KVB 80684 München

Geschäftsführung

Ihr Ansprechpartner:
KVB eTec Support
Telefon: 089 57093-40040
Unser Zeichen: GT-DIG

08.05.2025

Neue IT-Sicherheitsrichtlinie nach § 390 SGB V in Kraft getreten und veröffentlicht

Das Wichtigste auf einen Blick:

IT-Sicherheits-richtlinie aktua-lisiert

Zum 1. April 2025 ist die neue IT-Sicherheitsrichtlinie nach § 390 SGB V in Kraft getreten. Neuerungen müssen bis 1. Oktober 2025 von den Praxen umgesetzt werden.

Neue Inhalte

Neu sind insbesondere Regelungen, um das Sicherheitsbewusstsein beim Praxispersonal zu erhöhen und die Mitarbeitenden für Informationssicherheit zu sensibilisieren und zu schulen. Alle Neuerungen sind in der Anlage zu diesem Schreiben aufgeführt.

Sehr geehrte Damen und Herren,

die IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV) nach § 390 SGB V (ehemals § 75b SGB V) wurde überarbeitet und am 7. März 2025 von der Vertreterversammlung der KBV beschlossen. Nach Zustimmung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), ist die aktualisierte Richtlinie zum 1. April 2025 in Kraft getreten und von der KBV veröffentlicht worden.

Die Neuerungen sind innerhalb von sechs Monaten nach dem Inkrafttreten von den Praxen umzusetzen, also spätestens bis 1. Oktober 2025.

Zum Hintergrund

Die KBV ist seit 2020 gesetzlich verpflichtet, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung in Form einer Richtlinie festzulegen und diese regelmäßig „an den Stand der Technik und an das Gefährdungspotenzial anzupassen“. Ziel der IT-Sicherheitsrichtlinie ist es, die IT-Systeme und damit sensible Daten in den Praxen noch besser zu schützen, indem klare Vorgaben zur sicheren Verwaltung von Patientendaten und zur Risikominimierung adressiert werden.

Die Richtlinie bietet einen verlässlichen Rahmen für das, was Praxisinhaber in puncto IT-Sicherheit tun sollten. Dies soll Praxen helfen, sensible Daten noch sicherer zu verwalten und Risiken wie Datenverlust oder Betriebsausfall zu minimieren. Gesundheitsdaten sind stets angemessen zu schützen. Der Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität der Gesundheitsdaten kann schwerwiegende Folgen für Betroffene haben. Gleichzeitig sind die Praxen steten Gefährdungen ausgesetzt, denn Anzahl und Intensität der Angriffe auf IT-Systeme nehmen zu.

Nicht zuletzt vor dem Hintergrund der Einführung der „elektronischen Patientenakte für alle“ gewinnen Maßnahmen zur Gewährleistung der IT-Sicherheit in den Praxen stetig an Bedeutung. Der Schutz von Praxissystemen und Patientendaten behält oberste Priorität.

Die KBV hat sich zum Ziel gesetzt, praktikable und realistische Vorgaben für die Praxen zu erarbeiten, die möglichst aufwandsarm umgesetzt werden können.

Neuerungen in der IT-Sicherheitsrichtlinie

Die wichtigsten Neuerungen in der Richtlinie betreffen Regelungen

- zur Erhöhung des Sicherheitsbewusstseins beim Praxispersonal (Stichwort: Security Awareness),
- zur Sensibilisierung und Schulung des Praxispersonals zur Informationssicherheit,
- zur Sicherung von Daten, beispielsweise wie Daten gesichert werden und wer dafür zuständig ist,
- zur sicheren Konfiguration von E-Mail-Clients und -Servern sowie zum Umgang mit Spam bei E-Mails,
- zum Patch- und Änderungsmanagement, beispielsweise dass Updates zeitnah installiert werden und wer die Updates installiert,
- zur Sicherheit von Cloud-Anwendungen.

Die seit 2021 bereits bestehenden Vorgaben gelten weiter. Aus der Richtlinie gestrichen wurden zeitliche Vorgaben und Fristen, die in der Vergangenheit liegen.

Sie finden alle Anforderungen in der Anlage zu diesem Serviceschreiben. Zur leichteren Auffindbarkeit wurden neue Anforderungen und aktualisierte Inhalte zu bestehenden Vorgaben farblich hervorgehoben.

Aufbau und Gliederung der IT-Sicherheitsrichtlinie

Wie gehabt besteht die IT-Sicherheitsrichtlinie aus fünf Anlagen. Die Unterscheidung der Praxisarten bleibt gleich.

Praxisart		Relevante Inhalte
Praxis	Hier arbeiten **bis zu fünf Personen, die ständig mit der Datenverarbeitung betraut** sind.	• Anlage 1: Anforderungen an alle Praxen für Hardware und Software sowie ***neu* auch für Praxispersonal** • Anlage 5: Anforderungen für dezentrale Komponenten der Telematikinfrastruktur
Mittlere Praxis	Hier sind es **6 bis 20 ständig mit der Datenverarbeitung betraute Personen**.	• Anlage 1 • Anlage 2: Zusätzliche Anforderungen an mittlere Praxen • Anlage 5
Großpraxis	Hier sind **über 20 Personen ständig mit der Datenverarbeitung betraut** oder die Praxis verarbeitet Daten in einem **Umfang, der die normale Datenübermittlung übersteigt** (z.B. Groß-MVZ mit krankenhausähnlichen Strukturen, Großlabor, o.ä.).	• Anlage 1 • Anlage 2 • Anlage 3: Zusätzliche Anforderungen an Großpraxen • Anlage 5
Praxen mit medizinischen Großgeräten	Zum Beispiel Röntgengeräte, CT, MRT, PET, Linearbeschleuniger, Herzkatheter-Messplätze, Dialysegeräte, Gammakameras, Herz-Lungen-Maschinen.	• Anlage 4: Zusätzliche Anforderungen für medizinische Großgeräte

Was ist konkret zu tun?

Prüfen Sie die im Anhang beziehungsweise in der gesamten IT-Sicherheitsrichtlinie aufgeführten Anforderungen, die auf Ihre Praxisart/-konstellation zutreffen, rechtzeitig vor dem 1. Oktober 2025 und konsultieren Sie bei Bedarf Ihren IT-Dienstleister.

Wo finde ich weitere Informationen und Hilfestellung?

Auf unserer Themenseite https://www.kvb.de/mitglieder/praxisfuehrung/it-online-services-ti/it-sicherheitsrichtlinie finden Sie Verlinkungen auf:

- die aktuelle IT-Sicherheitsrichtlinie samt aller Anlagen
- die Internetseite der KBV zu dem Thema, u.a. mit einem Erläuterungs-Video
- eine Online-Plattform der KBV (genannt „Hub“), die Umsetzungshinweise und Begleitinformationen enthält, ebenso wie Musterdokumente für Praxen (z.B. eine Muster-Richtlinie für die Nutzung mobiler Geräte) sowie die häufigsten Fragen und Antworten zu technischen Aspekten

Schon seit mehreren Jahren bieten wir regelmäßig Live-Online-Seminare zu den Themen „IT-Sicherheitsrichtlinie“ und „Cyberschutz“ an. Details und Anmeldemöglichkeiten finden Sie auf unserer Themenseite https://www.kvb.de/mitglieder/praxisfuehrung/fortbildungsangebot.

Die KBV und auch die KV Bayerns planen weiteres Schulungs- und Informationsmaterial zur Unterstützung der Praxisinhaber bei der Umsetzung der Richtlinie bereitzustellen. Im Rahmen des wöchentlichen Newsletters KBV-PraxisNachrichten ist voraussichtlich ab Mai eine Serie zu ausgewählten Aspekten der IT-Sicherheit angedacht. Hierüber sowie über weitere Unterstützungsmaßnahmen informieren wir zu gegebener Zeit gesondert.

Unterstützung durch zertifizierte IT-Dienstleister

Es kann für Praxisinhaber ratsam sein, sich externe Unterstützung zu holen, wenn es um Datensicherheit geht. Die KBV listet in einem Verzeichnis (siehe KBV_ISAP_Dienstleister_ZERT_P390_SGBV.pdf) diejenigen IT-Dienstleister auf, die speziell zur Umsetzung der IT-Sicherheitsrichtlinie zertifiziert wurden. Dies ist ein optionales Angebot. Praxisinhaber können sich auch für einen nicht zertifizierten Dienstleister entscheiden, wenn sie sich Hilfe holen möchten.

Bei allgemeinen Fragen zur Umsetzung der IT-Sicherheitsrichtlinie hilft Ihnen unser KVB eTec Support unter der Telefonnummer **089 57093-400 40** oder unter **technik@kvb.de** gerne weiter.

Freundliche Grüße

gez.

Stephan Spring
Geschäftsführer

Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit – bis 01.10.2025 zu erfüllen

Neue / aktualisierte Inhalte sind in roter Schrift hervorgehoben

Anlage 1: Anforderungen für Praxen

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Personal	Geregelte Einarbeitung neuer Mitarbeitender	Mitarbeitende müssen zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeitenden müssen über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden.	Alle neuen Mitarbeitenden sollten in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und Anwendungen eingewiesen bzw. geschult werden. Es sollten alle Ansprechpartner vorgestellt werden, insbesondere die zu Fragen rund um Informationssicherheit und Datenschutz. Die Sicherheitsziele der Praxis sollten den neuen Mitarbeitenden vorgestellt werden. Alle hausinternen Regelungen und Vorschriften zur Informationssicherheit müssen erläutert werden. Für alle Arten von potenziellen Sicherheitsvorfällen sollten die Verhaltensregeln und Meldewege dargelegt werden. → Vorlage unter Musterdokumente erhältlich
2	Personal	Geregelte Verfahrensweise beim Weggang von Mitarbeitenden	Ausscheidende Mitarbeitende müssen alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen zurückgeben. Zugangsdaten (bspw. Passwörter), die dem ausscheidenden Mitarbeiter bekannt waren oder von ihm genutzt wurden, müssen geändert oder vernichtet werden. Vor der Verabschiedung muss noch einmal auf die fortdauernden Verschwiegenheitsverpflichtungen hingewiesen werden.	Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene Geräte, etc. zurückzufordern. Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Weggang einer der Personen die Zugangsberechtigung zu ändern. Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen

				Informationen weitergegeben werden dürfen. → Vorlage unter Musterdokumente erhältlich
3	Personal	Festlegung von Regelungen für den Einsatz von Fremdpersonal	Externes Personal muss wie alle eigenen Mitarbeitenden dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Kurzfristig oder einmalig eingesetztes Fremdpersonal muss in sicherheitsrelevanten Bereichen beaufsichtigt werden. Ggf. notwendige Zugangsberichtigungen sind so restriktiv wie möglich zu halten.	Externe Mitarbeitende, die eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten. Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind außerdem sämtliche eingerichteten Zugangs-, Zugriffs- und Zutrittsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sollte der Ausscheidende explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, das heißt beispielsweise, dass der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung erlaubt ist.
4	Personal	Vertraulichkeits-vereinbarungen für den Einsatz von Fremdpersonal	Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, müssen mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden.	Zum Abschluss der Vertraulichkeitsvereinbarung kann folgendes Musterdokument verwendet werden. → Vorlage unter Musterdokumente erhältlich
5	Personal	Aufgaben und Zuständigkeiten von Mitarbeitenden	Alle Mitarbeitenden müssen dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Die Mitarbeitenden müssen auf den rechtlichen Rahmen ihrer Tätigkeit hingewiesen werden. Die Aufgaben und Zuständigkeiten von Mitarbeitenden müssen in geeigneter Weise dokumentiert sein. Dabei sollte ebenfalls dokumentiert werden, welche Berechtigungen und Zugänge für die Mitarbeitenden bereitgestellt/genutzt werden. Außerdem müssen alle	Die Dokumentation der Aufgaben und Zuständigkeiten kann in den Arbeitsverträgen oder weiteren Vereinbarungen erfolgen. Für die Dokumentation der Berechtigungen und Zugänge bietet sich ein Formular wie das Musterdokument an. → Vorlage unter Musterdokumente erhältlich

			Mitarbeitenden darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind.	
6	Personal	Qualifikation des Personals	Mitarbeitende müssen regelmäßig geschult bzw. weitergebildet werden, insbesondere auch in Bezug auf die eingesetzte Technik/IT. Es müssen betriebliche Regelungen vorhanden sein, welche mit geeigneten Mitteln sicherstellen, dass die Mitarbeitenden auf einem aktuellen Kenntnisstand sind. Weiterhin sollte den Mitarbeitenden während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.	Werden Stellen besetzt, müssen die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend sollte geprüft werden, ob diese bei den Bewerbenden für die Stelle tatsächlich vorhanden sind. Es muss sichergestellt sein, dass Stellen nur von Mitarbeitenden besetzt werden, für die sie qualifiziert sind.
7	Personal	Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden	Bei der Einstellung neuer Mitarbeitenden sollte besonders auf ihre Vertrauenswürdigkeit, beispielsweise bei der Prüfung vorliegender Arbeitszeugnisse, geachtet werden. Soweit möglich, sollten alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerbenden, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind.	Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder externem Personal überprüfen zu lassen, sind in Deutschland rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitenden überprüft werden, ob - diese hinreichende Referenzen vorweisen können, z. B. aus bisherigen Projekten, und - der vorgelegte Lebenslauf des Bewerbenden aussagekräftig und vollständig ist.
8	Sensibilisierung und Schulung zur Informations-sicherheit	Sensibilisierung der Praxisleitung für Informationssicherheit	Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.	Es ist für den Sicherheitsprozess wichtig, dass dieser aktiv von der Praxisleitung unterstützt wird. Hierfür muss die Praxisleitung den Wert von Informationssicherheit erkannt und verinnerlicht haben. Wichtige Informationen, die dabei für die Praxisleitung relevant sind: - Darstellung der Sicherheitsrisiken und damit verbundenen Kosten - Auswirkungen auf die Geschäftsprozesse - Rechtliche Sicherheitsanforderungen

9	Sensibilisierung und Schulung zur Informations-sicherheit	Einweisung des Personals in den sicheren Umgang mit IT	Alle Mitarbeitenden und externen Benutzenden müssen in den sicheren Umgang mit IT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist.	Um Sicherheitsprobleme durch fehlerhafte Benutzung bzw. Konfiguration der IT zu vermeiden, sollten alle Mitarbeitende in den sicheren Umgang mit den IT-Komponenten der Praxis eingewiesen und geschult werden, soweit dies ihre Arbeitszusammenhänge betrifft. In einer Dokumentation ist zu beschreiben, welche Rahmenbedingungen es beim Einsatz der IT-Komponenten gibt und welche Sicherheitsmaßnahmen zu ergreifen sind. Folgenden Punkte könnten dokumentiert werden: - Hinweis, dass keine IT-Systeme, IT-Komponenten ohne ausdrückliche Erlaubnis benutzt werden dürfen - Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind - Einbringen von externen Daten in das eigene Haus (z.B. USB, Download oder Mailanhang) - Umgang mit Passwörtern - Nutzungsverbot nicht freigegebener Software - Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen, beziehungsweise eine präzise Beschreibung möglicher Ausnahmen von dieser Regel, falls es sie gibt - Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern - Schutz vor Computer-Viren und anderer Schadsoftware - Durchführung von Datensicherungen - Nutzung von Internet- und E-Mail-Diensten
10	Sensibilisierung und Schulung zur Informations-sicherheit	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Alle Mitarbeitenden sollten entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.	Um Sicherheitsprobleme durch fehlerhafte Benutzung bzw. Konfiguration der IT zu vermeiden, sollten alle Mitarbeitende entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.
11	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden. Primäres	Es wird dringend empfohlen eine Hardware-Firewall einzusetzen und diese nach den eigenen Anforderungen zu

			Ziel ist es, keine unerlaubten Verbindungen von außen in das geschützte Netz zuzulassen. Zusätzlich sollten nur erlaubte Verbindungen aus dem geschützten Netz nach außen aufgebaut werden können.	konfigurieren und zu warten. Mindestens sollte dabei Folgendes eingestellt werden: - Nur erlaubte Kommunikationsziele (IP-Adressen und Ports) zulassen (eingehend/ausgehend). - Nur erlaubte Kommunikationsprotokolle zulassen.
12	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	Die Dokumentation sollte die logische Struktur des Netzes enthalten, insbesondere die Subnetze und wie das Netz zoniert und segmentiert wird. Änderungen im Netzwerk sollten ebenfalls dokumentiert werden. → Vorlage unter Musterdokumente erhältlich
13	Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden. Alle Default-Passwörter müssen auf den Netzkomponenten geändert werden. Die neuen Passwörter müssen ausreichend stark sein. Es sollten mind. 3 verschiedene Zeichenarten verwendet werden (z. B. Buchstaben, Zahlen und Sonderzeichen). Die Länge eines Passworts sollte mind. 12 Zeichen betragen.
14	Patch- und Änderungs-management	Installation von Updates	Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.	Viele Produkte verfügen über automatische Update-Mechanismen (Autoupdate). Es sollte festgelegt werden, wie die Update-Funktionen konkret in den verschiedenen Produkten konfiguriert werden.
15	Patch- und Änderungs-management	Verantwortlichkeit für Updates	Es muss festgelegt werden, wer die Updates installiert. Das ausgewählte Personal muss geschult und entsprechend berechtigt werden.	Kein Mitarbeiter sollte Änderungen auf eigene Faust durchführen. Die Verantwortlichkeiten für das Patch- und Änderungsmanagement sollten festgelegt werden. Die Verantwortlichen müssen das notwendige Wissen und die entsprechenden Berechtigungen besitzen.
16	Patch- und Änderungs-management	Identifizierung ausbleibender Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.	Falls Hardware- oder Software-Produkte eingesetzt werden sollen, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, muss geprüft werden, ob diese dennoch sicher betrieben werden müssen bzw. können.

				Häufig kündigen die Hersteller an, ab wann sie ein Produkt nicht mehr unterstützen, bzw. stellen die Information bereit, dass sie ein Produkt nicht mehr unterstützen.
17	Patch- und Änderungs-management	Ausmusterung oder Separierung bei ausbleibenden Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert oder separiert in einem eigenen Netzwerksegment betrieben werden.	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert oder separiert in einem eigenen Netzwerksegment betrieben werden.
18	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.	Bei der Anschaffung neuer Geräte sollte darauf geachtet werden, dass die Kamera abgedeckt und das Mikrofon ausgeschaltet werden kann. Eine Diode weist meist auf die aktive Benutzung der Geräte hin, und bietet einen Indikator für missbräuchliche Nutzung.
19	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.	- Windows-Rechner: Windows-Taste + L - Linux-Rechner: Logout - Mobile Geräte: Sperrtaste
20	Endgeräte	Einsatz von Viren-Schutzprogrammen	Aktuelle Virenschutzprogramme sind einzusetzen.	Verwenden Sie "Windows Defender" oder ein kommerzielles Virenschutzprogramm. Konfigurieren Sie, welche Daten wann gescannt werden sollen (z. B. alle Dateien vor dem Schreiben, eingehende E-Mail, etc.).
21	Endgeräte	Regelmäßige Datensicherung	Sämtliche relevante Daten sind regelmäßig zu sichern.	Es ist festzulegen in welchen Intervallen die Datensicherung erfolgen soll.
22	Endgeräte	Schutz der Datensicherung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.	Der Schutz der Datensicherung kann entweder physisch erfolgen, indem die Medien der Datensicherung weggeschlossen werden, oder die Datensicherung kann kryptographisch verschlüsselt werden.
23	Endgeräte	Art der Datensicherung	Es muss festgelegt werden, wie die Daten gesichert werden.	Die Festlegung kann die einzusetzende Software, die Sicherungsmedien und die Art der Datensicherung umfassen. Eine Datensicherung kann vollständig sein oder inkrementell, d.h. nur Änderungen ab einem bestimmten Zeitpunkt werden erfasst, oder eine Kombination davon. Ein Beispiel ist die 3-2-1-Regel (3 Kopien auf 2 unterschiedlichen Medien, davon 1 außer Haus).
24	Endgeräte	Verantwortliche der Datensicherung	Es muss festgelegt werden, wer für die Datensicherung zuständig ist.	Damit die Datensicherung auch durchgeführt wird, muss festgelegt werden, wer für die Datensicherung zuständig ist.

25	Endgeräte	Test der Datensicherung	Es sollte getestet werden, ob gesicherte Daten funktionsfähig und vollständig vorhanden sind.	Damit im Ernstfall auf die Datensicherung zurückgegriffen werden kann, sollte vorher getestet werden, ob die relevanten Daten mit der Sicherung erfasst werden, und ob diese zurückgespielt werden können.
26	Endgeräte	Der Zugriff auf Geräte und Software muss abgesichert werden.	Es sollten Benutzer und Rollen in der Praxissoftware zum Steuern der Zugriffe auf Patientendaten oder zur Nutzung von Sicherheitskarten wie z.B. den eHBA für den Inhaber der Karte eingerichtet werden.	Im Gegensatz zum (physischen) Zutritt, wird der Zugriff durch ein Berechtigungskonzept mit unterschiedlichen Rechten für unterschiedliche Benutzer und Rollen realisiert.
27	Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisations-mechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.	Deinstallieren Sie „OneDrive“. Dazu klicken Sie auf den Windows-Button, dann auf Einstellungen. Klicken Sie in dem geöffneten Fenster auf "Apps", in der angezeigten App-Liste auf "OneDrive" und deinstallieren Sie die App über den Button "deinstallieren".
28	Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Berechtigungen und Zugriffe sind pro Personengruppe und pro Person zu regeln.	Regeln Sie die Berechtigungen nach dem Need-to-know-Prinzip. D. h. Jede Person sollte nur so viele Berechtigungen auf Programm-, Datei und Verzeichnisebene erhalten, wie zur Bewältigung der Aufgaben nötig sind. Mittels Gruppen und Rollen lassen sich Berechtigungen für mehrere Personen für Netzfreigaben einrichten.
29	Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	So wenige personenbezogene Daten wie möglich sind zu verwenden.	Jede Verwendung von personenbezogenen Daten muss begründet (Zweckbindung) und in einem "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Dies schließt auch die einzuhaltenden Löschfristen mit ein. Ein Beispiel für solch ein Verzeichnis und eine Ausfüllhilfe dazu gibt es auf den Seiten der KBV unter https://www.kbv.de/html/datensicherheit.php.
30	Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten sind durch eine PIN zu schützen. Super-PIN/PUK sind nur durch Verantwortliche anzuwenden.	Die Nutzung der SIM-Karte der Institution sollte durch eine PIN geschützt werden. Die Super-PIN/PUK sollte nur im Rahmen der definierten Prozesse von den Verantwortlichen benutzt werden.
31	Smartphone und Tablet	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräten das erforderliche Schutzniveau	Alle mobilen Endgeräte müssen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen

			für die verarbeiteten Daten sichergestellt werden muss.	zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden. Die Freischaltung von Kommunikationsschnittstellen muss geregelt und auf das dienstlich notwendige Maß reduziert werden. Nicht benutzte Schnittstellen sollten deaktiviert werden. Überprüfen Sie regelhaft die Datenschutzeinstellungen der Anwendungen (Apps). Wenn Sie sich unsicher sind, verweigern Sie sämtliche Zugriffe.
32	Smartphone und Tablet	Verwendung eines Zugriffschutzes	Geräte sind mit einem komplexen Gerätesperrcode zu schützen.	Smartphones und Tablets müssen mit einem angemessen komplexen Gerätesperrcode geschützt werden. Die Nutzung der Bildschirmsperre muss vorgeschrieben werden. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm muss deaktiviert sein. Alle mobilen Geräte müssen nach einer angemessen kurzen Zeitspanne selbsttätig die Bildschirmsperre aktivieren. Nach mehreren fehlgeschlagenen Versuchen, den Bildschirm zu entsperren, sollte sich das mobile Gerät in den Werkszustand zurücksetzen. Es sollten dabei die Daten oder die Verschlüsselungsschlüssel sicher vernichtet werden.
33	Smartphone und Tablet	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen der Endgeräte sollte in den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen muss angemessen eingeschränkt werden. Die Datenschutzeinstellungen müssen so restriktiv wie möglich konfiguriert werden. Insbesondere der Zugriff auf Kamera, Mikrofon sowie Ortungs- und Gesundheitsdaten muss auf Konformität mit den organisationsinternen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. deaktiviert werden.
34	Mobiltelefon	Sperrmaßnahmen bei Verlust eines Mobiltelefons	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Die dafür notwendigen Mobilfunkanbieter-Informationen sind zu hinterlegen, um bei Bedarf darauf zugreifen zu können.	Der Mobilfunkanbieter stellt die dafür notwendigen Informationen zur Verfügung.

35	Mobiltelefon	Nutzung der Sicherheits-mechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.	Die verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen konfiguriert und genutzt werden. Die SIM-Karte sollte durch eine sichere PIN geschützt werden. Das Mobiltelefon sollte durch einen Geräte-Code geschützt werden. Falls möglich, sollte das Gerät an die SIM-Karte gebunden werden (SIM-Lock). Die Benutzer sollten über diese Sicherheitsmechanismen informiert werden.
36	Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.	Mittels Antiviren- bzw. Anti-Malware-Programmen lassen sich Wechseldatenträger vor der Verwendung auf Schadsoftware prüfen.
37	Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Beim Versand von Datenträgern sollte der Absender diese für den Empfänger eindeutig kennzeichnen. Dabei sollte die Kennzeichnung möglichst keine Rückschlüsse auf den Inhalt für andere ermöglichen.	Entweder sollte der Sender eine Liste führen, die eine Kennzeichnung eines Datenträgers eindeutig zuordenbar macht, oder Sender und Empfänger einigen sich auf eine Systematik, die die Kennzeichnung der Datenträger für beide zuordenbar macht, aber keine Rückschlüsse für andere ermöglicht. Z.B. Datenträger: "dd2bbeab-d901-4043-b543-0ce74ce57aae" statt "onkologischer Befund Patient XY".
38	Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Zum Versand von Datenträgern sollten Versandanbieter mit sicherem Nachweis-System und eine möglichst manipulationssichere Versandart und Verpackung gewählt werden.	Über die Angebote der sicheren Nachweissysteme wie Einschreiben und Wertsendungen informiert Sie Ihr Postunternehmen.
39	Wechseldatenträger / Speichermedien	Sicheres Löschen der Datenträger vor und nach der Verwendung	Alle Datenträger müssen nach ihrer Verwendung durch den jeweiligen Mitarbeiter /Mitarbeiterin sicher und vollständig gelöscht werden.	Bevor wieder beschreibbare Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, sollten sie in geeigneter Weise gelöscht (mit spezieller Software mehrmals mit Zufallswerten überschrieben) werden. Diese Funktionalität bieten verschiedene kommerzielle Anti-Viren- und spezielle Open Source Programme an.
40	E-Mail-Client und -Server	Sichere Konfiguration der E-Mail-Clients	Bei der Konfiguration der E-Mail-Clients muss mindestens folgendes berücksichtigt werden:	Angriffe erfolgen oft initial über E-Mails. Daher ist eine sichere Konfiguration der E-Mail-Clients unerlässlich.

			- Dateianhänge von E-Mails sollten vor dem Öffnen auf Schadsoftware geprüft werden, - die automatische Interpretation von HTML-Code und anderen aktiven Inhalten in E-Mails sollte deaktiviert werden, - zur Kommunikation mit E-Mail-Servern über nicht vertrauenswürdige Netze sollte eine sichere Transportverschlüsselung eingesetzt werden.	
41	E-Mail-Client und -Server	Umgang mit Spam durch Benutzende	Grundsätzlich sollten die Benutzenden alle Spam-E-Mails ignorieren und löschen. Die Benutzenden sollten auf unerwünschte E-Mails nicht antworten. Sie sollten Links in diesen E-Mails nicht folgen.	Als Spam werden unerwünschte, massenhafte E-Mails bezeichnet, die dem Empfänger unverlangt zugestellt werden.
42	Mobile Anwendungen (Apps)	Sichere Apps nutzen	Apps sollten nur aus den offiziellen Stores geladen werden. Sofern Apps nicht mehr benötigt werden, ist der Benutzeraccount in der App / das Benutzerkonto zu löschen und danach die App auf dem Gerät zu deinstallieren.	Für IOS: "App Store" Für Android: "Google Play" verwenden und in den Sicherheitseinstellungen keine Apps aus externen Quellen zulassen.
43	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Es sollten nur Apps genutzt werden, die Dokumente verschlüsselt und lokal abspeichern.	Verschlüsselung von Android (PIN oder Passwort einrichten) / IOS ("Code-Sperre") aktivieren.
44	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.	Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden, muss der Datenversand entsprechend eingeschränkt werden. Vor der App-Benutzung sollte überprüft werden, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten.
45	Internet-Anwendungen - Anbieter	Authentisierung bei Webanwendungen	Sollten Sie als Praxis einen Webdienst anbieten: Der IT-Betrieb muss Webanwendungen und Webservices so konfigurieren, dass	Es sollte eine 2 Faktor Authentisierung angeboten werden, oder hinreichend komplexe Passwörter eingefordert werden.

			sich Clients gegenüber der Webanwendung oder dem Webservice authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür muss eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess sollte dokumentiert werden. Der IT-Betrieb muss geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.	Die Webanwendung sollte verschlüsselte Verbindungen bereitstellen.
46	Internet-Anwendungen - Anbieter	Schutz vertraulicher Daten	Sollten Sie als Praxis einen Webdienst anbieten: Der IT-Betrieb muss sicherstellen, dass Zugangsdaten zur Webanwendung oder zum Webservice serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden. Dazu müssen Salted Hash-Verfahren verwendet werden. Die Dateien mit den Quelltexten der Webanwendung oder des Webservices müssen vor unerlaubten Abrufen geschützt werden.	Falls Benutzernamen und Passwörter als Authentisierungsmethode angeboten werden, so dürfen die Passwörter nicht im Klartext, sondern mittels dem Salted Hash-Verfahren gespeichert werden.
47	Internet-Anwendungen - Anbieter	Einsatz von Web Application Firewalls	Sollten Sie als Praxis einen Webdienst anbieten: Institutionen sollten eine Web Application Firewall (WAF) einsetzen. Die Konfiguration der eingesetzten WAF sollte auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices sollte die Konfiguration der WAF geprüft werden.	Eine WAF ist eine Spezialform einer Application Firewall für das HTTP-Protokoll, um die damit verbundenen Angriffe zu minimieren. Bei der Bereitstellung einer Webanwendung sollten Sie entweder eine Open Source Lösung (wie ModSecurity, Waf2Py oder OctopusWAF) oder eine spezielle kommerzielle Appliance verwenden. Zu dem Einsatz einer WAF gehört auch die richtige Konfiguration der Firewall, ggf. die Härtung der zugrunde liegenden Hardware und des Betriebssystems und regelmäßige Wartung und Updates.
48	Internet-Anwendungen - Anbieter	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Sollten Sie als Praxis einen Webdienst anbieten: Der IT-Betrieb muss sicherstellen, dass Webanwendungen und Webservices vor	Mittels des sogenannten "Captcha-Mechanismus" lassen sich automatisierte Zugriffe begrenzen.

			unberechtigter automatisierter Nutzung geschützt werden. Dabei muss jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, muss dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.	Durch zeitlich verzögerte Anmeldeversuche bei Falscheingaben lassen sich missbräuchliche Anmeldeversuche erschweren.
49	Internet-Anwendungen - Anbieter	Kryptografische Sicherung vertraulicher Daten	Bei der Nutzung von Webanwendungen ist darauf zu achten, dass eine verschlüsselte Kommunikation zum Einsatz kommt (z.B. https statt http).	Auf http**s** achten, ggf. die Einstellungen des Browsers auf "HTTPS-only" ändern. Beispielsweise statt http://www.kbv.de besser https://www.kbv.de verwenden. Dies wird durch ein "Schloss" als Icon im Webbrowser visualisiert. Durch Anklicken des Schlosses lassen sich die Informationen zu dem Zertifikat und dem Herausgeber des Zertifikats einsehen.
50	Cloud-Anwendungen - Anbieter	Sicherheit von Cloud-Dienstleistern	Soweit Sozial- oder Gesundheitsdaten im Wege des Cloud-Computing verarbeitet werden sollen, muss der Anbieter der eingesetzten Cloud-Anwendung über ein aktuelles C5-Testat entsprechend § 393 SGB V in Verbindung mit § 384 SGB V verfügen.	Fragen Sie den Anbieter nach dem Testat der Cloud-Anwendung. Beachten Sie die in dem Testat aufgeführten "korrespondierende Kriterien für Kunden". Beachten Sie die Anforderungen aus § 393 Abs. 3 Satz 1 Nr. 1 SGB V über die notwendigen "angemessenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Informationssicherheit". In der vertragsärztlichen und vertragszahnärztlichen Versorgung können dies die Anforderungen nach § 390 SGB V sein.

Anlage 2: Zusätzliche Anforderungen für <u>mittlere Praxen</u>

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Netzwerksicherheit	Alarmierung und Logging	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.	Es sollten mindestens folgende Komponenten und Ereignisse auf einem zentralen Protokoll-Server protokolliert werden: - Active Directory: unautorisierte Zugriffe bzw. Zugriffsversuche - Firewall: Ereignisse wie erlaubte und unterbundene Zugriffe - Virenscanner: Start, Stop, Fehler bei Scannen; erkannte Malware - PVS: Anmeldungen, Verfügbarkeit, etc. Wenn der Durchsatz und die Erreichbarkeit der Netzwerkkomponenten und Dienste überwacht werden sollen, kann dies mit Open Source Tools wie Icinga erfolgen.
2	Endgeräte	Nutzung von verschlüsselten Kommunikations-verbindungen	Benutzer sollten darauf achten, dass zur Verschlüsselung von Kommunikationsverbindungen kryptografische Algorithmen nach dem Stand der Technik wie z.B. TLS verwendet werden.	Vgl. Anlage 1 - Anforderung Nr. 49. Auf http**s** achten.
3	Endgeräte	Restriktive Rechtevergabe	Rechte sollten so restriktiv wie möglich nach dem Need-to-know Prinzip vergeben werden.	Der verfügbare Funktionsumfang des IT-Systems sollte für einzelne Benutzer oder Benutzergruppen so eingeschränkt werden, dass sie nur genau die Rechte besitzen und nur auf die Funktionen zugreifen können, die sie für ihre Aufgabenwahrnehmung benötigen („Need-to-know-Prinzip“). Zugriffsberechtigungen sollten hierfür möglichst restriktiv vergeben werden. Es sollte regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf Systemdateien sollten möglichst nur die Systemadministratoren zugreifen können. Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden. Auch System-Verzeichnisse sollten nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

4	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.	In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie sollte die Verwendung älterer Protokolle verhindern. Der Schutz des Local Credential Store (LSA) sollte aktiviert werden (PPL, Protected Mode Light). Die Speicherung der LAN-Manager-Hashwerte bei Kennwortänderungen sollte per Gruppenrichtlinie deaktiviert werden. Die Überwachungseinstellungen sollten gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt werden. Es sollte eine Protokollierung auf Clientseite sichergestellt werden.
5	Smartphone und Tablet	Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten erstellt werden.	Es sollte eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente*. Diese sollte festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Darin sollten die Themen Aufbewahrung und Verlustmeldung behandelt werden. Außerdem sollte verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.
6	Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind. Andernfalls sollten sie deaktiviert werden. Generell sollte ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.
7	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente.*

				Jedem Benutzer eines Mobiltelefons muss ein Exemplar der Sicherheitsrichtlinie ausgehändigt werden. Es muss regelmäßig überprüft werden, ob die Sicherheitsrichtlinie eingehalten wird. Die Sicherheitsleitlinie zur dienstlichen Nutzung von Mobiltelefonen sollte Bestandteil der Schulung zu Sicherheitsmaßnahmen sein.
8	Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln. Die zur Übertragung erlaubten Schnittstellen sollten festgelegt werden. Außerdem sollte beschlossen werden, wie die Daten bei Bedarf zu verschlüsseln sind.
9	Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldaten-trägern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. Darin sollte festgelegt sein, welche Datenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei zu beachten sind. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente*.
10	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken bzw. zu vergeben.	Bevor eine App in einer Institution eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen müssen hinterfragt und gegebenenfalls unterbunden werden. Sicherheitsrelevante Berechtigungseinstellungen müssen so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können. Wo dies technisch nicht möglich ist, müssen die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

Anlage 3: Zusätzliche Anforderungen für <u>Großpraxen</u>

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Personal	Messung und Auswertung des Lernerfolgs	Die Lernerfolge im Bereich Informationssicherheit sollten zielgruppenbezogen gemessen und ausgewertet werden. Die Ergebnisse sollten bei der Verbesserung des Sensibilisierungs- und Schulungsangebots zur Informationssicherheit in geeigneter Weise einfließen.	Eine Methode, den Lernerfolg zu messen, sind Tests am Ende der Schulungen.
2	Netzwerksicherheit	Planung des internen Netzwerkes	Bei der Planung des internen Netzwerkes soll eine Netzwerksegmentierung erfolgen, die berücksichtigt, welche Daten in dem jeweiligen Segment verarbeitet und kommuniziert werden. Hierbei soll eine Trennung zwischen Gesundheitsdaten und weniger kritischen Daten erfolgen.	Durch Netzwerksegmentierung werden die einzelnen Segmente oder Bereiche zusätzlich geschützt. Wenn die Gesundheitsdaten in einem anderen Netzwerksegment verarbeitet werden als die E-Mails, dann kann Schadsoftware, die z.B. durch einen E-Mailanhang eingedrungen ist, nicht sofort auf die Gesundheitsdaten zugreifen, und es wird die Wahrscheinlichkeit erhöht, dass die Schadsoftware "rechtzeitig" erkannt wird und Gegenmaßnahmen ergriffen werden können bevor die Gesundheitsdaten kompromittiert werden. Netzwerksegmentierung kann durch Firewalls, Virtual Local Area Networks (VLANs) oder auch Software Defined Networking (SDN) durchgeführt werden.
3	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.	Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, muss nach Stand der Technik angemessen verschlüsselt und authentisiert werden.
4	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	Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der

			und Kontrolle der Geräte festgelegt werden.	Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente.* Hierbei muss unter anderem festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.
5	Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten vor einer gewünschten Installation durch die Verantwortlichen geprüft und freigegeben werden.	Apps aus öffentlichen App-Stores sollten vor einer gewünschten Installation durch die Verantwortlichen geprüft und freigegeben werden. Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden.
6	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.	Die Institution sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen. Grundlage für die Regelung sollte einerseits die Klassifikation der Institutionsdaten sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden. Die Benutzer der mobilen Endgeräte sollten nur freigegebene und geprüfte Apps aus als sicher klassifizierten Quellen installieren dürfen.
7	Mobile Device Management (MDM)	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM und das interne Netz der Institution muss angemessen abgesichert werden.	Die Verbindung der mobilen Endgeräte zum MDM und das interne Netz der Institution muss angemessen abgesichert werden. Dies bieten kommerzielle MDM-Lösungen in der Regel out-of-the-box an. Wenn Daten zwischen den mobilen Endgeräten und dem IT-Netz der Institution übertragen werden, sollte durch geeignete Maßnahmen (z. B. VPN) verhindert werden, dass Unbefugte sie verändern oder einsehen können.
8	Mobile Device Management (MDM)	Berechtigungs-management im MDM	Für das MDM muss ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.	Für das MDM muss ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden. Den Benutzergruppen und Administratoren sollte das MDM nur so viele Berechtigungen einräumen wie für die Aufgabenerfüllung notwendig sind (Minimalprinzip). Es sollte regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind und den Aufgaben entsprechen.
9	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.	Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.

				Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch den Benutzer sollte durch das MDM verhindert werden. Das MDM sollte Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen.
10	Mobile Device Management (MDM)	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM muss sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.	Das MDM muss sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können (Remote Wipe bei bestehender Datenverbindung). Werden in dem mobilen Endgerät externe Speicher genutzt, sollte geprüft werden, ob diese bei einem Remote Wipe ebenfalls gelöscht werden können. Diese Funktion sollte vom MDM unterstützt werden. Der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) sollte sicherstellen, dass keine schutzbedürftigen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies sollte insbesondere dann gelten, wenn das Unenrollment aus der Ferne ausgeführt wird.
11	Mobile Device Management (MDM)	Auswahl und Freigabe von Apps	Nur durch die Verantwortlichen geprüfte und freigegebene Apps dürfen über das MDM zur Installation angeboten werden.	Apps aus öffentlichen App-Stores müssen durch die Verantwortlichen geprüft und freigegeben werden. Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden und dort für die Benutzer verfügbar sein. Apps sollten gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden. Das MDM sollte die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht.
12	Mobile Device Management (MDM)	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis muss festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.	Die Institution muss festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen. Grundlage für die Regelung sollten einerseits die Klassifikation bzw. der Schutzbedarf der Informationen sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden, etwa in abgeschotteten Containern. Die Verantwortlichen müssen das MDM auf Basis dieser Regeln konfigurieren, sodass es diese auf allen mobilen Endgeräten durchsetzen kann.

				Den Benutzern müssen die Regeln in geeigneter Weise bekannt gegeben werden.
13	Wechseldatenträger / Speichermedien	Datenträger-verschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.	Es sollten sichere und nicht veraltete Verschlüsselungsverfahren eingesetzt werden. Empfehlungen zu geeigneten Algorithmen und Schlüssellängen bieten die Technischen Richtlinien des BSI „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1). Mittels Open-Source Lösungen wie VeraCrypt können entsprechende verschlüsselte Container angelegt werden.
14	Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.	Um beim Datenaustausch mittels mobiler Datenträger die Integrität von vertraulichen Informationen sicherzustellen, sollte ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden. Die Verfahren zum Schutz vor Veränderungen sollten dem aktuellen Stand der Technik entsprechen.
15	E-Mail-Client und -Server	Sicherer Betrieb von E-Mail-Servern	Bei dem Betrieb von E-Mail-Servern muss mindestens folgendes berücksichtigt werden: - es muss eine sichere Transportverschlüsselung für das Senden und Empfangen von E-Mails ermöglicht werden - es sollten Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergriffen werden - E-Mail-Server müssen so konfiguriert werden, dass sie nicht als Spam-Relay missbraucht werden können.	Der Empfang von E-Mails über unverschlüsselte Verbindungen sollte deaktiviert werden. Der E-Mail-Server sollte so konfiguriert werden, dass E-Mail-Clients nur über eine sichere Transportverschlüsselung auf Postfächer zugreifen können, wenn dies über nicht vertrauenswürdige Netze passiert.
16	E-Mail-Client und -Server	Datensicherung und Archivierung von E-Mails	Die Daten der E-Mail-Server und -Clients sind regelmäßig und verschlüsselt zu sichern.	Es sollte beachtet werden, dass E-Mails möglicherweise nur lokal auf Clients gespeichert sind.
17	E-Mail-Client und -Server	Spam- und Virenschutz auf dem E-Mail-Server	Eingehende und ausgehende E-Mails und deren Anhänge sind auf Spam-Merkmale und schädliche Inhalte zu überprüfen.	Es muss festlegt werden, wie mit verschlüsselten E-Mails zu verfahren ist, wenn diese nicht durch das Virenschutzprogramm entschlüsselt werden können.

Anlage 4: Zusätzliche Anforderungen für <u>medizinische Großgeräte</u>

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
1	Medizinische Großgeräte	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnitt-stellen	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.	Um unsichere Systemkonfigurationen zu vermeiden, sollte die Konfigurations- und Wartungsschnittstellen auf einen festgelegten Personenkreis eingeschränkt werden.
2	Medizinische Großgeräte	Nutzung sicherer Protokolle für die Konfiguration und Wartung	Für die Konfiguration und Wartung von medizinischen Großgeräten müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.	Nutzen Sie für die Konfiguration und Wartung der medizinischen Großgeräte verschlüsselte und authentisierte Protokolle wie HTTPS. Dies gilt insbesondere, falls externe Dienstleister die Konfiguration und Wartung durchführen.
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.	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. Bewahren Sie die Protokolldaten nicht zu lange, aber auch nicht zu kurz auf, z.B. für ein halbes Jahr. Die Vorgaben der DSGVO sind dabei einzuhalten. Bestimmen Sie, wer Zugriff auf die Protokolldaten erhält, z.B. die Administratoren.
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.	Verifizieren Sie, dass auf die medizinischen Großgeräte nicht von außerhalb Ihrer Praxis zugegriffen werden kann. Deaktivieren Sie ggf. ungewollte Dienste der vernetzten Medizintechnik oder passen Sie Ihre Firewall-Konfiguration an.

5	Medizinische Großgeräte	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.	Nicht genutzte Benutzerkonten der medizinischen Großgeräte müssen deaktiviert werden. Benutzerkonten zur Fernwartung sollten außerhalb der Wartungszeiten deaktiviert werden.
6	Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden.	Um die medizinischen Großgeräte - z.B. bei ausbleibenden Sicherheitsupdates der Hersteller - zu schützen, sollten diese von der weiteren IT durch Netzwerksegmente oder -Zonen getrennt und die erlaubten Kommunikationsverbindungen auf das notwendige Maß beschränkt werden.

Anlage 5: Anforderungen für dezentrale Komponenten der Telematikinfrastruktur

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
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.	Lassen Sie sich das Installationsprotokoll und die vom Dienstleister erstellten Dokumentationen aushändigen und bewahren Sie diese sicher auf.
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.	Informationen erhalten Sie auf der Webseite der gematik und von den Herstellern der TI-Komponenten.
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.	Informationen erhalten Sie auf der Webseite der gematik und von den Herstellern der TI-Komponenten.
4	Dezentrale Komponenten der TI	Internet-Verbindung parallel zur TI-Anbindung	Existiert zusätzlich zur TI-Anbindung eine Internet-Verbindung, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.	Überprüfen Sie bei einer parallelen Installation des Konnektors, ob Ihr Netz durch eine Firewall (vergleich Anlage 1, Nummer 11) ausreichend geschützt ist.
5	Gehosteter Konnektor	Verbindung absichern	Um die Verbindung zu einem gehosteten Konnektor vor unberechtigten Zugriff zu schützen, muss ein VPN-Tunnel zwischen Praxis und Konnektor eingerichtet und aufgebaut werden.	Informationen erhalten Sie auf der Webseite der gematik und von den Herstellern der TI-Komponenten.
6	TI-Gateway	Beachtung der Vorgaben des TI-Gateway-Anbieters	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch des TI-Gateway-Anbieters konfiguriert und betrieben werden.	Informationen erhalten Sie auf der Webseite der gematik und von den Herstellern der TI-Komponenten.
7	Primärsysteme	Geschützte Kommunikation mit dem Konnektor/TI-Gateway	Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.	Aktivieren Sie die TLS-Verbindung vom PVS zum Konnektor, und die Authentisierungsmöglichkeit am Konnektor. Für die Authentisierung mittels X.509 Client-Authentisierung, muss ein Zertifikat im Konnektor generiert und das PVS inklusive PIN und Zugriff auf den

				privaten Schlüssel konfiguriert, oder ein Konnektor-fremdes X.509 Zertifikat im PVS inklusive PIN und Zugriff auf den privaten Schlüssel und im Konnektor konfiguriert werden.
8	Dezentrale Komponenten der TI	Zeitnahes Installieren verfügbarer Aktualisierungen	Die TI-Komponenten 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.	Prüfen Sie, ob Updates Ihrer TI-Komponenten vorliegen und installieren Sie diese zeitnah.
9	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.	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 vertragliche, angemessen kurze Reaktionszeit und eine Herausgabe der Informationen am Ende des Vertrages. Eine weitere Möglichkeit ist es, die Administrationsdaten in einem versiegelten Umschlag zu erhalten, um im Notfall auf die TI-Komponenten zugreifen zu können. Wenn der Umschlag geöffnet wurde, ist dies dem Dienstleister anzuzeigen.