KBV

KASSENÄRZTLICHE
BUNDESVEREINIGUNG

IT-SICHERHEIT

HINWEISE ZUR RICHTLINIE, TIPPS ZUR UMSETZUNG, BEISPIELE FÜR DIE PRAXIS

DIESES THEMENHEFT ERGÄNZT DIE ONLINE-PLATTFORM ZUR IT-SICHERHEITSRICHTLINIE:
https://hub.kbv.de/site/its

PraxisWissen

Liebe Kolleginnen, liebe Kollegen,

Ihre Praxis verwendet ein aktuelles Virenschutzprogramm, nutzt verschlüsselte Internetanwendungen und sendet keine vertraulichen Daten über Apps? Dann erfüllt sie einen wichtigen Teil der Anforderungen, die durch die IT-Sicherheitsrichtlinie gelten. Der Gesetzgeber hat die KBV und die Kassenzahnärztliche Bundesvereinigung beauftragt, eine IT-Sicherheitsrichtlinie für alle Praxen zu entwickeln (§ 75b SGB V). Diese Richtlinie beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die IT-Sicherheit zu gewährleisten. Sie „erfindet" dabei keine zusätzlichen Vorgaben, sondern konkretisiert bestehende Regelungen und macht diese praxistauglich – zum Beispiel Vorgaben aus der EU-Datenschutzgrundverordnung. Somit werden viele Anforderungen bereits von den Niedergelassenen umgesetzt. Die klaren Vorgaben sollen dabei helfen, IT-Systeme und sensible Daten in den Praxen noch besser zu schützen.

Dieses PraxisWissen gibt Ihnen einen Überblick und stellt wichtige Schritte, Fristen und Anforderungen vor. Außerdem bietet es eine Checkliste, Beispiele und Praxis-Tipps sowie weiterführende Informationen. Es ist ein Serviceangebot zur IT-Sicherheitsrichtlinie, das Sie nutzen können und das Sie unterstützen soll. Die IT-Sicherheitsrichtlinie und alle zu erfüllenden Anforderungen sind auf einer Online-Plattform abrufbar, dem sogenannten Hub. Näheres lesen Sie auf den folgenden Seiten.

Wir wünschen Ihnen eine angenehme Lektüre.

Ihre Kassenärztliche Bundesvereinigung

INHALT

RECHTLICHER HINWEIS: Unabhängig von der IT-Sicherheitsrichtlinie sind die rechtlichen Vorgaben beispielsweise zur ärztlichen Schweigepflicht zu beachten. Mit der IT-Sicherheitsrichtlinie wurden keine neuen Sanktionsformen eingeführt. Grundlage für Sanktionen sind wie bisher unter anderem die EU-Datenschutzgrundverordnung (z. B. bei Verstößen gegen den Datenschutz), das deutsche Strafgesetzbuch (z. B. § 203 StGB bei Verletzung von Privatgeheimnissen) und das Berufsrecht (§ 9 Abs. 1 MBO-Ärzte bei Verstößen gegen die ärztliche Schweigepflicht).

SCHUTZ DER PRAXIS-IT

Jeder Praxisinhaber möchte, dass die ihm anvertrauten Daten sicher verwahrt sind. Allerdings fehlte bislang ein verlässlicher Rahmen, der nun mit der IT-Sicherheitsrichtlinie geschaffen wurde. Dabei geht es um Punkte wie Sicherheitsmanagement, IT-Systeme, Rechnerprogramme, mobile Apps und Internetanwendungen oder das Aufspüren von Sicherheitsvorfällen.

HINTERGRUND: DIGITALE-VERSORGUNG-GESETZ

Der Gesetzgeber hat mit dem Digitale-Versorgung-Gesetz die Kassenärztliche Bundesvereinigung und die Kassenzahnärztliche Bundesvereinigung beauftragt, eine IT-Sicherheitsrichtlinie für alle Praxen zu entwickeln. Darin sollen die Anforderungen zur Gewährleistung der IT-Sicherheit verbindlich festgelegt sein. Die Richtlinie wurde unter anderem im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik erstellt und wird jährlich aktualisiert.

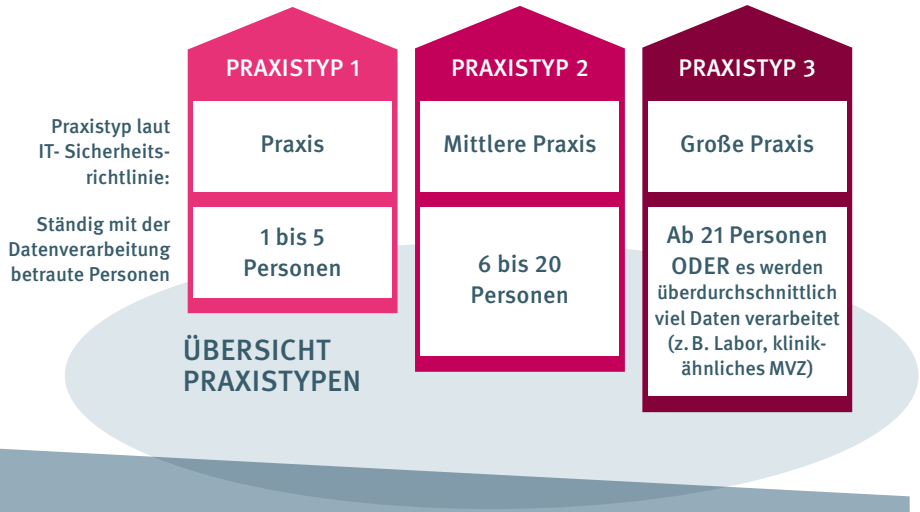
SICHERHEIT FÜR PRAXISINHABER

Die Richtlinie soll Praxisinhaberinnen und Praxisinhaber dabei unterstützen, alle nötigen Sicherheitsvorkehrungen zu treffen, um einen Datenmissbrauch zu verhindern. Sie bietet ihnen damit auch ein Stück Sicherheit. Denn die Richtlinie legt Sicherheitsanforderungen an Arzt- und Psychotherapeutenpraxen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen. Vieles davon wird im Praxisalltag bereits angewendet, da es durch die europäische Datenschutzgrundverordnung vorgegeben ist. Zudem erfolgt die Einführung schrittweise.

ANFORDERUNGEN RICHTEN SICH NACH DER PRAXISGRÖSSE

Neben den unterschiedlichen Fristen, bis wann was umzusetzen ist, gibt es eine weitere Besonderheit: Die Vorgaben an die IT-Sicherheit richten sich nach der Größe der Praxis. Dabei finden sich in der Richtlinie Anforderungen, die von allen Praxen erfüllt werden müssen, um die Sicherheit der verwendeten Hard- und Software zu gewährleisten. Für Praxen, in denen mehr als fünf Personen ständig mit der Datenverarbeitung beschäftigt sind oder in denen überdurchschnittlich viele Daten verarbeitet werden (z. B. Labore), gibt es zusätzliche Anforderungen. Kommen medizinische Großgeräte zum Einsatz, zum Beispiel CT, MRT, PET, Linearbeschleuniger, sind weitere Sicherheitsvorkehrungen zu treffen. Ärztinnen, Ärzte, Psychotherapeutinnen und Psychotherapeuten sollten deshalb zunächst schauen, zu welchem „Praxistyp“ sie gehören.

Die Anforderungen sind in den fünf Anlagen zur Richtlinie aufgeführt. Mehr dazu auf Seite 4.



ÜBERSICHT PRAXISTYPEN

WAS BEDEUTET „STÄNDIG MIT DER DATENVERARBEITUNG BETRAUT“?
Unter dem Begriff „Datenverarbeitung“ werden Tätigkeiten zusammengefasst wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten. In den Praxen beginnt dieser Prozess quasi bei der Terminvereinbarung am Telefon oder dem Einlesen der elektronischen Gesundheitskarte.

ÜBERSICHT DER ANFORDERUNGEN UND TERMINE (AUSWAHL)

Virenschutz, Firewall, Sperrcodes: Welche Anforderungen bestehen nach der IT-Sicherheitsrichtlinie und ab wann muss meine Praxis sie erfüllen? Hier finden Sie eine Auswahl – sortiert nach der Praxisgröße.

Die jeweiligen Anforderungen müssen nur erfüllt werden, wenn die Praxis entsprechende IT-Komponenten verwendet.

ANLAGEN ZUR RICHTLINIE:

Die IT-Sicherheitsrichtlinie gibt den Rahmen vor. Entscheidend sind die Anlagen. Sie listen die Anforderungen an Hard- und Software auf, die die Praxen je nach Größe erfüllen müssen.

ANLAGE 1
Anforderungen, die alle Praxen erfüllen müssen.

ANLAGE 2
Anforderungen, die mittlere und große Praxen zusätzlich zu Anlage 1 erfüllen müssen.

ANLAGE 3
Anforderungen, die ausschließlich große Praxen zusätzlich zu Anlage 1 und Anlage 2 erfüllen müssen.

ANLAGE 4
Anforderungen, die alle Praxen zusätzlich zu Anlage 1, Anlage 2 und Anlage 3 erfüllen müssen, wenn sie medizinische Großgeräte wie CT oder MRT einsetzen.

ANLAGE 5
Anforderungen, die alle Praxen bezüglich der sogenannten dezentralen Komponenten der Telematikinfrastruktur (z. B. Konnektor, Kartenlesegerät, Praxisausweis) erfüllen müssen.

BASISANFORDERUNGEN FÜR ALLE PRAXEN SOWIE ERLÄUTERUNGEN

Anlagen 1 und 5

PRAXISTYP 1 | PRAXISTYP 2 | PRAXISTYP 3

AB 1. APRIL 2021

Anlage 1 Nummer 1 / Sichere Apps nutzen: Apps werden nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.

Anlage 1 Nummer 4 / Verhinderung von Datenabfluss: Es werden keine vertraulichen Daten über Apps versendet.

Anlage 1 Nummer 8 / Schutz vertraulicher Daten: Der Internet-Browser ist so eingestellt, dass in dem Browser keine vertraulichen Daten gespeichert werden.

Anlage 1 Nummer 10 / Kryptografische Sicherung vertraulicher Daten: Es werden NUR verschlüsselte Internet-Anwendungen genutzt.

Anlage 1 Nummer 13 / Abmelden oder Sperren: Nach der Nutzung eines Gerätes meldet sich die Person ab oder sperrt es.

Anlage 1 Nummer 15 / Einsatz von Virenschutzprogrammen: In der Praxis werden aktuelle Virenschutzprogramme eingesetzt.

Anlage 1 Nummer 22 / Zugriffsschutz verwenden: Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt.

Anlage 1 Nummer 33 / Dokumentation des Netzes: Das interne Netzwerk ist anhand eines Netzplanes dokumentiert. *Musterdokument online verfügbar*

Anlage 1 Nummer 12 / Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras: Kamera und Mikro sollten grundsätzlich deaktiviert sein und nur bei Bedarf aktiviert und danach wieder deaktiviert werden.

Anlage 1 Nummer 27 / Updates von Mobiltelefonen: Regelmäßig prüfen, ob es Updates gibt.

AB 1. JANUAR 2022

Anlage 1 Nummer 3 / Sichere Speicherung lokaler App-Daten: Es werden nur Apps genutzt, die Dokumente verschlüsselt und lokal abspeichern.

Anlage 1 Nummer 9 / Firewall benutzen: Bei der Bereitstellung und dem Betreiben von Internet-Anwendungen wie Praxis-Homepage oder Online-Kalender wird eine Web Application Firewall eingesetzt.

Anlage 1 Nummer 11 / Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen: Bei der Bereitstellung und dem Betreiben von Internet-Anwendungen werden keine automatisierten Zugriffe beziehungsweise Aufrufe auf Webanwendungen eingerichtet oder zugelassen.

Anlage 1 Nummer 14 / Regelmäßige Datensicherung: Auf Endgeräten, zum Beispiel einem Praxisrechner, erfolgt eine regelmäßige Datensicherung, wobei in einem Plan festgelegt ist, welche Daten wie oft gesichert werden sollen.

Anlage 1 Nummer 25 / Sperrmaßnahmen bei Verlust eines Mobiltelefons: Bei Verlust eines Mobiltelefons (Diensthandy) muss die darin verwendete SIM-Karte zeitnah gesperrt werden.

Anlage 1 Nummer 28 / Schutz vor Schadsoftware: Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.

Anlage 5 Nummer 6 / Zeitnahes Installieren verfügbarer Aktualisierungen: Für die dezentralen Komponenten der Telematikinfrastruktur werden Updates zeitnah installiert.

Anlage 5 Nummer 7 / Sicheres Aufbewahren von Administrationsdaten: Für die dezentralen Komponenten der Telematikinfrastruktur werden die Administrationsdaten sicher aufbewahrt.

ZUSÄTZLICHE ANFORDERUNGEN

FÜR MITTLERE UND GROSSE PRAXEN
2 3
Anlage 2

AB 1. APRIL 2021

Anlage 2 Nummer 1 / Minimierung und Kontrolle von App-Berechtigungen: Bevor eine App eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält; weitere müssen hinterfragt und gegebenenfalls unterbunden werden.

AB 1. JANUAR 2022

Anlage 2 Nummer 8 / Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung: Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.
Musterdokument online verfügbar

AB 1. JULI 2022

Anlage 2 Nummer 6 / Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten: Werden Smartphones und Tablets genutzt, muss es dazu eine verbindliche Richtlinie für Mitarbeiter geben.
Musterdokument online verfügbar

Anlage 2 Nummer 10 / Regelung zur Mitnahme von Wechseldatenträgern: Werden Wechseldatenträger eingesetzt, muss es eine Regelung zur Mitnahme geben.
Musterdokument online verfügbar

FÜR GROSSE PRAXEN
3
Anlage 3

AB 1. JANUAR 2022

Anlage 3 Nummer 1 / Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets: Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.
Musterdokument online verfügbar

AB 1. JULI 2022

Anlage 3 Nummer 2 / Auswahl und Freigabe von Apps: Bevor Apps genutzt werden, müssen sie geprüft und freigegeben werden.

FÜR ALLE PRAXEN MIT MEDIZINISCHEN GROSSGERÄTEN
1 2 3
Anlage 4

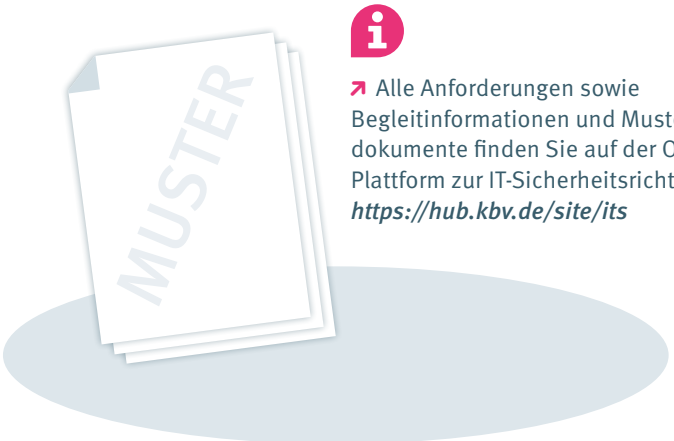
AB 1. JULI 2021

Anlage 4 Nummer 1 / Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen: Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können.

Anlage 4 Nummer 2 / Nutzung sicherer Protokolle für die Konfiguration und Wartung: Für die Konfiguration und Wartung von medizinischen Großgeräten müssen sichere Protokolle genutzt werden.

AB 1. JANUAR 2022

Anlage 4 Nummer 6 / Netzsegmentierung: Medizinische Großgeräte sind von der weiteren IT getrennt.



↗ Alle Anforderungen sowie Begleitinformationen und Musterdokumente finden Sie auf der Online-Plattform zur IT-Sicherheitsrichtlinie: ***https://hub.kbv.de/site/its***

CHECKLISTE
SO KÖNNEN SIE VORGEHEN

Sie wollen prüfen, ob Sie die Anforderungen der IT-Sicherheitsrichtlinie erfüllen oder welche Maßnahmen Sie zusätzlich ergreifen müssen, um vertrauliche Daten noch besser vor unberechtigten Zugriffen zu schützen? Doch womit fangen Sie am besten an? Die Checkliste soll Ihnen helfen, einen Einstieg zu finden.

1 PRAXISTYP FESTLEGEN

Welcher Praxistyp sind wir?
Je nach Praxistyp müssen die Anforderungen nach den entsprechenden Anlagen erfüllt werden:

Praxis mit 1 bis 5 Personen*
Anlage 1, 5 (und 4 bei medizinischen Großgeräten)

Mittlere Praxis mit 6 bis 20 Personen*
Anlage 1, 2, 5 (und 4 bei medizinischen Großgeräten)

Große Praxis mit mehr als 21 Personen* oder sehr vielen Daten
Anlage 1, 2, 3, 5 (und 4 bei medizinischen Großgeräten)

* ständig mit der Datenverarbeitung betraute Personen

2 IT-KOMPONENTEN FINDEN

Welche IT-Komponenten nutzen wir in unserer Praxis?
Erstellen Sie eine Liste der IT-Komponenten. Nur wenn eine IT-Komponente vorhanden ist, müssen Sie die Anforderungen erfüllen und Sicherungsmaßnahmen umsetzen.

Dezentrale Komponenten der TI, zum Beispiel Konnektor, Kartenlesegerät, Praxisausweis

Endgeräte, zum Beispiel Computer, Laptop, Notebook

Endgeräte mit Windows-Betriebssystem, zum Beispiel Computer, auf denen Windows läuft

Internet-Anwendungen, zum Beispiel praxisbetriebene Webpräsenz, selbst betriebene Onlineterminvergabe

Medizinische Großgeräte, zum Beispiel CT, MRT, PET

Mobile Anwendungen (Apps)

Mobile Device Management / MDM, zum Beispiel mobile Geräte wie Praxis-Laptops oder Praxis-Tablets werden zentralisiert überwacht/verwaltet

Mobiltelefone, die dienstlich genutzt werden

Netzwerksicherheit, zum Beispiel (W)LAN-Sicherheit

Office-Produkte, zum Beispiel Programme für Textverarbeitung, Tabellenkalkulation, Präsentationen

Smartphones und Tablets

Wechseldatenträger, Speichermedien, zum Beispiel USB-Sticks, Speicherkarten, externe Festplatten

↗ Die IT-Komponenten sind im Hub in den Anlagen unter „Zielobjekt“ aufgeführt: ***https://hub.kbv.de/display/itsrl***

3 SICHERUNGSMASSNAHMEN FESTLEGEN

Mit welchen Maßnahmen schützen wir die IT-Zielobjekte unserer Praxis?
Prüfen Sie, mit welchen Maßnahmen Sie Ihre IT-Komponenten bereits schützen und welche weiteren Maßnahmen Sie ergreifen können.

↗ Weiterführende Informationen dazu finden Sie auf den Seiten 8 bis 9 und ausführlich auf der Online-Plattform: ***https://hub.kbv.de/display/itsrl***

4 DIENSTLEISTER JA ODER NEIN?

Beauftragen wir einen IT-Dienstleister, der uns berät und unterstützt?
Die KBV veröffentlicht eine Liste der IT-Dienstleister, die speziell für die Umsetzung der Vorgaben aus der IT-Sicherheitsrichtlinie zertifiziert wurden. Dies ist ein optionales Angebot. Praxisinhaberinnen und -inhaber können sich auch für einen nicht zertifizierten Dienstleister entscheiden, wenn sie sich Hilfe holen möchten.

↗ Die Liste der IT-Dienstleister steht online zur Verfügung: ***www.kbv.de/media/sp/KBV_ISAP_Dienstleister_ZERT_P75b_SGBV.pdf***

5 UMSETZUNG STARTEN

Beginnen Sie mit der Umsetzung und tauschen Sie sich dazu gegebenenfalls mit Ihrem IT-Dienstleister aus.

PRAXIS-TIPPS

DER HUB ZUR IT-SICHERHEIT
EIN ONLINE-SERVICE DER KBV

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

Sie wollen sich detailliert zu den einzelnen Sicherheitsanforderungen informieren, suchen Musterdokumente oder wollen eine Frage stellen? Dann nutzen Sie den Hub der KBV.

Die Online-Plattform wurde speziell zur IT-Sicherheitsrichtlinie eingerichtet und bündelt alle Informationen. Dort finden Sie die Richtlinie mit ihren Anlagen. Jede Anlage ist als Tabelle aufgebaut und besteht aus diesen Spalten:

- Nummer der Anforderung
- Zielobjekt
- Anforderung
- Erläuterung
- Geltungsdatum

Eine weitere Spalte enthält Hinweise wie Sie, beziehungsweise der von Ihnen beauftragte IT-Dienstleister, die Anforderungen umsetzen kann.

Außerdem können Sie im Hub Musterdokumente für Ihre Praxis herunterladen, zum Beispiel einen Muster-Netzplan und eine Muster-Richtlinie für Mitarbeitende zur Nutzung von mobilen Geräten.

WEITERE SERVICEANGEBOTE

ONLINE-FORTBILDUNG

Die KBV bietet eine Online-Fortbildung für Ärzte und Psychotherapeuten zur IT-Sicherheitsrichtlinie an. Diese steht im Fortbildungsportal der KBV bereit, hier ist ein Login erforderlich.

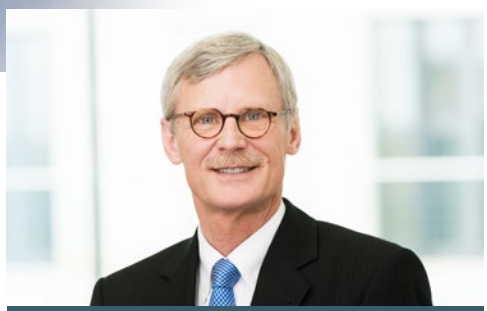
Die Fortbildung ist von der Ärztekammer Berlin anerkannt. Bei erfolgreicher Teilnahme können zwei CME-Punkte erworben werden. Ärzte erhalten sie auf dem Fortbildungskonto gutgeschrieben, Psychotherapeuten bekommen eine Teilnahmebestätigung.

↗ *www.kbv.de/html/7703.php*

THEMENSEITE MIT ERKLÄRVIDEO

Auf der Online-Themenseite der KBV zur IT-Sicherheitsrichtlinie sind alle Informationen und Serviceangebote abrufbar beziehungsweise es wird darauf verlinkt. Das Video „IT-Sicherheitsrichtlinie im Überblick“ bietet einen anschaulichen Einstieg ins Thema. In wenigen Minuten wird erläutert, warum die IT-Sicheheitsrichtlinie wichtig ist und was dazu gehört.

↗ *www.kbv.de/html/it-sicherheit.php*



DR. THOMAS KRIEDEL
MITGLIED DES VORSTANDS DER KBV

„Die IT-Sicherheitsrichtlinie für die vertragsärztliche Versorgung zu erstellen, war ein Auftrag aus dem Digitale-Versorgung-Gesetz. Der KBV war es wichtig, praktikable und realistische Vorgaben für die Praxen zu erarbeiten, die möglichst aufwandsarm umzusetzen sind. Vieles wird im Praxisalltag bereits angewendet, weil es beispielsweise durch die EU-Datenschutzgrundverordnung vorgegeben ist.

Es geht um sensible Gesundheitsdaten, die besonders geschützt werden müssen. Praxisinhaberinnen und Praxisinhaber tragen hierfür eine hohe Verantwortung. Die Richtlinie soll sie dabei unterstützen und ihnen einen verlässlichen Handlungsrahmen bieten.

Im Gesetz ist auch festgelegt, dass der Umfang der Richtlinie jährlich überprüft werden muss. Das ist ein guter Weg, jeweils auf Veränderungen im IT-Bereich und Sicherheitsfragen zu reagieren. Wir werden darauf achten, dass auch bei den Anpassungen immer die Praktikabilität im Vordergrund steht.“

IT-SICHERHEIT IN DER PRAXIS ERSTE STUFE AB APRIL 2021

Nach dem Überblick auf den Seiten 4 und 5 stellen wir hier beispielhaft einige der Anforderungen vor, die ab April 2021 zu erfüllen sind. Tipps und Hinweise sollen Sie bei der Umsetzung unterstützen. Die Regelungen müssen von allen Praxen erfüllt werden, sofern die entsprechenden IT-Komponenten verwendet werden. Fachbegriffe wie Firewall oder Ports und Bezeichnungen wie „vertrauliche Daten“ werden kurz erläutert.

PRAXISCOMPUTER

Anlage 1 Nummer 15

Ihre Praxis setzt aktuelle Virenschutzprogramme ein.

TIPP

↗ Verwenden Sie „Windows Defender“ oder ein anderes kommerzielles Virenschutzprogramm.
↗ Legen Sie fest, welche Daten wann gescannt werden sollen, zum Beispiel jede eingehende E-Mail.

HINWEIS: *Ein Virenschutz- oder Antivirenprogramm ist eine Software, die Computerviren, aber beispielsweise auch sogenannte Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll.*

Anlage 1 Nummer 13

Jede Person, die in Ihrer Praxis Daten verarbeitet, muss sich nach der Nutzung eines Gerätes abmelden oder das Gerät sperren.

TIPP

↗ Es gibt Tastenkombinationen, zum Beispiel „Windows“ + „L“ für die Sperrung bei Windows.
↗ Weisen Sie Ihr Team auf die Abmeldung hin, beispielsweise durch einen Hinweis auf einem Zettel.

OFFICE-PRODUKTE

Anlage 1 Nummer 5

Sie verzichten auf Cloud-Speicherung bei Ihren Office-Produkten.

TIPP

↗ Deaktivieren Sie die in Office-Produkten integrierten Cloud-Speicher zur Speicherung personenbezogener Informationen.
↗ Verwenden Sie kein Microsoft 365 (ehemals Office 365) und kein OneDrive.
↗ Vermeiden Sie Office-Produkte, die Rohdaten sammeln und per automatischer Datenübertragung durch einen im Hintergrund laufenden Dienst an den Entwickler übertragen (Telemetrie).
↗ Nutzen Sie lokal installierte Office-Produkte ohne „integrierte Cloud“-Speicherungen.

HINWEIS: *Office-Produkte sind zum Beispiel Programme für Textverarbeitung, Kalkulationen, Präsentationen oder auch für das Versenden und Empfangen von E-Mails. Clouds sind Speichermöglichkeiten im Internet, die umstritten und nicht ungefährlich sind. Beispielsweise wird es bei Cloud-basierten Office-Produkten immer schwerer abzuschätzen, wie weit der Anbieter der Cloud personenbezogene Daten außerhalb seiner „legitimen Geschäftszwecke“ verarbeitet. Die Datenschutzkonferenz der Datenschutzaufsichtsbehörden der Länder und des Bundes kam 2020 zu dem nicht einstimmigen Ergebnis, dass Microsoft 365 nicht datenschutzkonform einsetzbar ist (https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf).*

PRAXISNETZWERK

Anlage 1 Nummer 13

Ihr internes Netzwerk ist anhand eines Netzplanes dokumentiert.

TIPP

↗ Nutzen Sie das Musterdokument im Hub zur IT-Sicherheitsrichtlinie.
↗ Dokumentieren Sie sowohl die logische Struktur des Netzes insbesondere der Subnetze als auch wie das Netz zoniert und segmentiert wird.
↗ Dokumentieren Sie Änderungen im Netzwerk mit Datum.

HINWEIS: *Ein Netzwerk ist die Infrastruktur der von Ihnen verwendeten Hard- und Software sowie der jeweiligen Verbindungen. Ähnlich einem Stromnetz kann es schematisch als Netzplan dargestellt werden.*

Anlage 1 Nummer 32

Sie schützen den Übergang zu anderen Netzen, zum Beispiel das Internet, durch eine Firewall.

TIPP

↗ Stellen Sie die Firewall so ein, dass nur erlaubte IP-Adressen, Ports (ein- und ausgehend) und Kommunikationsprotokolle zugelassen werden.

HINWEIS: *Eine Firewall ist ein Programm, das Computer oder Netzwerke vor unerwünschten Zugriffen schützen soll. Eine IP-Adresse macht in einem Netzwerk die daran angeschlossenen Geräte erreichbar (adressierbar). Ports sind während einer Verbindung die jeweiligen Endstellen. Kommunikationsprotokolle bilden eine Grundlage für die Vernetzung. Die Datenübertragung zwischen mehreren Parteien wird hier definiert, also wie die Kommunikation erfolgt.*

RECHTLICHER HINWEIS: Diese Übersicht ist keine Rechtsquelle. Die rechtlich verbindlichen Anforderungen stehen in der IT-Sicherheitsrichtlinie mit ihren Anlagen. Diese ist auf der Online-Plattform zur IT-Sicherheitsrichtlinie abrufbar. Auf dieser extra eingerichteten Plattform sind alle Anforderungen aufgeführt und mit Erläuterungen, Hinweisen und Begleitinformationen versehen. Dort befinden sich auch Musterdokumente: *https://hub.kbv.de/site/its*

INTERNET-ANWENDUNG

Anlage 1 Nummer 8

Ihr Internet-Browser ist so eingestellt, dass im Browser keine vertraulichen Daten gespeichert werden.

TIPP

↗ Verwenden Sie zum Löschen der Browserdaten die folgenden Tastenkombinationen:
„Strg“ + „Umschalt“ + „Entf“ bei Chrome, Firefox, Edge;
„cmd“ + „alt“ + „E“ bei Safari
↗ Verwenden Sie Browser wie “Firefox Klar“, die diese Daten mit einem Klick oder nach Beendigung der Anwendung automatisch löschen.

HINWEIS: *Ein Internet-Browser, auch Webbrowser genannt, ist ein Computerprogramm zur Darstellung von Internet- beziehungsweise Webseiten im World Wide Web oder allgemein von Dokumenten und Daten.*

Anlage 1 Nummer 10

In Ihrer Praxis werden verschlüsselte Internetanwendungen genutzt.

TIPP

↗ Achten Sie auf Internetseiten, die mit „https://“ beginnen. https steht für hypertext transfer protocol secure und ist ein sicheres Hypertext-Übertragungsprotokoll, mit dem Daten verschlüsselt übertragen werden können.
↗ Achten Sie auf ein Schloss, das als Icon im Webbrowser angezeigt ist. Durch Anklicken des Schlosses lassen sich Informationen zum Zertifikat und dem Herausgeber einsehen.

HINWEIS: *Verschlüsselung bedeutet, dass eine Klarschrift in eine Geheimschrift umgewandelt wurde und nur mit dem richtigen Schlüssel zurückverwandelt werden kann.*

MOBILE ANWENDUNGEN (APPS)

Anlage 1 Nummer 1

In Ihrer Praxis werden Apps nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.

TIPP

↗ Verwenden Sie für IOS „App Store“ und für Android „Google Play“.
↗ Lassen Sie in den Sicherheitseinstellungen keine Apps aus externen Quellen zu.

HINWEIS: *Apps gibt es für etliche Anwendungen, zum Beispiel um Schritte zu zählen oder Text-, Sprach- und Bildnachrichten auszutauschen. Zu finden sind die mobilen Anwendungen in App-Stores, den digitalen Vertriebsplattformen. Offizielle App-Stores sind beispielsweise der App Store von Apple oder der Google Play Store.*

Anlage 1 Nummer 4

In Ihrer Praxis werden keine vertraulichen Daten über Apps versendet.

TIPP

↗ Senden Sie vertrauliche Daten wie Diagnosen oder Befunde nicht über eine App, auch nicht, wenn ein Patient oder eine Patientin dies wünscht.
↗ Kommunizieren Sie dieses Vorgehen in Ihrem Team.
↗ Schränken Sie den Datenversand ein, um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden.
↗ Überprüfen Sie vor der App-Benutzung, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten.

HINWEIS: *Vertrauliche Daten sind zum Beispiel Patientenbefunde und andere personenbezogene Daten, die nicht für die Öffentlichkeit bestimmt sind und deren Verlust oder Veröffentlichung zu einem Nachteil oder Schaden führen kann.*

SMARTPHONES UND TABLETS

Anlage 1 Nummer 22

Die Smartphones und Tablets Ihrer Praxis sind mit einem komplexen Gerätesperrcode geschützt.

TIPP

↗ Verwenden Sie keine einfachen Codes, die beispielsweise nur aus vier Zahlen bestehen. Wählen Sie komplexe, lange Codes (zum Beispiel insgesamt zwölf Zeichen), die aus einer Kombination von Ziffern und Buchstaben in Groß- und Kleinschreibung bestehen. Damit wird verhindert oder zumindest erschwert, einen Code zu knacken.
↗ Setzen Sie nicht denselben Code für alle Geräte ein.

WECHSELDATENTRÄGER / SPEICHERMEDIEN

Anlage 1 Nummer 30

Wenn Sie Wechseldatenträger oder Speichermedien versenden, tun Sie dies mit einer sicheren Versandart und Verpackung.

TIPP

↗ Informieren Sie sich bei Ihrem Versanddienstleister über sichere Nachweissysteme wie Einschreiben und Wertsendungen.

DIENSTHANDYS

Anlage 1 Nummer 27

Mobiltelefone müssen geupdatet werden.

TIPP

↗ Aktivieren Sie die Funktion, dass Updates automatisch erfolgen (Autoupdates).

FOKUS

TELEMATIKINFRASTRUKTUR: ANFORDERUNGEN AN DEZENTRALE KOMPONENTEN

Die Telematikinfrastruktur, kurz TI, vernetzt Akteure im Gesundheitswesen und ermöglicht eine schnelle und sichere Kommunikation zwischen ihnen. Dabei gelten für alle Komponenten – unabhängig vom Inkrafttreten der IT-Sicherheitsrichtlinie – hohe Anforderungen an die Funktionalität und Sicherheit. So dürfen zum Beispiel nur Konnektoren und Kartenterminals genutzt werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert und von der gematik, der Betreibergesellschaft der TI, zugelassen sind.

UNTERSCHEIDUNG ZWISCHEN ZENTRALEN UND DEZENTRALEN KOMPONENTEN

Die Komponenten der zentralen TI-Plattform werden im Auftrag der gematik in Rechenzentren betrieben, sodass hier die gematik für deren Sicherheit zuständig ist. Dagegen werden die dezentralen Komponenten der TI-Plattform in den Praxen betrieben. Auf diese Komponenten bezieht sich die IT-Sicherheitsrichtlinie. Dazu gehören insbesondere:

- Konnektoren
- Kartenlesegeräte
- Praxisausweis (SMB-C Karte)
- elektronische Heilberufsausweis (eHBA)

Die Anforderungen sind in Anlage 5 der IT-Sicherheitsrichtlinie enthalten. Sie müssen von allen Praxen erfüllt werden und gelten ab Januar 2022 – bis auf eine Ausnahme, die bereits Anfang 2021 in Kraft trat (Nummer 5: Geschützte Kommunikation mit dem Konnektor).

↗ Themenseite Telematikinfrastruktur:
www.kbv.de/html/telematikinfrastruktur.php

ZWEI BEISPIELE AB 1. JANUAR 2022

BEISPIEL 1

UPDATES MÜSSEN ZEITNAH INSTALLIERT WERDEN

Automatische Updates könnten dazu führen, dass der laufende Praxisbetrieb mitten in einer medizinischen Behandlung unterbrochen wird. Daher wird bei der TI das Vorhandensein neuer Updates, beispielsweise für den Konnektor, nur angezeigt, diese werden aber nicht automatisch installiert. In der IT-Sicherheitsrichtlinie ist für alle Praxen ab Januar 2022 ein „zeitnahes Installieren verfügbarer Aktualisierungen“ vorgegeben (Anlage 5 Nummer 6). Praxisinhaber müssen somit ein Update aufspielen, sie können aber selbst bestimmen, dass dies zum Beispiel nicht um 12 Uhr mittags, sondern um 2 Uhr nachts erfolgt. Updates sind für die Sicherheit und Funktionalität erforderlich.

BEISPIEL 2

ADMINISTRATIONSDATEN MÜSSEN SICHER AUFBEWAHRT WERDEN

Die bei der Installation der TI-Komponenten eingerichteten Administrationsdaten müssen sicher aufbewahrt werden (Anlage 5 Nummer 7). Das sind insbesondere Passwörter für den Administrator-Zugang des Konnektors. Jedoch muss gewährleistet sein, dass Praxisinhaber auch ohne den IT-Dienstleister Zugriff auf die Daten haben. Sie können die Administrationsdaten beispielsweise in einem versiegelten Umschlag an einem sicheren Ort hinterlegen. Sollte ein Dienstleister sich weigern, die Daten herauszugeben, so sollte zumindest mit ihm vereinbart werden, dass er die Zugangsdaten zum Vertragsende herausgibt.