTTPS oder SSH.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 2

Deaktivierung nicht genutzter Benutzerkonten

Gültig ab 01.07.2021

Bei Nutzung medizinischer Großgeräte
Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert oder gelöscht werden. Auch Konten, die nur gelegentlich für Fernwartungszwecke benötigt werden, sollten nur für die Fernwartung aktiviert werden.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 5

Hinweise zur nach §75b SGB V

IT-Sicherheitsrichtlinie

mit Umsetzungsdatum ab

2022

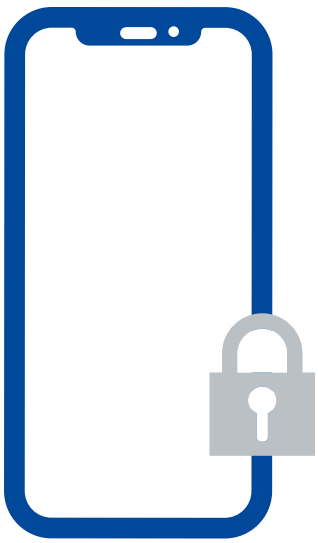
Mobile Anwendungen (Apps)

Sichere Speicherung lokaler App-Daten

Gültig ab 01.01.2022

Alle Praxen
Android und iOS verschlüsseln standardmäßig das gesamte Gerät. Bitte deaktivieren Sie diese Funktion in keinem Fall.

Anlage 1: Anforderungen für Praxen, Nr. 3



Internet-Anwendungen

Firewall benutzen

Gültig ab 01.01.2022

Alle Praxen
In dem seltenen Fall, dass Sie Webanwendungen auf einem eigenen Webserver in Ihrem Praxisnetz betreiben, können Sie zur Erhöhung der Sicherheit eine sog. Web Application Firewall (WAF) einsetzen. Es handelt sich hierbei nicht um eine Standard-Firewall, sondern um eine sog. Application Layer Firewall, die auf das Protokoll HTTP spezialisiert ist.

Da die Konfiguration eines solchen Firewalls sehr komplex ist, sprechen Sie bitte ggfs. Ihren IT-Dienstleister an.

Anlage 1: Anforderungen für Praxen, Nr. 9

Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen

Gültig ab 01.01.2022

Alle Praxen
In dem seltenen Fall, dass Sie Webanwendungen auf einem eigenen Webserver in Ihrem Praxisnetz betreiben, sollten Sie Ihre Webanwendungen durch Captcha-Mechanismen oder Anmeldeverzögerungen vor automatisierten Eingaben schützen. Diese Maßnahmen müssen bereits bei der Entwicklung der Anwendungen berücksichtigt werden.

Anlage 1: Anforderungen für Praxen, Nr. 11

Zugriffskontrolle bei Webanwendungen

Gültig ab 01.01.2022

Mittlere und große Praxen
In dem seltenen Fall, dass Sie Internetanwendungen auf einem eigenen Webserver in Ihrem Praxisnetz betreiben, muss es ein Rechtekonzept geben, das durch eine Authentisierungs- und Autorisierungskomponente in der jeweiligen Anwendung technisch umgesetzt wird. Diese Maßnahmen müssen bereits bei der Entwicklung der Anwendungen berücksichtigt werden.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 2

Endgeräte

Regelmäßige Datensicherung

Gültig ab 01.01.2022

Alle Praxen
Erstellen Sie ein Backup-Konzept, das regelt, wann und in welchem Umfang Ihre Daten gesichert werden. Falls Sie wesentliche praxisrelevante Daten auf den PCs speichern, müssen auch hier Datensicherungen erfolgen. Das Konzept muss tägliche, wöchentliche und monatliche Teil- und Vollsicherungen festlegen. Speichern Sie Ihre Backups grundsätzlich zusätzlich auch auf entfernbaren Datenträgern oder externen Festplatten, die nach der Sicherung vom Rechner getrennt und an einem sicheren Ort aufbewahrt werden. Der Ort muss diebstahl- und brandgeschützt sein. So sind sie für Schadsoftware wie Verschlüsselungs-Trojaner nicht erreichbar.

Erstellen Sie, wenn möglich, verschlüsselte Datensicherungen. Testen Sie die Wiederherstellung von Daten mit den Sicherungen regelmäßig.

Weitere Informationen finden Sie auch im BSI-Grundschutzkompendium im Baustein CON.3.

Anlage 1: Anforderungen für Praxen, Nr. 14

Nutzung von TLS

Gültig ab 01.01.2022

Mittlere und große Praxen
Achten Sie bitte unbedingt darauf, dass alle genutzten Internetverbindungen das sichere Protokoll HTTPS verwenden, das auf Transport Layer Security (TLS) basiert. Dies erkennen Sie z. B. an dem Schloss, das bei sicheren Verbindungen im Adressfeld des Webbrowsers angezeigt wird. Die URLs beginnen dann auch mit https:// statt mit http://. Viele Browser versuchen sogar automatisch das Protokoll HTTPS zu verwenden.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 3

Restriktive Rechtevergabe

Gültig ab 01.01.2022

Mittlere und große Praxen
Legen Sie für jeden Benutzer einen eigenen Account an. Logins dürfen nicht von mehreren Benutzern gemeinsam genutzt werden. Fassen Sie Benutzer mit gleichen Berechtigungen zu Gruppen zusammen. Arbeiten Sie nur mit dem Administrator-Konto, wenn Sie wirklich Administrator-Rechte benötigen. Halten Sie den Kreis der Administratoren klein. Legen Sie Freigaben nur an, wenn dies unumgänglich ist. Schützen Sie insbesondere auch Systemdateien vor unberechtigtem Zugriff. Lassen Sie sich von dem Prinzip leiten, dass jeder Mitarbeiter nur so viele Berechtigungen erhält, wie er zur Erfüllung seiner Aufgaben benötigt. Unterziehen Sie die Berechtigungen einer regelmäßigen Revision. Denken Sie bitte auch daran, Personalzu- und abgänge zu berücksichtigen.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 4

Endgeräte mit dem Betriebssystem MS Windows

Konfiguration von Synchronisationsmechanismen

Gültig ab 01.01.2022

Alle Praxen
Die Synchronisation von Nutzerdaten mit Microsoft-Clouddiensten **sollte** vollständig deaktiviert bzw. deinstalliert werden (z. B. One-Drive).

Anlage 1: Anforderungen für Praxen, Nr. 16

Datei- und Freigabeberechtigungen

Gültig ab 01.01.2022

Alle Praxen
Legen Sie für jeden Benutzer einen eigenen Account an. Logins dürfen nicht von mehreren Benutzern gemeinsam genutzt werden. Fassen Sie Benutzer mit gleichen Berechtigungen zu Gruppen zusammen. Arbeiten Sie nur mit dem Administrator-Konto, wenn Sie wirklich Administrator-Rechte benötigen. Legen Sie Freigaben nur an, wenn dies unumgänglich ist. Lassen Sie sich von dem Prinzip leiten, dass jeder Mitarbeiter nur so viele Berechtigungen erhält, wie er zur Erfüllung seiner Aufgaben benötigt. Unterziehen Sie die Berechtigungen einer regelmäßigen Revision. Denken Sie bitte auch daran, Personalzu- und abgänge zu berücksichtigen.

Anlage 1: Anforderungen für Praxen, Nr. 17

Datensparsamkeit

Gültig ab 01.01.2022

Alle Praxen
Verarbeiten Sie so wenig personenbezogene Daten wie möglich und beachten Sie dabei die Zweckbindung. Löschen Sie zeitnah nicht mehr benötigte Daten gemäß den Angaben in Ihrem Verzeichnis der Verarbeitungstätigkeiten (Artikel 30 Datenschutzgrundverordnung (DSGVO)).

Anlage 1: Anforderungen für Praxen, Nr. 18

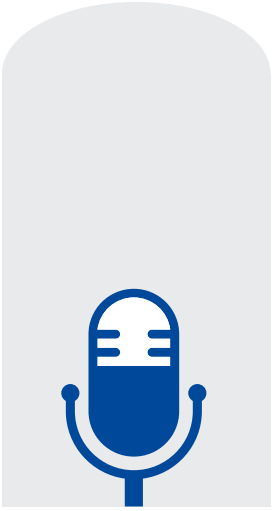
Sichere zentrale Authentisierung in Windows-Netzen

Gültig ab 01.07.2022

Mittlere und große Praxen
Bei großen Windows-Netzen **sollte** eine zentrale Authentisierung mit Single-Sign-On über das sog. Kerberos-Protokoll (Authentisierungsverfahren für Windows) realisiert werden. Hierzu ist üblicherweise ein zentraler Verzeichnisdienst für Windows (Active Directory) zu installieren.

Wegen der Komplexität des Themas empfehlen wir Ihnen, sich ggfs. mit Ihrem IT-Dienstleister in Verbindung zu setzen.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 5



Smartphone und Tablet

Sichere Grundkonfiguration für mobile Geräte

Gültig ab 01.01.2022

Alle Praxen
Aktivieren Sie auf den mobilen Geräten einen Sperrbildschirm und legen Sie eine PIN bzw. ein Passwort zum Entsperren fest. Aktivieren Sie, falls nicht standardmäßig eingestellt, die Verschlüsselung des Geräts und bei Android auch der SD-Karte falls vorhanden. Aktivieren Sie Sicherheitseinstellungen wie das Zurücksetzen des Geräts bei mehr als z. B. zehn erfolglosen Entsperrversuchen. Deinstallieren Sie Apps, die nicht benötigt werden.

Anlage 1: Anforderungen für Praxen, Nr. 21

Datenschutz-Einstellungen

Gültig ab 01.01.2022

Alle Praxen
Jeder App dürfen nur die minimal notwendigen Berechtigungen zugewiesen werden. Hierbei geht es beispielsweise um den Zugriff auf Kamera, Mikrofon, Standort, Telefon, SMS, Kontaktlisten, Speicher etc.

Anlage 1: Anforderungen für Praxen, Nr. 24

Verwendung von Sprachassistenten

Gültig ab 01.01.2022

Mittlere und große Praxen
Nutzen Sie Sprachassistenten wirklich nur dann, wenn es unabdingbar ist.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 7

Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten

Gültig ab 01.07.2022

Mittlere und große Praxen
Regeln Sie in einer verbindlichen Richtlinie, wie mobile Endgeräte in Ihrer Praxis verwendet werden dürfen. Regeln Sie u. a. auch, wie die Geräte aufzubewahren sind und was bei Verlust zu tun ist. Siehe Musterdokument „Muster-Richtlinie – Mobile Geräte" der KBV.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 6

Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets

Gültig ab 01.01.2022

Große Praxen
Siehe Punkt: „Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten" (siehe links unten).

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 1

Definition der erlaubten Informationen und Applikationen auf mobilen Geräten

Gültig ab 01.01.2022

Große Praxen
Alle Informationen, die dienstlich auf den Geräten verarbeitet werden sollen, **sollten** vorab definiert werden.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 3

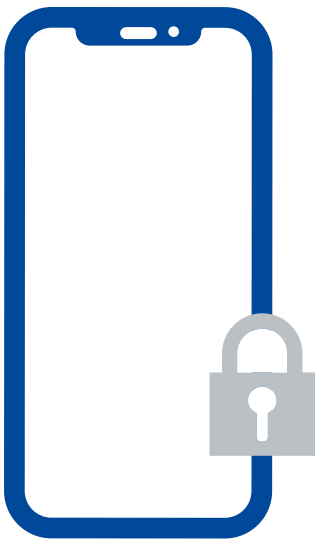
Mobiltelefon

Auswahl und Freigabe von Apps

Gültig ab 01.07.2022

Große Praxen
Alle Apps, die dienstlich genutzt werden sollen, **sollten** über einen definierten Freigabeprozess geprüft und freigegeben werden.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 2



Sperrmaßnahmen bei Verlust eines Mobiltelefons

Gültig ab 01.01.2022

Alle Praxen
Bei Verlust des Mobiltelefons muss die SIM-Karte schnellstmöglich beim Mobilfunkanbieter gesperrt werden.

Anlage 1: Anforderungen für Praxen, Nr. 25

Nutzung der Sicherheitsmechanismen von Mobiltelefonen

Gültig ab 01.01.2022

Alle Praxen
Auch bei den Mobiltelefonen **sollten**, wie bei den Smartphones und Tablets, die verfügbaren Sicherheitsmechanismen aktiviert werden.

Anlage 1: Anforderungen für Praxen, Nr. 26

Wechseldatenträger/Speichermedien

Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Gültig ab 01.07.2022

Mittlere und große Praxen
Erstellen Sie eine Sicherheitsrichtlinie für die Mobiltelefon-Nutzung. Regeln Sie insbesondere die Erstkonfiguration, Beschaffung, Administration und Verlustmeldung etc. Orientieren Sie sich hierbei an dem Musterdokument „Muster-Richtlinie – Mobile Geräte“ der KBV.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 8

Sichere Datenübertragung über Mobiltelefone

Gültig ab 01.01.2022

Mittlere und große Praxen
Legen Sie fest, ob, wie und für welche Daten eine Datenübertragung per Mobiltelefon stattfinden darf. Da Mobiltelefone nur sehr eingeschränkte Möglichkeiten der Datenübermittlung bieten, dürfte dieser Punkt in den allermeisten Fällen für Sie nicht relevant sein.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 9

Schutz vor Schadsoftware

Gültig ab 01.01.2022

Alle Praxen
Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.

Anlage 1: Anforderungen für Praxen, Nr. 28

Sicheres Löschen der Datenträger vor und nach der Verwendung

Gültig ab 01.01.2022

Alle Praxen
Wiederbeschreibbare mobile Datenträger müssen nach jeder Verwendung mit geeigneten Programmen vollständig und sicher gelöscht werden. Hierzu verwenden Sie vom BSI empfohlene Programme bzw. bei Festplatten vom SSD-Typ die Programme des jeweiligen Herstellers.

Anlage 1: Anforderungen für Praxen, Nr. 31

Regelung zur Mitnahme von Wechseldatenträgern

Gültig ab 01.01.2022

Mittlere und große Praxen
Erstellen Sie eine Richtlinie zur Mitnahme von Wechseldatenträgern. Regeln Sie insbesondere die Prüfung auf Malware, Datenverschlüsselung, Entsorgung und Verlustmeldung etc. Orientieren Sie sich hierbei an dem Musterdokument „Muster-Richtlinie – Wechseldatenträger" der KBV.

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 10

Integritätsschutz durch Checksummen oder digitale Signaturen

Gültig ab 01.01.2022

Große Praxen
Sichern Sie optional die Integrität der Daten auf den mobilen Datenträgern durch Aufbringung einer qualifizierten elektronischen Signatur (QES).

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 11

Mobile Device Management (MDM)

Sichere Anbindung der mobilen Endgeräte an die Institution

Gültig ab 01.01.2022

Große Praxen
Sie **sollten** eine sichere Anbindung an das Praxisnetz mithilfe eines MDM realisieren. Kommerzielle MDM-Systeme (wie Citrix XenMobile, Cortado etc.) bieten die geforderte sichere Anbindung an das Praxisnetz in der Regel „out of the box" an.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 4

Berechtigungsmanagement im MDM

Gültig ab 01.01.2022

Große Praxen
Sie **sollten** ein Berechtigungskonzept für die Administration des MDM nach dem Minimalprinzip erstellen und die vergebenen Berechtigungen regelmäßig auf Aktualität prüfen.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 5

Verwaltung von Zertifikaten

Gültig ab 01.01.2022

Große Praxen
Falls Sie Zertifikate zur Nutzung von Diensten auf den Mobilgeräten einsetzen, **sollten** Sie diese mit dem MDM zentral verwalten, d. h. installieren, deinstallieren und aktualisieren.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 6

Fernlöschung und Außerbetriebnahme von Endgeräten

Gültig ab 01.01.2022

Große Praxen
Sie **sollten** sicherstellen, dass Sie mit dem MDM bei Bedarf (Ausscheiden von Mitarbeitern, Verlust, Diebstahl) sämtliche Daten auf den mobilen Endgeräten aus der Ferne löschen können.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 7

Festlegung erlaubter Informationen auf mobilen Endgeräten

Gültig ab 01.01.2022

Große Praxen
Sie **sollten** festlegen, welche Informationen auf den mobilen Endgeräten gespeichert und verarbeitet werden dürfen. Die Auswahl der durch ein MDM zugelassenen Apps stellt für sich schon eine Einschränkung bzgl. der möglichen Nutzung des Endgeräts dar.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 9

Auswahl und Freigabe von Apps

Gültig ab 10.07.2022

Große Praxen
Sie **sollten** mit einem MDM-Standardkatalog die Apps bereitstellen, die die Nutzer auf den Mobilgeräten verwenden dürfen.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 8

Netzwerk-sicherheit

Grundlegende Authentisierung für den Netzwerkmanagement-Zugriff

Gültig ab 01.01.2022

Alle Praxen
Ändern Sie alle gesetzten Standardpasswörter! Wählen Sie für alle Managementzugriffe auf Netzkomponenten starke Passwörter (z. B. mindestens zwölf Zeichen zusammengesetzt aus Buchstaben, Zahlen und Sonderzeichen).

Anlage 1: Anforderungen für Praxen, Nr. 34

Umfassende Protokollierung, Alarmierung und Logging von Ereignissen

Gültig ab 01.01.2022

Mittlere und große Praxen
Sicherheitsrelevante Ereignisse, die von Ihren Systemen gemeldet werden, **sollten** an ein zentrales System- und Netzwerküberwachungstool übermittelt und dort angezeigt und protokolliert werden. Neben kommerziellen sog. SIEM-Systemen gibt es auch freie Open-Source-Lösungen wie z. B. Icinga.

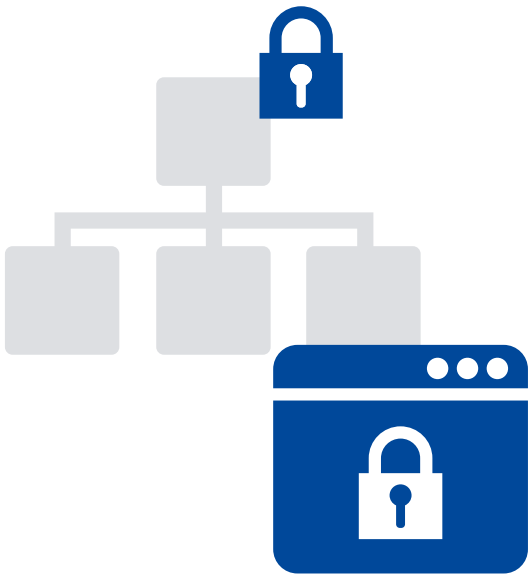
Anlage 2: Zusätzliche Anforderungen für mittlere Praxen, Nr. 11

Absicherung von schützenswerten Informationen

Gültig ab 01.01.2022

Große Praxen
Gewährleisten Sie, dass Daten mit hohem Schutzbedarf nur über entsprechend gesicherte Verbindungen übertragen werden (z. B. VPN, HTTPS, SSH, SFTP, SMBv3 mit Verschlüsselung). Nutzen Sie hierbei Algorithmen und Schlüssellängen, die dem Stand der Technik (BSI TR-02102-1) genügen. Nur bei der Kommunikation über vertrauenswürdige (physisch gesicherte) Netzsegmente kann hierauf verzichtet werden.

Anlage 3: Zusätzliche Anforderungen für große Praxen, Nr. 12



Medizinische Großgeräte

Protokollierung

Gültig ab 01.01.2022

Bei Nutzung medizinischer Großgeräte
Um Fehlfunktionen und mögliche Sicherheitsvorfälle erkennen zu können, müssen die Protokollfunktionalitäten der medizinischen Großgeräte entsprechend konfiguriert und ausgewertet werden. Protokollieren Sie Systemereignisse – nicht die medizinischen Daten. Bestimmen Sie, wer Zugriff auf die Protokolldaten erhält, z. B. die Administratoren.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 3

Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen

Gültig ab 01.01.2022

Bei Nutzung medizinischer Großgeräte
Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden. Stellen Sie sicher, dass auf diese Geräte nicht von außerhalb Ihrer Praxis zugegriffen werden kann.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 4

Netzsegmentierung

Gültig ab 01.01.2022

Bei Nutzung medizinischer Großgeräte
Hängen Sie medizinische Großgeräte niemals in öffentliche Netzwerkbereiche, da diese dann ggf. vom Internet zugänglich sein könnten. Die medizinischen Großgeräte **sollten** in einem eigenen Netzsegment betrieben werden. Verbinden Sie dieses Netzsegment über eine Firewall mit den weiteren Netzsegmenten. Erlauben Sie nur notwendige Kommunikationsverbindungen.

Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte, Nr. 6

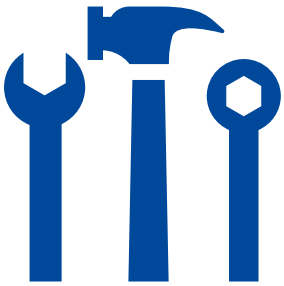
Dezentrale Komponenten der TI

Planung und Durchführung der Installation

Gültig ab 01.01.2022

Alle Praxen
Achten Sie bitte darauf, dass der IT-Dienstleister bei der Installation ein Installationsprotokoll ausfüllt. Idealerweise nutzt er das Muster-Installationsprotokoll „Sichere TI-Installation“ der gematik. Das Protokoll soll neben technischen Details auch einen Vermerk über die Beratung zu sicherheitsrelevanten Aspekten enthalten. Sprechen Sie Ihren IT-Dienstleister an, wenn Sie gravierende Abweichungen feststellen.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 1



Betrieb

Gültig ab 01.01.2022

Alle Praxen
Informationen zum Betrieb erhalten Sie auf der Webseite der gematik sowie von den Herstellern der TI-Komponenten.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 2

Schutz vor unberechtigtem physischem Zugriff

Gültig ab 01.01.2022

Alle Praxen
Schützen Sie die TI-Komponenten vor dem physischen Zugriff unberechtigter Personen, insbesondere Patienten, durch Aufstellung in abschließbaren Schränken oder Räumen.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 3

Betriebsart „parallel“

Gültig ab 01.01.2022

Alle Praxen
In Praxen mit einer größeren Anzahl von Endgeräten kann die Betriebsart „parallel“ sinnvoll sein. Der Internetzugang wird hierbei über einen separaten Router realisiert, der gleichzeitig die Rolle einer Firewall für die Anbindung an das Internet übernehmen kann. Auch hier sollten wieder die Leitsätze „Alles, was nicht explizit erlaubt ist, ist verboten“ und „So wenig wie möglich erlauben“ gelten.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 4

Zeitnahes Installieren verfügbarer Aktualisierungen

Gültig ab 01.01.2022

Alle Praxen
Prüfen Sie fortwährend, ob Updates für Ihre TI-Komponenten vorliegen, und installieren Sie diese umgehend. Ggfs. bieten Ihre TI-Komponenten eine Autoupdate-Funktion an.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 6

Sicheres Aufbewahren von Administrationsdaten

Gültig ab 01.01.2022

Alle Praxen
Lassen Sie sich die notwendigen Informationen von Ihrem Dienstleister aushändigen und bewahren Sie diese sicher auf. Wenn der Dienstleister die Informationen nicht zur Verfügung stellen möchte, achten Sie auf eine vertraglich fixierte, angemessen kurze Reaktionszeit und eine Herausgabe der Informationen bei Vertragsende. Ggfs. besteht auch die Möglichkeit, die Administrationsdaten in einem versiegelten Umschlag zu erhalten, um im Notfall selbst auf die TI-Komponenten zugreifen zu können. Wenn der Umschlag geöffnet wurde, sollten Sie dies dem Dienstleister anzeigen.

Anlage 5: Anforderungen für Dezentrale Komponenten der Telematikinfrastruktur, Nr. 7

Grundlegende Empfehlungen der KVWL zur

IT-Sicherheit

Diese Empfehlungen stellen ergänzende Informationen der KVWL zur IT-Sicherheit in Ihren Praxen dar. Die erste Version aus Januar 2020 ist im März 2021 an die Anforderungen der IT-Sicherheitsrichtlinie angepasst worden. Die Umsetzung dieser grundlegenden Empfehlungen ist gesetzlich nicht vorgeschrieben. Sie ersetzen nicht die IT-Sicherheitsrichtlinie sowie die individuelle eigene Analyse und Risikobewertung, die sinnvollerweise auch einen externen Systembetreuer mit einschließen sollte.

Organisation

- Informieren Sie sich und Ihr Praxispersonal regelmäßig zu aktuellen Sicherheitsproblemen und -techniken, z. B. auf der Website des BSI unter der Rubrik „Verbraucherinnen und Verbraucher“.
- Sprechen Sie die Themen Sicherheit und Datenschutz regelmäßig in Ihrer Praxis an, damit Ihnen grundlegende Gefahren wie Verschlüsselungstrojaner / Ransomware sowie Gegenmaßnahmen dazu bekannt sind (z. B. dass nicht unbedacht jeder Mailanhang geöffnet wird). Sinnvollerweise kann Ihr Datenschutzbeauftragter oder Systembetreuer hierbei unterstützen.
- Lassen Sie Fernwartungen von externen Technikern nur nach vorheriger Absprache zu. Halten Sie die nötigen Passwörter oder Codes unter Verschluss.
- Beachten Sie schon bei der Beschaffung von neuen IT-Geräten deren Sicherheitsfunktionen.
- Lassen Sie niemals Dienstleister (z. B. IT-Support) Tests mit echten Patientendaten durchführen. Entweder werden diese vorher anonymisiert oder der Dienstleister muss selber generierte Daten ohne Patientenbezug verwenden.

Smartphone und Tablet

- Schalten Sie den Passwortschutz des Gerätes ein, ggf. kombiniert mit Fingerabdruck oder Gesichtserkennung.
- Speichern Sie keine unverschlüsselten Patientendaten auf Smartphones oder Tablets.
- Schalten Sie zum Schutz der eigenen Daten, Bilder, Kontakte oder Kalender insbesondere bei Android-Geräten auch die Verschlüsselung des Speichers ein.

Office-Produkte

- Löschen Sie regelmäßig den „Papierkorb“ im System (meist über einen Rechtsklick auswählbar), damit sensible Dokumente wirklich gelöscht werden. Denn in den meisten Systemen werden Dokumente beim Löschen erst nur in einen „Papierkorb“ verschoben, sind dort aber weiterhin zugreifbar.

Internet-Anwendungen

- Trennen Sie private und dienstliche Tätigkeiten im Internet (Surfen, Social Media, Chatten etc.), da sonst die Angriffsfläche vergrößert wird.
- Nutzen Sie einen gesonderten Rechner für Internetrecherchen und nicht den PVS-PC.
- Setzen Sie Skript- und Werbeblocker ein, die im Browser als Erweiterung installiert werden können. Hierdurch werden viele unnötige – und teilweise auch schadhafte – Inhalte rausgefiltert.

Endgeräte

- Schalten Sie die in Windows enthaltene Firewallfunktion ein. Oft bringen heute die Sicherheitsprogramme namhafter Hersteller neben dem Virenschutzprogramm auch eine Firewallfunktion mit, die verwendet werden kann.
- Vergeben Sie unterschiedliche Passwörter für die Anmeldung am Betriebssystem und an Ihrem Praxisverwaltungssystem (PVS).
- Richten Sie zum Schutz vor Daten-Diebstahl eine Festplattenverschlüsselung ein. Wenn hierbei – abhängig vom Betriebssystem und verwendeter Software – Passwörter nötig sind, verwenden Sie hierfür komplexe Passwörter und hinterlegen diese an sicheren Stellen (z. B. Passwort-Tresor-Programme).
- Installieren Sie keine dienstlich unnötigen Programme (Spiele, Chats, Video etc.) auf den Praxisrechnern.

Wechseldatenträger/ Speichermedien

- Vernichten Sie alte Festplatten mit Patientendaten physisch oder überschreiben Sie diese mehrfach mit Zufallsdaten; hierzu verwenden Sie vom BSI empfohlene Programme bzw. bei neueren Festplatten des SSD-Typs die Programme des jeweiligen Herstellers. Alternativ beauftragen Sie einen Dienstleister mit der Entsorgung/ Zerstörung der Platten.

Netzwerksicherheit

- Schalten Sie die WLAN-Funktion aus, wenn sie nicht zwingend benötigt wird.
- Stellen Sie Server und Netzwerkkomponenten zutrittsgeschützt auf (z. B. abgeschlossener Raum oder abgeschlossener Schrank).
- Schalten Sie die Verschlüsselung (mindestens WPA2) an, falls WLAN für interne Zwecke der Praxis nötig ist. Nutzen Sie lange und sichere Passwörter zur Einwahl. Schalten Sie den Netzwerknamen (SSID) auf unsichtbar. Legen Sie die zugelassenen Geräte im Router fest (MAC-Filter).
- Nutzen Sie die Gast-WLAN-Funktionen des Routers, falls Sie Ihren Patienten ein WLAN im Wartezimmer bereitstellen möchten. Hierdurch wird Ihr internes WLAN vom Gast-WLAN getrennt.
- Schalten Sie die im DSL-Router enthaltene Firewallfunktion ein. Sperren Sie dabei alle Netzverbindungen von außen.

Medizinische Großgeräte

- Schalten Sie wenn möglich die Verschlüsselung der gespeicherten medizinischen Daten ein, damit niemand durch den Diebstahl des Gerätes oder seiner Speicher an Patientendaten gelangen kann.

Dezentrale Komponenten der TI

- Wenn Sie keine Internetdienste nutzen wollen und nur wenige Endgeräte in Ihrem Netzwerk verwenden, empfehlen wir Ihnen, den Konnektor in Reihe zu schalten. Im Reihenbetrieb befinden sich alle Komponenten im selben Praxisnetzwerk und erhalten Zugang über den Konnektor zur TI. Durch die integrierte Firewall des Konnektors wird das Praxisnetz vor unautorisierten Zugriffen von außen geschützt. Im Reihenbetrieb kann optional der Sichere Internet Service (SIS) aktiviert werden, um im Praxisnetzwerk einen Internetzugang zu ermöglichen, um beispielsweise Updates des Betriebssystems oder des PVS herunterzuladen. In diesem Fall baut der Konnektor einen zweiten sicheren Kanal zum SIS des Zugangsdienstbetreibers auf. Detaillierte Informationen zum Leistungsangebot des SIS erhalten Sie von Ihrem Zugangsdienstbetreiber.
- Der Reihenbetrieb ermöglicht auch durch eine Netztrennung einen uneingeschränkten Internetzugang für Geräte, die direkt an den Internetrouter angeschlossen sind. Der Konnektor setzt dabei eine Netztrennung zwischen dem Praxisnetz und dem Netz mit direktem Internetzugang durch. Für das Praxisnetz kann der optionale SIS aktiviert werden.
- Stellen Sie – aus Haftungsgründen – sicher, dass die TI-Geräte (Konnektor, Chipkartenleser etc.) ordnungsgemäß aufgestellt und betrieben werden. Hierzu gehört, dass der Konnektor an einem zugriffsgeschützten Ort installiert wird, angebotene Sicherheitsupdates für den Konnektor und das Kartenterminal stets umgehend eingespielt werden sowie eine regelmäßige Kontrolle, dass die Geräte unverändert sind (Gehäuse, Siegel), und keine unerlaubten Geräte angeschlossen wurden. Informieren Sie bei Beschädigungen sofort den Support.

Weitere Informationen zur TI unter:
Telematikinfrastruktur – das digitale Netz für alle Leistungserbringer im Gesundheitswesen

E-Mail

- Versenden Sie personenbezogene / medizinische Daten verschlüsselt. Nutzen Sie hierzu die vom BSI empfohlenen Programme bzw. Standards wie S/MIME oder GnuPG. Für einzelne Dateien im Mailanhang kann auch die Verschlüsselung von Archivprogrammen wie WinZIP oder 7zip verwendet werden.
- Trennen Sie private und dienstliche Mailkonten, da sonst die Angriffsfläche vergrößert wird.
- Nutzen Sie bestenfalls einen gesonderten Rechner für den Zugriff auf Mailkonten und nicht den PVS-PC.
- Seien Sie kritisch bei E-Mails mit merkwürdigen Absender- oder Empfängeradressen. Löschen Sie solche E-Mails besser direkt. Weitere Verdachtsmomente sind Inhalte, mit denen man offensichtlich nichts zu tun hat (z. B. Rechnungen von eBay, wenn man dort gar nicht angemeldet ist) oder auch Webadressen und Anhänge, die man unbedingt anklicken oder öffnen soll. Lassen

Sie sich auch nicht von E-Mails, die angeblich von Banken, Polizei oder Behörden kommen, einschüchtern. Solche Behörden würden wirklich relevante Schreiben nicht per E-Mail zustellen.

Drucker

- Stellen Sie Drucker so auf, dass keine Praxisfremden, z. B. Patienten, Zugang dazu bekommen können.
- Vernichten Sie Ausdrucke mit personenbezogenen Daten, die nicht mehr benötigt werden, datenschutzkonform, z. B. per Aktenvernichter (DIN 66399, Cross-Cut). Oder beauftragen Sie einen Dienstleister damit, sogenannte Datenschutz-Tonnen aufzustellen.
- Nehmen Sie gedruckte Dokumente umgehend aus dem Drucker, damit sie nicht längere Zeit offen herumliegen.
- Sollten Sie einen Drucker verwenden, der über eine WLAN-Hotspotfunktion verfügt, denken Sie daran, die Standardeinstellungen (z.B. Passwort) abzuändern.

Telefax

- Stellen Sie Faxgeräte so auf, dass keine Praxisfremden, z. B. Patienten, Zugang dazu bekommen können.
- Verwenden Sie gespeicherte Empfängernummern, um Tippfehler beim Eingeben der Nummern zu vermeiden.
- Schalten Sie die Faxgeräte außerhalb der Dienstzeiten aus, damit niemand Zugriff auf zwischenzeitlich eingegangene Faxe im Gerät hat.
- Vereinbaren Sie bei sensiblen Daten einen Sendezeitpunkt mit dem Empfänger, da Sie als Absender keine Kontrolle über das Faxgerät auf Empfangsseite haben.
- Nutzen Sie alle von den Faxgeräten angebotenen Sicherheitsmaßnahmen (Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Passwort, Sperrung der Fernwartungsmöglichkeit etc.).
- Löschen Sie vor Verkauf, Weitergabe oder Aussortierung alle im Gerät gespeicherten Daten wie z. B. Textinhalte, Verbindungsdaten und Kurzwahlziele.
- Verzichten Sie auf das Versenden von sehr sensiblen Daten per Telefax, da dieses bekannte Schwächen aufweist (insbesondere die fehlende Verschlüsselung). Versuchen Sie, sicherere Kommunikationsformen wie den eArztbrief hierfür zu verwenden.

Notfallplan

- Erstellen Sie einen Notfallplan, um die Abläufe und Zuständigkeiten während der Bewältigung des Notfalles zu regeln und die Beteiligten in die Lage zu versetzen, wieder den Normalbetrieb herzustellen. Bereiten Sie sich auf mögliche Szenarien wie einen Rechner-Ausfall oder Schadsoftware vor.
- Stellen Sie Möglichkeiten eines Notbetriebs auf, z. B. für den Ausfall von PCs, den Aus-

fall des PVS, den Ausfall des Internets oder einen Stromausfall. Halten Sie z. B. einen Ersatzrechner bereit.

- Überlegen Sie, wen Sie im jeweiligen Notfall informieren müssen. Das können je nach Art des Notfalls die Polizei, die Datenschutzbehörden, die Versicherungen oder Patienten sein.

Cyberversicherung

- Eine Cyberversicherung kann im Schadenfall (IT-Ausfall, Schadsoftware, Bedienungsfehler, vorsätzliche Manipulation etc.) die Kosten für Sachverständige, externe Berater, Krisenmanager, Juristen, Presse-/Medienexperten, Call-Center erstatten, Schadenersatz leisten oder auch den Ertragsausfall nach einer Betriebsunterbrechung kompensieren.
- Meist stellt die Versicherung Ansprechpartner zur Verfügung, die im Notfall schnell Hilfe leisten können. Hierzu zählen Service-Hotlines, Sicherheits-Experten und IT-Forensiker.
- Die einzelnen genauen Pflichten und Leistungen sind vor Vertragsabschluss mit der Versicherung zu klären. Da es bei den Verträgen und Rahmenbedingungen durchaus Unterschiede geben kann, sollten Sie mehrere Angebote einholen und vergleichen.

Glossar / Abkürzungen

Active Directory (AD)	MS Windows Verzeichnisdienst
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BSI	Bundesamt für Sicherheit in der Informationstechnik
Checksumme	eine Prüfsumme, mit der die Integrität von Daten überprüft werden kann
Datenverarbeitung	Erhebung, Verarbeitung, Speicherung, Administration und Einsicht in personenbezogene Daten
DSGVO	Datenschutzgrundverordnung
HTTP(S)	(Secure) Hypertext Transfer Protocol, Standardprotokoll im Internet
Icinga	freie System- und Netzwerk-Überwachungssoftware
MDM	Mobile Device Management, System zur zentralisierten Verwaltung von Mobilgeräten
Medizinische Großgeräte	z. B. CT, MRT, PET, Linearbeschleuniger
Minimalprinzip (Rechtevergabe)	nur so viele Berechtigungen wie nötig vergeben
Mobiltelefon	klassisches Handy ohne Touchscreen
QES	qualifizierte elektronische Signatur, die im Rechtsverkehr die handschriftliche Unterschrift ersetzt
SFTP	Secure File Transfer Protocol, Protokoll für die sichere Übertragung von Dateien
SIEM	Security Information and Event Management, System zur zentralen Zusammenführung und Auswertung von Sicherheitsinformationen
SMB	Server Message Block, Protokoll für Datei- und Druckdienste, ab Version 3 ist Verschlüsselung möglich
SSH	Secure Shell, Protokoll für die sichere Fernbedienung von Computern
TI	Telematikinfrastruktur
TLS	Transport Layer Security, Verschlüsselungsprotokoll für sichere Datenübertragung, wird von HTTPS verwendet
VPN	Virtual Private Network, Technik zur sicheren Kopplung von Netzwerken
WAF	Web Application Firewall, auf HTTP spezialisiertes Firewall, z. B. zum Schutz von Webanwendungen

Weitere Informationsquellen

https://hub.kbv.de/display/itsrl

https://www.kbv.de/html/datensicherheit.php

https://www.bsi.bund.de/DE/Themen/
Verbraucherinnen-und-Verbraucher/
verbraucherinnen-und-verbraucher_node.html

https://www.bsi.bund.de/DE/Themen/
Unternehmen-und-Organisationen/
Standards-und-Zertifizierung/
IT-Grundschutz/IT-Grundschutz-Kompendium/
it-grundschutz-kompendium_node.html

https://fachportal.gematik.de/

https://www.datenschutzkonferenz-online.de/
kurzpapiere.html

https://www.bundesaerztekammer.de/aerzte/
telematiktelemedizin/
sicherheit-von-gesundheitsdaten/

Impressum

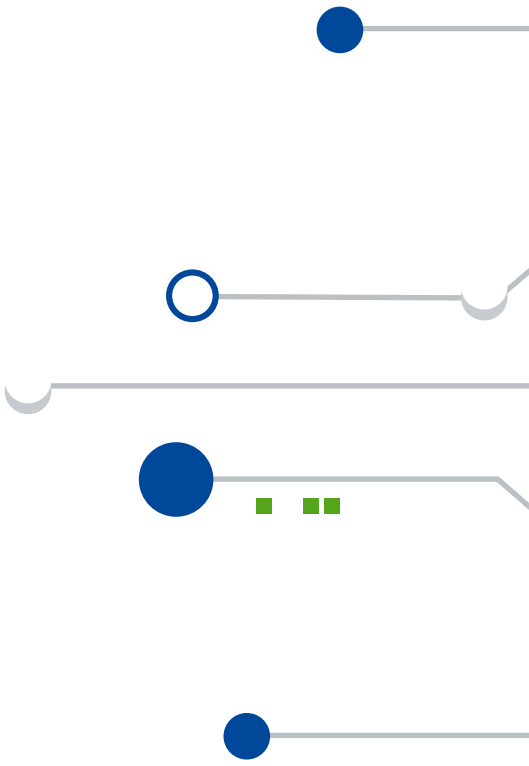
Kassenärztliche Vereinigung
Westfalen-Lippe
Robert-Schimrigk-Straße 4–6
44141 Dortmund

Geschäftsbereich IT & eHealth
E-Mail: mitgliederberatung@kvwl.de
Tel.: 0231/94 32 39 90

www.kvwl.de

Stand: 21. Mai 2021

Ihr Ansprechpartner zum Thema IT-Sicherheit in Praxen ist die Mitglieder-beratung der KVWL: Tel. 0231/94 32 39 90



www.kvwl.de