

Persönliche Checkliste* zur Umsetzung der IT-Sicherheitsrichtlinie § 390 SGB V zum 02.01.2026

* = entfällt/nicht relevant ? = unbekannt ! = in Planung → = Umsetzung begonnen ✓ = wird umgesetzt

zu Anlage 1: Anforderungen für Praxen

Nr.	Anforderung	Erläuterung	*	?	!	→	✓
Zielobjekt: Personal							
1.	Geregelte Einarbeitung neuer Mitarbeitender	Mitarbeitende müssen zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet und über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden.					
2.	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 ausscheidenden Mitarbeitenden bekannt waren oder von diesen genutzt wurden, müssen geändert oder vernichtet werden. Vor der Verabschiedung muss noch einmal auf die fortdauernden Verschwiegenheitsverpflichtungen hingewiesen werden.					
3.	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 Zugangsberechtigungen sind so restriktiv wie möglich zu halten.					
4.	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.					
5.	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.	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.					

Nr.	Anforderung	Erläuterung	x	?	!	→	✓
7.	Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden	Bei der Einstellung neuer Mitarbeitenden <u>sollte</u> besonders auf ihre Vertrauenswürdigkeit, beispielsweise bei der Prüfung vorliegender Arbeitszeugnisse, geachtet werden. Soweit möglich, <u>sollten</u> alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerbenden, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind.					
Zielobjekt: Sensibilisierung und Schulung zur Informationssicherheit							
8.	Sensibilisierung der Praxisleitung für Informationssicherheit	Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.					
9.	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.	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Alle Mitarbeitenden <u>sollten</u> entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.					
Zielobjekt: Netzwerksicherheit							
11.	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 <u>sollten</u> nur erlaubte Verbindungen aus dem geschützten Netz nach außen aufgebaut werden können.					
12.	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.					
13.	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.					
Zielobjekt: Patch- und Änderungsmanagement							
14.	Installation von Updates	Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.					
15.	Verantwortlichkeit für Updates	Es muss festgelegt werden, wer die Updates installiert. Das ausgewählte Personal muss geschult und entsprechend berechtigt werden.					
16.	Identifizierung ausbleibender Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.					
17.	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.					
Zielobjekt: Endgeräte							
18.	Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras	Mikrofon und Kamera am Rechner <u>sollten</u> grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.					
19.	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.					

Nr.	Anforderung	Erläuterung	x	?	!	→	✓
20.	Einsatz von Viren-Schutzprogrammen	Aktuelle Virenschutzprogramme sind einzusetzen.					
21.	Regelmäßige Datensicherung	Sämtliche relevante Daten sind regelmäßig zu sichern.					
22.	Schutz der Datensicherung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.					
23.	Art der Datensicherung	Es muss festgelegt werden, wie die Daten gesichert werden.					
24.	Verantwortliche der Datensicherung	Es muss festgelegt werden, wer für die Datensicherung zuständig ist.					
25.	Test der Datensicherung	Es <u>sollte</u> getestet werden, ob gesicherte Daten funktionsfähig und vollständig vorhanden sind.					
26.	Der Zugriff auf Geräte und Software muss abgesichert werden.	Es <u>sollten</u> 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.					
Zielobjekt: Endgeräte mit dem Betriebssystem Windows							
27.	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten <u>sollte</u> vollständig deaktiviert werden.					
28.	Datei- und Freigabeberechtigungen	Berechtigungen und Zugriffe sind pro Personengruppe und pro Person zu regeln.					
29.	Datensparsamkeit	So wenige personenbezogene Daten wie möglich sind zu verwenden.					
Zielobjekt: Smartphone und Tablet							
30.	Verwendung der SIM-Karten-PIN	SIM-Karten sind durch eine PIN zu schützen. Super-PIN/PUK sind nur durch Verantwortliche anzuwenden.					
31.	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten <u>sollten</u> die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräten das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss .					
32.	Verwendung eines Zugriffsschutzes	Geräte sind mit einem komplexen Gerätesperrcode zu schützen.					
33.	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen der Endgeräte <u>sollte</u> in den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.					
Zielobjekt: Mobiltelefon							
34.	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.	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen <u>sollten</u> auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.					
Zielobjekt: Wechseldatenträger/Speichermedien							
36.	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.					

Nr.	Anforderung	Erläuterung	x	?	!	→	✓
37.	Angemessene Kennzeichnung der Datenträger beim Versand	Beim Versand von Datenträgern <u>sollte</u> der Absender diese für den Empfänger eindeutig kennzeichnen. Dabei <u>sollte</u> die Kennzeichnung möglichst keine Rückschlüsse auf den Inhalt für andere ermöglichen.					
38.	Sichere Versandart und Verpackung	Zum Versand von Datenträgern <u>sollten</u> Versandanbieter mit sicherem Nachweis-System und eine möglichst manipulationssichere Versandart und Verpackung gewählt werden.					
39.	Sicheres Löschen der Datenträger vor und nach der Verwendung	Alle Datenträger müssen nach ihrer Verwendung durch die jeweiligen Mitarbeitenden sicher und vollständig gelöscht werden.					
Zielobjekt: E-Mail-Client und -Server							
40.	Sichere Konfiguration der E-Mail-Clients	Bei der Konfiguration der E-Mail-Clients muss mindestens Folgendes berücksichtigt werden: <ul style="list-style-type: none"> • Dateianhänge von E-Mails <u>sollten</u> vor dem Öffnen auf Schadsoftware geprüft werden • die automatische Interpretation von HTML-Code und anderen aktiven Inhalten in E-Mails <u>sollte</u> deaktiviert werden • zur Kommunikation mit E-Mail-Servern über nicht vertrauenswürdige Netze <u>sollte</u> eine sichere Transportverschlüsselung eingesetzt werden 					
41.	Umgang mit Spam durch Benutzende	Grundsätzlich <u>sollten</u> die Benutzenden alle Spam-E-Mails ignorieren und löschen. Die Benutzenden <u>sollten</u> auf unerwünschte E-Mails nicht antworten. Sie <u>sollten</u> Links in diesen E-Mails nicht folgen.					
Zielobjekt: Mobile Anwendungen (Apps)							
42.	Sichere Apps nutzen	Apps <u>sollten</u> 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 inkl. aller enthaltenen Daten auf dem Gerät zu deinstallieren.					
43.	Sichere Speicherung lokaler App-Daten	Es <u>sollten</u> nur Apps genutzt werden, die Dokumente verschlüsselt und lokal abspeichern.					
44.	Verhinderung von Datenabfluss	Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.					
Zielobjekt: Internet-Anwendungen - Anbieter							
45.	Authentisierung bei Webanwendungen	<u>Sollten</u> 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 <u>sollte</u> dokumentiert werden. Der IT-Betrieb muss geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.					
46.	Schutz vertraulicher Daten	<u>Sollten</u> 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.	Anforderung	Erläuterung	x	?	!	→	✓
47.	Einsatz von Web Application Firewalls	Sollten Sie als Praxis einen Webdienst anbieten: Institutionen <u>sollten</u> eine Web Application Firewall (WAF) einsetzen. Die Konfiguration der eingesetzten WAF <u>sollte</u> auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices <u>sollte</u> die Konfiguration der WAF geprüft werden.					
48.	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.	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).					
Zielobjekt: Cloud-Anwendungen - Anbieter							
50.	Sicherheit von Cloud-Dienstleistern	Soweit Sozial- oder Gesundheitsdaten im Wege des Cloud-Computing verarbeitet werden <u>sollen</u> , muss der Anbieter der eingesetzten Cloud-Anwendung über ein aktuelles C5-Testat entsprechend §393 SGB V in Verbindung mit §384 SGB V verfügen.					

zu Anlage 2: Zusätzliche Anforderungen für mittlere Praxen

✖ = entfällt/nicht relevant ? = unbekannt ! = in Planung → = Umsetzung begonnen ✓ = wird umgesetzt

Nr.	Anforderung	Erläuterung	✖	?	!	→	✓
Zielobjekt: Netzwerksicherheit							
1.	Alarmierung und Logging	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen <u>sollten</u> automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.					
Zielobjekt: Endgeräte							
2.	Nutzung von verschlüsselten Kommunikationsverbindungen	Benutzende <u>sollten</u> darauf achten, dass zur Verschlüsselung von Kommunikationsverbindungen kryptografische Algorithmen nach dem Stand der Technik wie z.B. TLS verwendet werden.					
3.	Restriktive Rechtevergabe	Rechte <u>sollten</u> so restriktiv wie möglich nach dem Need-to-know Prinzip vergeben werden.					
Zielobjekt: Endgeräte mit dem Betriebssystem Windows							
4.	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen <u>sollte</u> zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.					
Zielobjekt: Smartphone und Tablet							
5.	Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten	Es <u>sollte</u> eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten erstellt werden.					
6.	Verwendung von Sprachassistenten	Sprachassistenten <u>sollten</u> nur eingesetzt werden, wenn sie zwingend notwendig sind.					
Zielobjekt: Mobiltelefon							
7.	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, <u>muss</u> eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.					
8.	Sichere Datenübertragung über Mobiltelefone	Es <u>sollte</u> geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.					
Zielobjekt: Wechseldatenträger/Speichermedien							
9.	Regelung zur Mitnahme von Wechseldatenträgern	Es <u>sollte</u> klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.					
Zielobjekt: Mobile Anwendungen (Apps)							
10.	Minimierung und Kontrolle von App-Berechtigungen	Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken bzw. zu vergeben.					

zu Anlage 3: Anforderungen für Großpraxen oder Praxis mit Datenverarbeitung im erheblichen Umfang

✖ = entfällt/nicht relevant ? = unbekannt ! = in Planung → = Umsetzung begonnen ✓ = wird umgesetzt

Nr.	Anforderung	Erläuterung	✖	?	!	→	✓
Zielobjekt: Personal							
1.	Messung und Auswertung des Lernerfolgs	Die Lernerfolge im Bereich Informationssicherheit <u>sollten</u> zielgruppenbezogen gemessen und ausgewertet werden. Die Ergebnisse <u>sollten</u> bei der Verbesserung des Sensibilisierungs- und Schulungsangebots zur Informationssicherheit in geeigneter Weise einfließen.					
Zielobjekt: Netzwerksicherheit							
2.	Planung des internen Netzwerkes	Bei der Planung des internen Netzwerkes <u>soll</u> eine Netzwerksegmentierung erfolgen, die berücksichtigt, welche Daten in dem jeweiligen Segment verarbeitet und kommuniziert werden. Hierbei <u>soll</u> eine Trennung zwischen Gesundheitsdaten und weniger kritischen Daten erfolgen.					
3.	Absicherung von schützenswerten Informationen	Schützenswerte Informationen <u>müssen</u> über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.					
Zielobjekt: Smartphone und Tablet							
4.	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, <u>muss</u> eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.					
5.	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores <u>sollten</u> vor einer gewünschten Installation durch die Verantwortlichen geprüft und freigegeben werden.					
6.	Definition der erlaubten Informationen und Applikationen auf mobilen Geräten	Die Praxis <u>sollte</u> festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.					
Zielobjekt: Mobile Device Management (MDM)							
7.	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM und das interne Netz der Institution <u>muss</u> angemessen abgesichert werden.					
8.	Berechtigungsmanagement im MDM	Für das MDM <u>muss</u> ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.					
9.	Verwaltung von Zertifikaten	Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät <u>sollten</u> zentral über das MDM installiert, deinstalliert und aktualisiert werden.					
10.	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM <u>muss</u> sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.					
11.	Auswahl und Freigabe von Apps	Nur durch die Verantwortlichen geprüfte und freigegebene Apps dürfen über das MDM zur Installation angeboten werden.					
12.	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis <u>muss</u> festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.					

Nr.	Anforderung	Erläuterung	x	?	!	→	✓
Zielobjekt: Wechseldatenträger/Speichermedien							
13.	Datenträgerverschlüsselung	Wechseldatenträger <u>sollten</u> vollständig verschlüsselt werden.					
14.	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen <u>sollte</u> eingesetzt werden.					
15.	Sicherer Betrieb von E-Mail-Servern	Bei dem Betrieb von E-Mail-Servern muss mindestens Folgendes berücksichtigt werden: <ul style="list-style-type: none"> • es muss eine sichere Transportverschlüsselung für das Senden und Empfangen von E-Mails ermöglicht werden • es <u>sollten</u> 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.					
16.	Datensicherung und Archivierung von E-Mails	Die Daten der E-Mail-Server und -Clients sind regelmäßig und verschlüsselt zu sichern.					
17.	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 <u>sollte</u> zum Schutz des Clients auf dem Mail-Server erfolgen.					

zu Anlage 4: Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte

✘ = entfällt/nicht relevant ? = unbekannt ! = in Planung → = Umsetzung begonnen ✓ = wird umgesetzt

Nr.	Anforderung	Erläuterung	✘	?	!	→	✓
Zielobjekt: Medizinische Großgeräte							
1.	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechnete Mitarbeitende auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellereitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellereitig gesetzte Benutzerkonten <u>sollten</u> gewechselt werden.					
2.	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.	Protokollierung	Es muss festgelegt werden: <ul style="list-style-type: none"> • welche Daten und Ereignisse protokolliert werden <u>sollen</u>, • wie lange die Protokolldaten aufbewahrt werden und • wer diese einsehen darf. Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.					
4.	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.	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.					
6.	Netzsegmentierung	Medizinische Großgeräte <u>sollten</u> von der weiteren IT getrennt werden. Insbesondere <u>sollten</u> ferngewartete medizinische Großgeräte in einem eigenen Netzwerksegment eingebunden werden.					

zu Anlage 5: Dezentrale Komponenten der Telematikinfrastruktur

✖ = entfällt/nicht relevant ? = unbekannt ! = in Planung → = Umsetzung begonnen ✓ = wird umgesetzt

Nr.	Anforderung	Erläuterung	✖	?	!	→	✓
Zielobjekt: Dezentrale Komponenten der TI							
1.	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.	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.	Schutz vor unberechtigtem physischem Zugriff	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.					
Zielobjekt: Konnektor							
4.	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.					
Zielobjekt: gehosteter Konnektor							
5.	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.					
Zielobjekt: TI Gateway							
6.	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.					
Zielobjekt: Primärsysteme							
7.	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.					
Zielobjekt: Dezentrale Komponenten der TI							
8.	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.	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 die Praxis auch ohne ihre Dienstleister die Daten kennt.					

*) Dies ist ein persönliches, fakultatives Arbeitsmaterial, das der Kontrolle der Umsetzung der IT-Sicherheitsrichtlinie dienen soll. Es ist nicht Bestandteil der IT-Sicherheitsrichtlinie. Keine Gewähr für Richtigkeit und Vollständigkeit der Angaben. Es gilt die IT-Sicherheitsrichtlinie einschließlich ihrer Anlagen!