RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 390 Sozialgesetzbuch (SGB) Fünftes Buch (V) den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung und –psychotherapeutischen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorischen Maßnahmen im Sinne des Artikel 32 Datenschutz-Grundverordnung (DSGVO) zu standardisieren. Die hier getroffene Richtlinie erfüllt diesen Auftrag und dient damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche und –psychotherapeutische Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen und –psychotherapeutischen Praxis. Die Richtlinie legt technische und organisatorische Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

II. GELTUNGSBEREICH

1. Diese Richtlinie legt die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest.
2. Der/die Praxisinhaber ist/sind verantwortlich für die IT-Sicherheit der Praxis und für die Einhaltung der Anforderungen dieser Richtlinie. Dies umfasst insbesondere auch, die erforderlichen Festlegungen und Regelungen gemäß dieser Richtlinie vorzugeben. Der/die Praxisinhaber kann/können die Umsetzung der einzelnen Anforderungen delegieren.

III. PRAXISGRÖSSEN UND ANFORDERUNGSKATEGORIEN

Die umzusetzenden Anforderungen richten sich nach der Größe der Arztpraxis. Dabei gilt Folgendes:

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

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

3. Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang: Eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichem Umfang ist eine Arztpraxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Arztpraxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Groß-Labore).

IV. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT IN PRAXEN

1. Praxen nach A. III. 1. haben die Anforderungen aus Anlage 1 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

2. Praxen nach A. III. 2. haben die Anforderungen aus Anlage 1, 2 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

3. Praxen nach A. III. 3. haben die Anforderungen aus Anlage 1, 2, 3 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

4. Sofern in der Praxis medizinische Großgeräte, wie medizinische Analysegeräte (IVD-Geräte) in Laboren, Computertomograph, Magnetresonanztomograph, Positronenemissionstomograph und Linearbeschleuniger, eingesetzt werden, sind ergänzend die Anforderungen aus Anlage 4 umzusetzen.

Die in dieser Richtlinie formulierten Anforderungen unterliegen einem kontinuierlichen Verbesserungsprozess mit einer jährlichen Evaluationspflicht. Die erforderliche Evaluation richtet sich an der jeweiligen Informationssicherheitslage aus.

B. INKRAFTTRETEN UND GELTUNG

1. Diese Richtlinie tritt am Tag nach der Veröffentlichung in Kraft. Sie ersetzt die bisherige Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit vom 16.12.2020 und setzt diese außer Kraft.

2. Diese Richtlinie gilt ab dem Tag nach ihrer Veröffentlichung. Hiervon ausgenommen sind folgende mit dieser Richtlinie neu hinzugekommenen Anforderungen:

A1)	1-7	Personal
	8-10	Sensibilisierung und Schulung zur Informationssicherheit
	14-17	Patch- und Änderungsmanagement
	22-26	Endgeräte
	40,41	E-Mail-Client und -Server
	50	Cloud-Anwendungen
A3)	1	Personal
	2	Netzwerksicherheit

	15-17	E-Mail-Client und -Server
A5)	5	gehosteter Konnektor
	6	TI-Gateway

Diese gelten ab dem 01.10.2025.

ANLAGE 1

Anforderungen für Praxen

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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 ausscheidendem 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.
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.
4.	Personal	Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal	Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, müssen mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden.

Nr	Zielobjekt	Anforderung	Erläuterung
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 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 im 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.
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.

Nr	Zielobjekt	Anforderung	Erläuterung
8.	Sensibilisierung und Schulung zur Informationssicherheit	Sensibilisierung der Praxisleitung für Informationssicherheit	Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.
9.	Sensibilisierung und Schulung zur Informationssicherheit	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.
10.	Sensibilisierung und Schulung zur Informationssicherheit	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Alle Mitarbeitenden sollten entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.
11.	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere dem Internet muss durch eine Firewall geschützt werden. Primäres 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.
12.	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.
13.	Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.
14.	Patch- und Änderungsmanagement	Installation von Updates	Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.
15.	Patch- und Änderungsmanagement	Verantwortlichkeit für Updates	Es muss festgelegt werden, wer die Updates installiert. Das ausgewählte Personal muss geschult und entsprechend berechtigt werden.

Nr	Zielobjekt	Anforderung	Erläuterung
16.	Patch- und Änderungsmanagement	Identifizierung ausbleibender Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.
17.	Patch- und Änderungsmanagement	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.
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.
19.	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.
20.	Endgeräte	Einsatz von Viren-Schutzprogrammen	Aktuelle Virenschutzprogramme sind einzusetzen.
21.	Endgeräte	Regelmäßige Datensicherung	Sämtliche relevante Daten sind regelmäßig zu sichern.
22.	Endgeräte	Schutz der Datensicherung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.
23.	Endgeräte	Art der Datensicherung	Es muss festgelegt werden, wie die Daten gesichert werden.
24.	Endgeräte	Verantwortliche der Datensicherung	Es 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.
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.

Nr	Zielobjekt	Anforderung	Erläuterung
27.	Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.
28.	Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Berechtigungen und Zugriffe sind pro Personengruppe und pro Person zu regeln.
29.	Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	So wenige personenbezogene Daten wie möglich sind zu verwenden.
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.
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 für die verarbeiteten Daten sichergestellt werden muss.
32.	Smartphone und Tablet	Verwendung eines Zugriffschutzes	Geräte sind mit einem komplexen Gerätesperrcode zu schützen.
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.
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.
35.	Mobiltelefon	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.
36.	Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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.
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.
40.	E-Mail-Client und -Server	Sichere Konfiguration der E-Mail-Clients	Bei der Konfiguration der E-Mail-Clients muss mindestens Folgendes berücksichtigt werden: • 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.
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

Nr	Zielobjekt	Anforderung	Erläuterung
			und danach die App inkl. aller enthaltenen Daten auf dem Gerät zu deinstallieren.
43.	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Es sollten nur Apps genutzt werden, die Dokumente verschlüsselt und lokal abspeichern.
44.	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.
45.	Internet-Anwendungen - Anbieter	Authentisierung bei Webanwendungen	Sollten Sie als Praxis einen Webdienst anbieten: Der IT-Betrieb muss Webanwendungen und Webservices so konfigurieren, dass 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.
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.

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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 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.
49.	Internet-Anwendungen - Anwender	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).
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.

ANLAGE 2

Zusätzliche Anforderungen für mittlere Praxen

Nr	Zielobjekt	Anforderung	Erläuterung
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.
2.	Endgeräte	Nutzung von verschlüsselten Kommunikationsverbindungen	Benutzer sollten darauf achten, dass zur Verschlüsselung von Kommunikationsverbindungen kryptografische Algorithmen nach dem Stand der Technik wie z.B. TLS verwendet werden.
3.	Endgeräte	Restriktive Rechtevergabe	Rechte sollten so restriktiv wie möglich nach dem Need-to-know Prinzip vergeben werden.
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.
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.
6.	Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.
7.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.
8.	Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.
9.	Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.
10.	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken bzw. zu vergeben.

ANLAGE 3

Zusätzliche Anforderungen für Großpraxen

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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.
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.
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 und Kontrolle der Geräte festgelegt werden.
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.

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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.
8.	Mobile Device Management (MDM)	Berechtigungsmanagement im MDM	Für das MDM muss ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.
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.
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.
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.
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.
13.	Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.
14.	Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.
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

Nr	Zielobjekt	Anforderung	Erläuterung
			als Spam-Relay missbraucht werden können.
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.
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. Diese Prüfung sollte zum Schutz des Clients auf dem Mail-Server erfolgen.

ANLAGE 4

Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte

Nr	Zielobjekt	Anforderung	Erläuterung
1.	Medizinische Großgeräte	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeitende 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.
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.
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.
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.
5.	Medizinische Großgeräte	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.
6.	Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden. Insbesondere sollten ferngewartete medizinische Großgeräte in einem eigenen Netzwerksegment eingebunden werden.

ANLAGE 5

DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR

Nr	Zielobjekt	Anforderung	Erläuterung
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.
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.
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.
4.	Konnektor	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.
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.
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.
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.
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.
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

Nr	Zielobjekt	Anforderung	Erläuterung
			gewährleistet sein, dass der Leistungserbringer auch ohne seinen Dienstleister die Daten kennt.