Leitfaden

zur IT-Sicherheitsrichtlinie der KBV nach § 75b SGB V

Informationssicherheit und Datenschutz in ärztlichen und zahnärztlichen Praxen mit Cyber-Versicherungen

Die vollständigen Inhalte sind mit dem Autorisierungs-Code über MC-PRAXIS 75b digital nutzbar.

MCSS AG
MioCloud
Solution Systems

Leitfaden für Informationssicherheit und Datenschutz in ärztlichen und zahnärztlichen Praxen mit Cyber-Versicherungen

Überblick

Informationssicherheit (inkl. Cyberschutz) und Datenschutz in ärztlichen und zahnärztlichen Praxen hat durch aktuelle Entwicklungen eine hohe Priorität bekommen. Mit dem Abschluss einer Cyber-Versicherung wurde ein wichtiger Schritt für mehr Sicherheit eingeleitet. Jede Praxis hat nach der KBV IT-Sicherheitsrichtlinie gemäß § 75b Sozialgesetzbuch V (SGB V) eine ausdrückliche Verpflichtung, geeignete organisatorische und technische Maßnahmen (TOM) umzusetzen. Dieser Leitfaden bietet als Assistenz-Service im Rahmen der Cyber-Versicherung pragmatische Unterstützung bei der Einführung der Sicherheits- und Schutz-Maßnahmen.

Checkliste zu Anforderungen nach § 75b SGB V

Die IT-Sicherheitsrichtlinie der KBV und des Bundesamts für Sicherheit in der Informationstechnik (BSI) stellt eine gute Basis für notwendige Maßnahmen dar. Die in diesem Leitfaden enthaltene Checkliste erlaubt einen schnellen Überblick über den Ist-Zustand und die zu treffenden Maßnahmen nach Prioritäten.

Curriculum (Einführungsplan) für 12 Monate

Natürlich sind die Belastungen in allen Praxen in diesen Zeiten hoch und Kapazitäten sind begrenzt.
Deshalb wurde dieser Leitfaden und das **MCSS Assistenz-System** zeit- und kostensparend entwickelt.
Ein Curriculum für einen ersten Einführungszeitraum von 12 Monaten gibt einen realistischen „Fahrplan“ vor.
Begleitet wird dieser mit 4 Webinaren für die Verantwortlichen (eine Schulung pro Quartal).

Cloudsystem MC-PRAXIS 75b

Der Leitfaden ist als schnelle und einfache Einführung in Informationssicherheit und Datenschutz entwickelt worden. Dahinter steht ein cloudbasiertes Sicherheitsmanagementsystem für Cyberschutz, Informationssicherheit und Datenschutz. Mit Abschluss der Cyber-Versicherung haben die versicherten Praxen Zugang zu dem **MC-PRAXIS 75b** Managementsystem über das Internet. Dazu nutzt man einen digitalen Zugangs-Code, der per E-Mail bzw. Schreiben mitgeteilt wurde. Das System kann mit PCs, Laptops, Tablet-Computern und auch Smartphones überall dort genutzt werden, wo ein Internet-Anschluss zur Verfügung steht.

Während dieser analoge Leitfaden nur begrenzte Informationen und Wissens-Module zur Verfügung stellen kann, bietet das cloudbasierte **MC-PRAXIS 75b** System über 2.400 Funktionen und Komponenten:

- **Status-Analysen** erlauben die Bewertung bereits eingesetzter technischer, organisatorischer und rechtlicher Maßnahmen. Die Analysen liefern Messwerte über den „Reifegrad“ der Praxis-Organisation.
- **Wissenstests** mit „Multiple Choice“ Antworten geben den Mitarbeitenden die Möglichkeiten, ihre Kenntnisse zu den wichtigsten Anforderungen für Informationssicherheit und Datenschutz zu prüfen.
- **Checklisten** sind eine praktische Anleitung, um Cyberschutz zusammen mit dem Team in Schulungen nach einem strukturierten Plan (siehe Curriculum) umzusetzen.
- **Verfahrensanweisungen** (nach ISO 9001) und Interne Regelungen (nach QEP) bilden die Grundlage für ein professionelles Qualitätsmanagement auch für die Sicherheitsmaßnahmen.
- **MC-SMARTLEARN** ist ein speziell für die Mitarbeitenden entwickeltes Trainingsprogramm, das zeitgemäß als App auf dem Smartphone abgerufen werden kann.
- **Berichts-Generierung** zur Erfüllung der gesetzlichen Verpflichtungen nach § 75b SGB V und DSGVO ist durch entsprechende Vorlagen mit geringem Zeitaufwand möglich.
- **Webinare** können Verantwortliche in den Praxen bei der Führung der Teams mit Fachwissen und Unterlagen unterstützen.
- **Schulungsnachweise** können vom **MCSS Kundenservice** digital zur Verfügung gestellt werden (Sicherheit bei Sicherheits-Audits).

Zugang zum Cloudsystem

Der Zugang zum digitalen Assistenz-System für Cyber-Versicherte ist bereits durch die Versicherungsprämie lizenziert und sehr einfach zu nutzen. **MCSS** stellt den sicheren Zugangs-Code allen Versicherten zur Verfügung. Dazu wird die im Versicherungsvertrag angegebene E-Mail-Adresse verwendet.

Achtung: Wenn der Code bislang nicht eingegangen ist, bitte auch im SPAM Ordner des Postfachs nachschauen.
Ansonsten Nachfrage an: anwenderservice@mcss-ag.de mit Angabe der Cyber-Versicherungs-Nr.

Einleitung zur IT-Sicherheitsrichtlinie der KBV

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen 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 ITDienstleister 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 Einhaltung der Anforderungen dieser Richtlinie.

III. PRAXISGRÖSSEN UND ANFORDERUNGSKATEGORIEN

Die umzusetzenden Anforderungen richten sich nach der Größe der Praxis.

Dabei gilt Folgendes:

1. Praxis:
   Eine Praxis ist eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen.
2. Mittlere Praxis:
   Eine mittlere Praxis ist eine vertragsärztliche Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen.
3. Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang:
   Eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichem Umfang ist eine Praxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore).

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 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

Diese Richtlinie tritt am Tag nach der Veröffentlichung in Kraft. Die Anforderungen gelten ab den in den Anlagen angegebenen Zeitpunkten.

KBV Anlage 1

Nr.	Zielobjekt	Anforderung	Priorität			Status (in %)			Verantwortung	Datum
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen		**1**	**2**	**3**	**0**	**50**	**100**		
1	Mobile Anwendungen	**Sichere Apps nutzen**								
		Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps löschen.		x						
2	Mobile Anwendungen	**Aktuelle App-Versionen**								
		Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.		x						
3	Mobile Anwendungen	**Sichere Speicherung lokaler App-Daten**								
		Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.			x					
4	Mobile Anwendungen	**Verhinderung von Datenabfluss**								
		Keine vertraulichen Daten über Apps versenden.		x						
5	Office-Produkte	**Verzicht auf Cloud-Speicherung**								
		Keine Nutzung der in Office-Produkte integrierten Cloud-Speicher zur Speicherung personenbezogener Informationen.			x					
6	Office-Produkte	**Beseitigung von Rest Informationen vor Weitergabe von Dokumente**								
		Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.			x					
7	Internet-Anwendungen	**Authentisierung bei Webanwendungen**								
		Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.		x						
8	Internet-Anwendungen	**Schutz vertraulicher Daten**								
		Stellen Sie Ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.			x					
9	Internet-Anwendungen	**Firewall benutzen**								
		Verwendung und regelmäßiges Update einer Web App Firewall.	**x**							
10	Internet-Anwendungen	**Kryptografische Sicherung vertraulicher Daten**								
		Nur verschlüsselte Internet-Anwendungen nutzen.		x						
11	Internet-Anwendungen	**Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen**								
		Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.			x					
12	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.	**x**							
13	Endgeräte	**Abmelden nach Aufgabenerfüllung**								
		Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.	**x**							
14	Endgeräte	**Regelmäßige Datensicherung**								
		Sichern Sie regelmäßig Ihre Daten.	**x**							
15	Endgeräte	**Einsatz von Viren Schutzprogrammen**								
		Setzen Sie aktuelle Virenschutzprogramme ein.	**x**							
16	Endgeräte (Windows)	**Konfiguration von Synchronisationsmechanismen**								
		Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.		x						
17	Endgeräte (Windows)	**Datei- und Freigabeberechtigungen**								
		Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.	**x**							
18	Endgeräte (Windows)	**Datensparsamkeit**								
		Verwenden Sie so wenige persönliche Daten wie möglich.		x						
19	Smartphone und Tablet	**Schutz vor Phishing und Schadprogrammen im Browser**								
		Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.	**x**							
20	Smartphone und Tablet	**Verwendung der SIM-Karten PIN**								
		SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.		x						
21	Smartphone und Tablet	**Sichere Grundkonfiguration für mobile Geräte**								
		Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräte das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.		x						
22	Smartphone und Tablet	**Verwendung eines Zugriffschutzes**								
		Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.	**x**							
23	Smartphone und Tablet	**Updates von Betriebssystem und Apps**								
		Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.	**x**							

24	Smartphone und Tablet	**Datenschutz-Einstellungen**								
		Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.		x						
25	Mobiltelefon	**Sperrmaßnahmen bei Verlust eines Mobiltelefons**								
		Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.			x					
26	Mobiltelefon	**Nutzung der Sicherheitsmechanismen von Mobiltelefonen**								
		Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.		x						
27	Mobiltelefon	**Updates von Mobiltelefonen**								
		Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.			x					
28	Wechseldatenträger / Speichermedien	**Schutz vor Schadsoftware**								
		Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.	**x**							
29	Wechseldatenträger / Speichermedien	**Angemessene Kennzeichnung der Datenträger beim Versand**								
		Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.			x					
30	Wechseldatenträger / Speichermedien	**Sichere Versandart und Verpackung**								
		Versand-Anbieter mit sicherem Nachweis-System, manipulationssichere Versandart und Verpackung.			x					
31	Wechseldatenträger / Speichermedien	**Sicheres Löschen der Datenträger vor und nach der Verwendung**								
		Datenträger nach Verwendung immer sicher und vollständig Löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.		x						
32	Netzwerksicherheit	**Absicherung der Netzübergangspunkte**								
		Der Übergang zu anderen Netzen, insbesondere dem Internet, muss durch eine Firewall geschützt werden.	**x**							
33	Netzwerksicherheit	**Dokumentation des Netzes**								
		Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	**x**							
34	Netzwerksicherheit	**Grundlegende Authentisierung für den Netzmanagement-Zugriff**								
		Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.	**x**							

KBV Anlage 5

Nr.	Zielobjekt	Anforderung	Priorität			Status (in %)			Verantwortung	Datum
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen		1	2	3	0	50	100		
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.	**x**							
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.	**x**							
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.		x						
4	Konnektor	**Betriebsart „parallel“**								
		Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungserbringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.		x						
5	Primärsysteme	**Geschützte Kommunikation mit dem Konnektor**								
		Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.	**x**							
6	Dezentrale Komponenten der TI	**Zeitnahes Installieren verfügbarer Aktualisierungen**								
		Die TI-Komponeten 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.	**x**							
7	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.		x						

Leitfaden Curriculum Informationssicherheit und Datenschutz (Planungszeitraum 12 Monate)

Quartal	Themenblöcke	Referenz
Q 01	Informationssicherheit: Kenntnisse der Rechtsnormen	Informationssicherheit
	Datenschutz: Kenntnisse der rechtlichen Verpflichtungen	Datenschutz
	(kann mit Qualitätsmanagement Maßnahmen ergänzt werden)	*Qualitätsmanagement*
	Anwendung von sicheren Passwörtern	Informationssicherheit
	Datenschutzleitlinie & -richtlinien	Datenschutz
		Qualitätsmanagement
Q 02	Einsatz von Firewalls & Virenschutz	Informationssicherheit
	AV-Verträge (Auftragsverarbeitungs-Verträge)	Datenschutz
		Qualitätsmanagement
	Prävention für Phishing-Angriffe	Informationssicherheit
	Zustimmungen für Datenverarbeitung	Datenschutz
		Qualitätsmanagement
Q 03	Private Nutzung des Internets/eigene Geräte	Informationssicherheit
	Weitergabe von Personendaten	Datenschutz
		Qualitätsmanagement
	Zutrittskontrolle, Zugangskontrolle, Zugriffs- und Weitergabekontrolle	Informationssicherheit
	Geheimhaltung & berufliche Schweigepflicht	Datenschutz
		Qualitätsmanagement
Q 04	Kommunikation und Information im Team zur Informationssicherheit	Informationssicherheit
	Verbale Kommunikation und Datenschutz	Datenschutz
		Qualitätsmanagement
	Notfallmanagement in der IT-Sicherheit	Informationssicherheit
	Verhalten bei Datenpannen	Datenschutz
		Qualitätsmanagement

Anwendungshinweise zur Checkliste und der Curriculum-Vorlage zur IT-Sicherheitsrichtlinie der KBV (§ 75b)

Überblick

Die Kassenärztliche Bundesvereinigung (KBV) hat in enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die IT-Sicherheitsrichtlinie gemäß § 75b Sozialgesetzbuch V (SGB V) veröffentlicht und zum 1.1.2020 in Kraft gesetzt. Ärztliche und zahnärztliche Praxen können selbst entscheiden, wie diese Richtlinie für Informationssicherheit und Cyberschutz praktisch umgesetzt wird. Dabei ist die individuelle Lage einer Praxis mit den Risiken und Möglichkeiten zu berücksichtigen. Das **MC-PRAXIS 75b** System, das im Rahmen der Cyber-Versicherung zur Verfügung gestellt wird, bietet eine pragmatische Unterstützung für dieses Projekt.

Checkliste zu Anforderungen nach § 75b SGB V

Die Anforderungen der IT-Sicherheitsrichtlinie der KBV und des BSI (Anlage 1&5) wurden im Leitfaden zu einer einfachen Checkliste zusammengestellt.

- **Wer kann die Checkliste bearbeiten?**
  - Mitarbeitende mit Grundkenntnissen zum Einsatz von Informationstechnologie können die Checkliste für die Praxis bearbeiten.
  - Falls notwendig, kann der externe IT-Partner/die externe IT-Partnerin einbezogen werden.
- **Was wird in die Checkliste eingetragen?**
  - In den Spalten „Priorität“ sind bereits die Prioritäten 1-3 eingetragen. Bei der Umsetzung wird empfohlen, mit Priorität 1 (sehr wichtig) zu starten. Anschließend können die weiteren Prioritäten bearbeitet werden.
  - In den rechten Spalten kann eingetragen werden, wie der Status bei der Umsetzung der einzelnen Anforderung aktuell zum Start des Projekts ist:
    - **0%** = noch nicht begonnen oder nicht relevant
    - **50%** = bereits eingeleitet und in Bearbeitung
    - **100%** = vollständig umgesetzt
  - In jeder Organisation ist es wichtig, dass die Zuständigkeit und Verantwortung klar definiert sind. Es wird empfohlen, 2 Mitarbeitende als Koordinierende einzusetzen (inkl. einer Vertretung).
  - Als Datum kann man das Datum der ersten Statusanalyse eintragen. Natürlich kann man die Checkliste auch kopieren und den Status regelmäßig (z.B. alle 3 Monate) überprüfen.
- **Welche Informationen stehen zusätzlich zur Verfügung?**
  - Im Rahmen der Cyber-Versicherung steht das digitale Assistenz-System **MC-PRAXIS 75b** zur Verfügung. Über den individuellen Zugangs-Code (siehe E-Mail) kann das cloudbasierte System genutzt werden. In der Cloud stehen alle relevanten Unterlagen wie Verfahrensanweisungen, Checklisten und Trainingsunterlagen zur Verfügung.
  - Die **MCSS AG** als Partnerin der Cyber-Versicherung bietet auch unterstützende Webinare an. Die Termine erfährt man unter www.mcss-ag.de.

Curriculum (Einführungsplan) für 12 Monate

Je nach Reifegrad der eigenen Praxis-Organisation und der verfügbaren Kapazitäten und Qualifikationen benötigen Praxen zwischen 12 und 24 Monate zur vollständigen Umsetzung der KBV-Richtlinie.
In diesem Leitfaden-Dokument ist eine Beispiel-Vorlage für 12 Monate enthalten:

- **Wie können die Aufgaben eingeteilt werden?**
  - Die Aufgaben sind unterteilt nach 3 Rubriken:
    - Informationssicherheit nach § 75b SGB V
    - Datenschutz nach DSGVO
    - Qualitätsmanagement nach § 135ff SGB V
  - Je nach Praxis-Organisation können die einzelnen Bereiche parallel bearbeitet werden. Wenn sowohl Datenschutz wie auch QM optimal umgesetzt sind, kann jeweils nur die Aufgabe zur Informationssicherheit (IS) bearbeitet werden.
- **Welche Unterstützung steht für die Umsetzung nach Curriculum zur Verfügung?**
  - Die Praxen werden im Rahmen der Cyber-Versicherung durch Webinare unterstützt. Pro Quartal wird ein Webinar (40 min.) angeboten. Die Inhalte entsprechen den Aufgaben im Curriculum.
  - Für alle Aufgaben stehen in der Cloud (**MC-PRAXIS 75b**) umfangreiche Vorlagen (wie Verfahrensanweisungen, Wissenstests, Erklärvideos etc.) zur Verfügung:
    Man wählt im Hauptmenü den Bereich „Coaching“.

Einführung in die Informationssicherheit (MC-SMARTLEARN)

1 IT-Sicherheitsregelungen nach Art. 32 DSGVO

- Mit Inkrafttreten der **Datenschutz-Grundverordnung** gelten auch Regelungen für die Datensicherheit und den Cyberschutz.
- Nach **Art. 32 DSGVO** müssen Maßnahmen zur Sicherheit der Datenverarbeitung umgesetzt werden.
- Wichtig ist, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen.
- Die wichtigsten verpflichtenden Anforderungen sind:
  - Regelmäßige Datensicherungen
  - Einsatz von Virenschutzprogrammen
- Weitere Anforderungen sind:
  - Regelungen für **Berechtigungen und Zugriffe** zu IT-Systemen
  - **Schutz vor „Phishing“** und Schadprogrammen
- Weitere Standards sind:
  - Einsatz von **Firewalls**
  - Regelungen für die Netzwerk-Administration
- Die entsprechenden Regelungen können im Zusammenhang mit einem **QM-System** etabliert werden.

2 Anwendung von Passwörtern

- Es ist bekannt, dass schlecht gewählte Passwörter, wie beispielsweise 123456, viel zu unsicher und leicht zu „hacken“ sind.
- Auch ein und dasselbe Passwort für viele verschiedene Programme oder Zugänge zu nehmen, ist ebenfalls sehr riskant.
- Namen, Geburtsdaten oder dergleichen sind nicht als Passwörter geeignet.
- Das vollständige Passwort sollte möglichst nicht in Wörterbüchern vorkommen, da Hacker-Systeme alle gebräuchlichen Wörter in Sekundenbruchteilen „knacken“ können.
- Ein gutes Passwort sollte mindestens acht Zeichen lang sein und Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben enthalten.
- Passwörter sollten nicht offen im System gespeichert werden und natürlich auch nicht auf Zetteln (Post-it) aufgeschrieben werden.
- Ein Passwort sollte nur dann geändert werden, wenn Verdacht auf einen Missbrauch besteht.
- Weitere Informationen erhält man über das **Bundesamt für Sicherheit in der Informationstechnik** (www.bsi.org) unter dem Stichwort „Passwort“.

3 Einsatz von Firewalls + Virenschutz

- In der IT-Sicherheit spielt eine Firewall („Feuerwand“/Brandschutzwand) eine wichtige Schutz-Rolle.
- Die Firewall ist ein digitaler „Türsteher“, der ankommende und abgehende Datenpakete im Netzwerk kontrolliert und regelt.
- Die Firewall ist ein Baustein des IT-Sicherheitskonzepts. Diese muss ständig aktualisiert werden.
- Die Koordination der Firewall wird von den IT-Verantwortlichen übernommen.
  Sie benötigen die Kooperation aller Nutzenden, z.B. bei der Meldung von Vorkommnissen.
- Zusätzlich zur Firewall wird ein „**Virenschutzprogramm**“ von den IT-Verantwortlichen eingesetzt.
- Es kann entweder ein Virenschutz über das Betriebssystem (z.B. MS Windows) oder ein externer Virenschutz eingesetzt werden.
- **Meldungen am Bildschirm** sind aufmerksam zu lesen, Hinweise sind zu beachten und bei Wichtigkeit (zeitnah) weiterzugeben.
- Es ist wichtig, dass alle Mitarbeitenden wissen, an wen relevante **Informationen zu melden** sind und auch dass klar ist, wem man Fragen stellen kann.
- Mehr Informationen zur Firewall und Virenschutz erhält man vom **Bundesamt für Sicherheit in der Informationstechnik** (**BSI**). Im Internet erreicht man das Bundesamt über www.bsi-fuer-buerger.de.

4 Prävention Phishing Angriffe

- Als Phishing bezeichnet man den Eingang betrügerischer E-Mails, die zu Handlungen auffordern, die von Kriminellen zu Schädigungen genutzt werden.
- Wichtig ist, dass diese Phishing-Mails erkannt und sofort neutralisiert werden.
- Am besten erkennt man Phishing an gefälschten Absendenden-Adressen.
- Zuerst ist die E-Mail-Adresse der absendenden Person durch **Vergleich mit bekannten Adressen zu prüfen**.
- Die wichtigsten Fragen: Kann die absendende Person den Versand der Mail **telefonisch bestätigen?**
- Werden vertrauliche Daten abgefragt oder fordert die E-Mail zur Eingabe **persönlicher Informationen?**
- Werden Geheimnummern oder Passwörter abgefragt?
- Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf?
- Enthält die E-Mail Verlinkungen, die auf **andere Webseiten** verweisen?
- Welche Ziel-URL wird bei einem Mouseover angezeigt?
- Ist die Anrede unpersönlich formuliert oder enthält der Text Rechtschreib- oder Zeichenfehler?
- Das Motto für mehr Cybersicherheit: **Besser einmal zu viel prüfen** und richtig reagieren als unkonzentriert einfach „klicken“. Aufmerksamkeit ist Professionalität.

5 Private Nutzung Internet/eigene Geräte

- Die Nutzung von Smartphones und Tablets erfordert besondere Sicherheitsmaßnahmen.
- Es müssen immer aktuelle Schutzprogramme vor „**Phishing**“ und Schadprogrammen im Browser genutzt werden.
- SIM-Karten sollten grundsätzlich durch eine **PIN** geschützt werden.
- Die **Super-PIN/PUK** sind grundsätzlich nur durch Verantwortliche anzuwenden.
- Besonders auf mobilen Endgeräten sollten die strengsten & sichersten Einstellungen gewählt werden.
- Alle mobilen Geräte sollten mit einem komplexen Gerätesperrcode geschützt werden.
- Damit Schwachstellen vermieden werden, müssen **Updates** des Betriebssystems und der eingesetzten Apps **zeitnah** installiert werden.
- Es ist sinnvoll, einen festen Turnus (z.B. monatlich) festzulegen, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.
- Zugriffe von Apps auf Daten und Schnittstellen der mobilen Geräte sollten in den **Einstellungen restriktiv auf das Notwendigste** eingeschränkt werden.

6 Zutritts-, Zugangs- und Zugriffsschutz

- Die technischen Maßnahmen zur IT-Sicherheit sind Teil eines einrichtungsinternen QM.
- Alle wichtigen Räumlichkeiten sind durch **Sicherheitsschlösser, Alarmsicherung, Videoüberwachung** und andere Sicherungen zu schützen.
- Die Datensicherungsaufbewahrung ist z.B. durch geeignete **Tresore** zu planen oder über **externe Back-Ups** zu realisieren.
- Wichtiger als die technischen Maßnahmen sind die organisatorischen Umsetzungen des Zutrittsschutzes.
- Zu den organisatorischen Maßnahmen gehören **Schulungen**, verständliche Verfahrensanweisungen, Regelungen für Servicepersonal und ein Protokollbuch für IT-Serviceeinsätze.
- Die wichtigsten Regelungen zur IT-Sicherheit sind **Prozessbeschreibungen** zur Datensicherungserstellung, -aufbewahrung und/oder der externen Archivierung.
- Zum Standard gehören Regelungen zum Gebäudezugang mit einem allgemeinen **Schlüsselmanagement**, inklusive Schlüsselverlust-Regelungen.
- Die Ergebnisse der Evaluierung zum Zutrittsschutz sind in Protokollen für den **Jahres-Sicherheitsbericht** zu dokumentieren.

7 Kommunikation im Team

- Mehr als 70% der ungeplanten Vorfälle in der Informationssicherheit sind auf den **„Faktor Mensch“** zurückzuführen.
- Im Informationssicherheitsmanagement spielt deshalb die **Orientierung, Aufklärung und Schulung** des gesamten Teams eine zentrale Rolle.
- Am Anfang steht die Orientierung über die Regulatorik wie **Gesetze, Verordnungen, Richtlinien etc.**
- Dies kann z.B. über **Merkblätter** oder kurze digitale **Storyboards** erfolgen.
- Außerdem können Aufklärungen zu Cyberschutz und Informationssicherheit in die **Standard-Schulungen** der Mitarbeitenden einbezogen werden.
- In **Teambesprechungen** können die Wissensbereiche Informationssicherheit und Datenschutz in der Einrichtung als regelmäßige Besprechungspunkte aufgenommen werden.
- Bei aktuellen Risiken oder bei bereits eingetretenen Störfällen ist die Unterrichtung des Teams je nach Infrastruktur zu organisieren: z.B. über **Sofort-Meldungen** auf das Mobiltelefon oder per Aushang.

8 IT-Notfallmanagement

- Wichtig für das Verhalten bei IT-Notfällen: **Ruhe bewahren** & IT-Notfall melden:
  Besser einmal mehr als einmal zu wenig anrufen!
- Standard ist: **Meldungen an IT-Sicherheitsbeauftragte** und IT-Sicherheitskoordinierende, Einrichtungsleitung sowie bei kritischen Störungen an die IT-Dienstleistenden.
- Nach der Meldung des Notfalls sind unverzüglich die erforderlichen **Sofortmaßnahmen** zu ergreifen.
- Zielsetzung des Notfallmanagements ist es, zu verhindern, dass die Unterbrechung oder Störung von wichtigen Prozessen der Organisation betroffen sind.
- Daher sollten möglichst rasch die vorbereiteten **Kontinuitätspläne** aktiviert werden:
  - Mitarbeitende ausführlich informieren, Aktionsplan einbeziehen, **Reservesystem aktivieren**, Rekonstruktion der Datensicherung mit IT-Verantwortlichen vorbereiten.
  - Mögliche **Terminverschiebung organisieren** und betroffene Personen informieren.
  - Sobald alle Voraussetzungen für einen funktionsfähigen Normalbetrieb erfüllt sind, kann er wieder mit Protokoll aufgenommen werden.
  - **Aus Krisen kann gelernt werden:** Wie kam es dazu? Welche Auswirkungen hat es? Festgestellte Mängel und **Verbesserungsmöglichkeiten** werden offen kommuniziert und zeitnah umgesetzt.

Anlage zum Mitarbeitervertrag mit *(Name)* **vom *(Datum)***

Generelle Orientierung

Die medizinische Versorgung in Arztpraxen und Kliniken stellt besondere verpflichtende Anforderungen an alle Mitarbeiter. Die folgende Übersicht stellt die wichtigsten gesetzlichen Regelungen, die zu befolgen sind, global zusammen:

Patientensicherheit, Mitarbeitersicherheit (z.B. IFSG, MPG etc.)

Die Sicherheit aller Personen in der Praxis hat höchste Priorität. Dazu gelten z.B. die Anforderungen nach dem Infektionsschutz Gesetz (IFSG), dem Medizinprodukte Gesetz (MPG) und die Vorschriften der Berufsgenossenschaften (BGV).

Datenschutz und ärztliche Schweigepflicht (z.B. DSGVO, BDSG)

Die ärztliche Schweigepflicht ist ein hohes ethisches Gut in der medizinischen Versorgung. Die Schweigepflicht und die zusätzlichen Anforderungen der Datenschutz-Gesetzgebung (Datenschutz-Grundverordnung/DSGVO und Bundesdatenschutz Gesetz/BDSG) gelten verpflichtend:

IT-Sicherheit und Cyberschutz (z.B. DVG und IT-Sicherheitsrichtlinie nach § 75b)

Im Rahmen des „Digitale-Versorgung-Gesetz“ (DVG) werden technische und besonders organisatorische Maßnahmen zur Gewährleistung der IT-Sicherheit dokumentiert.
Diese sind von allen Personen in der Praxis einzuhalten.

Notfallmanagement (z.B. BG Vorschriften)

In ärztlichen Versorgungseinrichtungen ist das Notfallmanagement von besonderer Bedeutung für die Sicherheit von Patienten und den Personen (Ärzte/und Mitarbeiter) in der Versorgung.

Weiterbildungsverpflichtung

Die Mitarbeitenden haben Zugang zu den wesentlichen und relevanten Wissensinhalten durch analoge und durch digitale Schulungsangebote. Dazu steht ein gedruckter Leitfaden (analoge Schulung) und ein Trainingsprogramm über Smartphone Nutzung zur Verfügung.

Die Mitarbeitenden sind verpflichtet, diese Schulungs- und Weiterbildungsangebote regelmäßig zu nutzen und dies zu dokumentieren.

Datum/Unterschrift

Zusatzvereinbarung zum IT-Service- und Lizenzvertrag vom (Datum)

Für medizinische Versorgungseinrichtungen, wie ärztliche und zahnärztliche Praxen sowie kleine und mittlere Kliniken, gilt ab 1. April die IT-Sicherheitsrichtlinie nach § 75b SGB V. Diese macht besondere technische und organisatorische Maßnahmen für Ärzt*innen/Zahnärzt*innen verpflichtend.

Zu den Maßnahmen und Anforderungen gehören insbesondere nach der aktuell beschlossenen Fassung:

- Passwort-Management nach dem Stand der Technik
- Schutz und Protokollierung des Zugriffs auf Arbeitsplatzrechner
- Einsatz von Virenschutz Programmen und IT-Firewalls
- Datensicherung, Archivierung und Datenrekonstruktion (intern und extern)
- Austausch, Entsorgung und Reparatur von IT-Systemen und Datenträgern
- Rollen- und Rechtevergabe inkl. Administrationsmanagement
- Jährliche Überprüfung und Anpassung der Sicherheitsmaßnahmen

Hiermit wird bestätigt, dass mit dem bestehenden o.g. Vertragsverhältnis die o.g. Funktionen und Maßnahmen der IT-Sicherheitsrichtlinie erfüllt werden.

Soweit die konkret verpflichtenden Anforderungen nicht zu den vereinbarten Leistungen gehören, werden sie im Folgenden aufgelistet:

Liste der nicht durch das Vertragsverhältnis geregelten IT-Sicherheitsfunktionen und -Maßnahmen:

- 1
- 2
- 3
- 4

(Evtl. genauere Spezifikation in einem mitgeltenden Dokument der Vertragspartner)

Mitgeltende Dokumente:

- IT-Sicherheitsrichtlinie nach § 75b SGB V (verpflichtend)
- Empfehlungen der Bundesärztekammer und KBV/KZBV zur IT-Sicherheit und Datenschutz (informativ spezifizierend)
- Technische Anlage zu den Empfehlungen der Bundesärztekammer und der KBV/KZBV (informativ spezifizierend)

Datum/Unterschrift | Datum/Unterschrift

Auftraggeber | Auftragnehmer

Leitlinie zur Informationssicherheit

Im Interesse von Patienten und Mitarbeitern der Praxis/Klinik müssen Daten und IT-Prozesse durchgängig und wirksam vor Missbrauch und dem Verlust der Integrität, Vertraulichkeit und Verfügbarkeit bewahrt werden.

Informationsverarbeitung und -sicherheit spielt damit eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt.
Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können.
Auch in Teilbereichen muss unsere Praxis/Klinik immer funktionsfähig bleiben.

Die Informationssicherheit hat für alle Ärzte durch die rechtliche Verankerung der Schweigepflicht in Gesetzen und Verordnungen eine besonders hohe Priorität.
Deshalb haben aktuelle Schulungen aller Personen in der Patientenversorgung einen hohen Stellenwert.

Übergeordnete Ziele

Angemessene Informationssicherheit ist integraler Bestandteil der Praxispolitik und leistet einen unverzichtbaren Beitrag zum Erfolg der Praxis. Informationssicherheit ist an den Geschäftszielen ausgerichtet und wird von der Praxisleitung verantwortet. Unsere Daten und unsere IT-Systeme in allen technikabhängigen und medizinischen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandzeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität).

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden. Alle Mitarbeiter der Praxis/ Klinik halten die einschlägigen Gesetze und Verordnungen (z. B. Digitale-Versorgung-Gesetz (DVG), IT-Sicherheitsrichtlinie der KBV nach § 75b SGB V, Datenschutz-Grundverordnung, Strafgesetzbuch und Vorschriften zur beruflichen Schweigepflicht) und vertraglichen Regelungen ein. Dazu gehören auch die Verpflichtungen aus Versicherungs-verträgen (z.B. Obliegenheiten aus Cyber-Versicherungen). Dazu werden auch die Zusatzvereinbarungen zu Arbeitsverträgen rechtskonform angepasst.

Negative finanzielle und immaterielle Folgen für die Praxis sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeiter und die Praxisleitung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften. Die Praxis-/Klinikleitung und alle Mitarbeiter der Praxis/Klinik sind zur Einhaltung der IT-Sicherheitsmaßnahmen verpflichtet. Externe Vertragspartner sind in rechtskonformen Verträgen ebenso zu verpflichten.

Die Leitlinie wird bei Bedarf den technischen, organisatorischen und rechtlichen Anforderungen angepasst.

Verfahrensanweisung (VA)
„Schulung zur IT-Sicherheit in ärztlichen Praxen“ (Beispiel)

Übersicht

Diese VA dient der internen Unterstützung der Informationssicherheitskoordinierenden (ISK) in medizinischen Einrichtungen wie Praxen, Kliniken, MVZ, speziell bei der rechtskonformen Umsetzung der Cyberschutz-, Informationssicherheits- und Datenschutz-Rahmenbedingungen.

Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zur Informationssicherheit in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und der Sicherstellung der Vollständigkeit und Qualität.

Anwendungsbereich

Diese Anweisung gilt für die Durchführung von Schulungen zur konformen Anwendung der IT-Sicherheitsrichtlinie nach § 75b SGB V und der Datenschutz-Grundverordnung (DSGVO).
Die Schulungen beziehen sich auf Anwendungen der IT-Sicherheit im Bereich der Verwaltung und der Informationstechnologie (z.B. elektronische Patientenakte (ePA)).
Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten erfasst verarbeitet, übertragen und gespeichert werden.

Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung / Mitglieder der Leitung (ärztlich und organisatorisch)
- Informationssicherheitsbeauftragte (ISB)
- Externe Dienstleistende, soweit rechtlich geregelt (externe IT-Sicherheitsberatende)

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

Prozesse

Die Schulungen können nach 4 Alternativen durchgeführt werden:

- Schulung im Selbststudium
- Schulung in Team Meetings
- Videoschulungen
- Schulung in Webinaren durch externe Dienstleistende

Die Schulungen bestehen aus unterschiedlichen Schulungsmodulen, **MC-SMARTLEARN**:

- Erklärvideos zu Informationssicherheit und Datenschutz
- Checklisten zur KBV IT-Sicherheitsrichtlinie nach § 75b SGB V
- „Multiple Choice“ Fragen zur Überprüfung des Wissensstatus (Wissenstests)

Schulung im Selbststudium (Schulungsvideos)

Unabhängig von Terminen können Teammitglieder zeitgünstig die Schulungsfragen mit den Antworten durcharbeiten. Dabei kann man pro Frage und Antwort ca. 3 Minuten planen (bei 20 Fragen und Antworten ca. eine Stunde). Es empfiehlt sich, ein Protokoll anzufertigen, das als Nachweisdokument für die Praxis-/Klinikleitung dienen kann.
Auf dem Protokoll werden vermerkt:

- Name des Teammitglieds
- Rolle/Funktion in der Praxis/Klinik
- Inhalt der Schulung (Hauptthema und Stufe)
- Erst- oder Folgeschulung zum Thema
- Datum des Selbststudiums
- Uhrzeit von - bis der Selbstschulung
- Offene Fragen für DSB oder Praxisleitung
- Antworten zu den Fragen

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.

Schulung in Team Meetings

Eine effektive Schulung der Mitarbeitenden kann integriert in Team Meetings durchgeführt werden.
Die Koordinierenden können IT-Sicherheitsbeauftragte, Datenschutzbeauftragte oder externe Dienstleistende (z.B. **MCSS AG**) sein. Die Schulungseinheiten richten sich nach dem Status der Datenschutz-Ausbildung.

Eine Einheit soll maximal 90 Minuten dauern (ca. 20-30 Fragen und Antworten).

Als Nachweisdokument fertigt die Schulungsleitung ein Protokoll mit folgenden Angaben an:

- Titel und Thema der Schulung
- Referent*in / Schulungs-Koordinator*in
- Ort der Schulung
- Datum der Schulung
- Uhrzeit von - bis
- Teammitglieder
  - Namen
  - Rollen/Funktionen
  - Erstschulung/Folgeschulung

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.

Schulung in Webinaren

Webinare sind Online-Schulungen, die von verschiedenen Organisationen und kommerziellen Anbieter*innen veranstaltet werden. Es wird von den Verantwortlichen geprüft, welche Webinar-Angebote eine Rechtskonformität gewährleisten.
Im Regelfall bieten Anbieter*innen von Schulungs-Webinaren auch Teilnahmenachweise. Ist dies nicht der Fall, dokumentieren die Mitarbeitenden ihre Teilnahme intern mit folgenden Angaben:

Name des Teammitglieds:

- Rolle / Funktion in der Praxis/Klinik
- Inhalt der Schulung (Hauptthema und Stufe)
- Veranstalter*in des Webinars
- Erst- oder Folgeschulung zum Thema
- Datum des Webinars
- Uhrzeit von - bis des Webinars

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.
Hinweis: Webinare können „Live“ oder auch als „Konserven“ (Videoschulungen) angeboten werden.

Dokumentation der Schulungen

Die Schulungen werden sowohl durch die Mitarbeitenden wie auch durch die Verwaltung dokumentiert.
Die Mitarbeitenden sammeln Kopien ihrer Schulungen in ihrem Qualifikations-Ordner für Audits und für Nachweise bei Wechsel des Arbeitsplatzes.

Mitgeltende Dokumente:

- Curriculum ISMS/DSMS zur Umsetzung von IT-Sicherheit und Datenschutz
- IT-Sicherheitsrichtlinie nach § 75b SGB V
- Bundesdatenschutzgesetz (BDSG) insbesondere § 64
- Datenschutz-Grundverordnung (DSGVO) insbesondere Art. 32
- § 136 SGB V QM Richtlinie des GBA (GBA-RI)
- Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz, Datenverarbeitung ärztliche Praxis BÄK & KBV
- Technische Anlage zu den BÄK/KBV Empfehlungen
- **MC-SMARTLEARN** Dokumentation für Mitarbeitende

Interne Regelung

Beispiel nach KBV QM-System „Qualität und Entwicklung in ärztlichen Praxen“

Notfallprozesse für das Management nach IT-Sicherheits-Richtlinie § 75b

Informationen zu QEP

QEP steht für Qualität und Entwicklung in Praxen. Es ist ein von der Kassenärztlichen Bundesvereinigung entwickeltes Qualitätsmanagementsystem. Es erfüllt die Anforderungen an Qualitätsmanagement (QM) nach § 135 ff. des Sozialgesetzbuchs V (SGB V). Nach Angaben der KBV setzen etwa 35% der Kassenärzt*innen ein QM nach der QEP Norm ein.

QEP gilt als Alternative zu QM-Systemen nach ISO 9001:2015 (siehe auch Beispiel der Verfahrensanweisung (VA) nach ISO Norm).

Ziel der Regelung

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Notfallmanagement in der IT-Sicherheit in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung des Prozesses, der geregelt wird und die Gewährleistung der Vollständigkeit sowie der geplanten Ergebnisqualität.

Die Informationstechnologie ist heute wesentlicher Bestandteil einer Praxis und Klinik. Es werden wesentliche sicherheitsrelevante Informationen zu den Patientenfällen gespeichert. Fällt das IT-Netzwerk aus, so können beispielsweise die Notfalldaten von Patient*innen fehlen und zu falschen Diagnose- und Therapieentscheidungen führen. Ziel dieser VA ist die Regelung für Notfälle in der IT-Sicherheit.

Inhalt der Regelung

Zur Gewährleistung der Patientensicherheit muss ein professionelles Notfallmanagement in jeder medizinischen Versorgungseinrichtung etabliert sein. Die Verpflichtungen für die Notfallversorgung sind in verschiedenen Gesetzen, Verordnungen und Richtlinien dokumentiert. Dazu gehört das Infektionsschutzgesetz, die Medizinprodukte-Regelungen, Hygienemanagement und auch Richtlinien für die IT-Sicherheit. Fällt das IT-Netzwerk aus, so stehen bei Einsatz der elektronischen Patientenakte auch keine umfassenden Notfallinformationen zu den einzelnen Patient*innen zur Verfügung.

Zum IT-Notfallmanagement gehört im ersten Schritt die Definition und Beschreibung eines IT-Notfalls.
Diese Festlegungen hängen von der einzelnen Praxis und dem Computerisierungsgrad ab.
So kann definiert werden, dass ein Notfall dann vorliegt, wenn für die Patientenversorgung wichtige Arbeitsplätze für einen längeren Zeitraum (z.B. länger als 15 Minuten) ausfallen. Für diesen Fall müssen Notfallpläne vorliegen, z.B. für unterbrochene oder abgebrochene Untersuchungen oder Therapien.

Konkrete Fragestellung: Wurde überprüft, ob es sich um einen tatsächlichen IT-Notfall handelt, erfolgt die Meldung an den oder die IT-Verantwortlichen? Dies erfolgt im Regelfall über ein Mobiltelefon, das immer unabhängig vom Computer- und Stromnetzwerk funktionieren muss. Dazu müssen die Notfallnummern wie auch die Telefonnummern der Feuerwehr, des Notarztes und der Polizei bekannt und deutlich sichtbar ausgehängt sein.

Für die praktische Nothilfe muss ein Aushang vorhanden sein, der den/die IT-Notfallbeauftragte*n und seine/ihre Telefonnummer enthält. Weiterhin müssen Verfahrensanweisungen oder interne Regelungen im Rahmen des Qualitätsmanagements vorliegen.

Danach sind die verschiedenen IT-Notfälle zu klassifizieren:

- **Ausfall eines einzelnen IT-Arbeitsplatzes**
- **Ausfall aller IT-Arbeitsplätze einer Abteilung**
- **Ausfall des gesamten IT-Netzwerks**

Im Rahmen des Qualitätsmanagements gibt es Checklisten und Verfahrensanweisungen / interne Regelungen für die möglichen Schweregrade eines IT-Notfalls.

Referenzen:

- Richtlinie nach § 75b SGB V
  - Datei und Freigabeberechtigungen
  - „Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.“
- BSI Grundschutz

Mitgeltende Dokumente:

- IT-Sicherheitsrichtlinie nach § 75b SGB V
- Empfehlungen der Bundesärztekammer und der KBV zum Datenschutz und zur Datenverarbeitung in der ärztlichen Praxis
- Technische Anlage zu den Empfehlungen der BÄK und der KBV
- Verträge mit externen IT-Partnern (z.B. DLO = Dienstleistende vor Ort)
- Interne Regelung „Notfallmanagement“

Name des Dokumentes: „Notfallmanagement für das IT-Management“

Verantwortlich für das Dokument:

- Leitung/Mitglieder der Leitung (ärztlich und organisatorisch)
- Informationssicherheitsbeauftragte (ISB)
- Datenschutzbeauftragte (DSB) und Datenschutzkoordinierende (DSK)
- Externe Dienstleistende, soweit rechtlich geregelt (Externe Datenschutzbeauftragte [DSB])

Aktualisierung: Bei Bedarf

Glossar für Informationssicherheit und Datenschutz (MC-PRAXIS 75b)

§ 75b SGB V
Gesetzliche Vorschrift zur Einführung von technischen und organisatorischen Maßnahmen in ärztlichen und zahnärztlichen Praxen (in Kraft seit dem 1.1.2020)

Anti-Virus SW
Spezial-Software, die Rechner vor dem Befall von Computer-Viren schützt (Forderung der Datensicherheit)

Art. 32 DSGVO
Gesetzliche Verpflichtung für Datensicherheit nach der Datenschutz-Grundverordnung

BSI
Bundesamt für Sicherheit in der Informationstechnik, zuständige Behörde für Cyberschutz und IT-Sicherheit in Deutschland

Cloudbasierte Systeme
Der Vorteil von cloudbasierten Computer-Systemen besteht vor allem darin, dass sie standardisierte Leistungen schneller und zu einem günstigeren Preis anbieten als die Anwendenden selbst dies mit ihrer internen IT können. Cloudbasierte Anwendungen können durch alle mobilen und stationären Endgeräte über das Internet abgerufen werden.

Curriculum
Unter einem Curriculum (lateinisch) versteht man einen Lehrplan, in dem die Lerninhalte und Lernziele über einen längeren Zeitraum definiert sind (beispielsweise für die Einführung von QM- und Datenschutz-managementsystemen).

Cyber-Sicherheit
Die Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikations-technik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationstechnik mit ein.

Cyber-Versicherung
Eine Cyber-Versicherung ist eine fakultative Zusatzversicherung für Organisationen, die Schäden im Zusammenhang mit Hacker-Angriffen oder sonstigen Akten von Cyberkriminalität absichert.

Datenschutz
Unter Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch, oft im Zusammenhang auch mit dem Schutz der Privatsphäre. Zweck und Ziel des Datenschutzes ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jede Person soll selbst bestimmen können, wem sie wann welche ihrer Daten und zu welchem Zweck zugänglich macht.

Datenschutzbeauftragte (DSB)
Ein Datenschutzbeauftragter/eine Datenschutzbeauftragte (DSB) wirkt in einer Organisation, wie einer Praxis oder Klinik, auf die Einhaltung des Datenschutzes hin. Die Person kann Mitarbeitende*r dieser Organisation sein oder als externe*r Datenschutzbeauftragte*r bestellt werden.
Der oder die Datenschutzbeauftragte muss die notwendige Fachkunde für die Ausübung besitzen und darf nicht in einen Konflikt oder in die Gefahr der Selbstkontrolle geraten. Die Berufung eines/einer DSB wird beispielsweise in der DSGVO geregelt.

Datenschutzmanagementsystem (DSMS)
Das Managementsystem organisiert den Datenschutz in der Organisationseinheit, insbesondere gemäß DSGVO und BDSG-neu. Es orientiert sich im Regelfall an der Norm ISO 9001:2015.

Datensicherung (englisch „Backup“):
Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbe-ständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

DIN EN ISO 9001
Im Qualitätsmanagement repräsentiert diese Norm ein Qualitätsmanagementsystem als Grundlage auch zur mög-lichen freiwilligen Zertifizierung. Über die reine Qualitätssicherung hinaus werden unter ISO 9001 umfangreiche Maß-nahmen, die alle Abläufe innerhalb von Praxis und Klinik eindeutig festlegen, definiert, dokumentiert und kontrolliert.

DSGVO
Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch Datenverarbeitende, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Firewall
Eine Firewall (oft auch als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze gegen Angriffe zu sichern.

ISB
Informationssicherheitsbeauftragte*r, Verantwortliche*r für Informationssicherheit und Cyberschutz in Organisationen

Informationssicherheitsmanagementsystem (ISMS)
Das ISMS ist die Sammlung von Dokumenten zur Umsetzung der Informationssicherheit in der Organisation. Es basiert im Regelfall auf der Norm ISO 27001.

Leitlinien
Unter Leitlinien versteht man Empfehlungen, die Handlungsvorgaben enthalten. Sie sollten dann übernommen werden, wenn keine qualifizierten Gründe dagegensprechen.

MCSS AG
Anbietende von cloudbasierten Assistenz-Systemen, speziell für Cyber-Versicherungen: www.mcss-ag.de

Mobiler Datenträger
Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z.B. Speichersticks und -karten sowie externe Festplatten.

Notbetrieb
Auf ein Minimum reduzierte Funktionstüchtigkeit, mit der ein Prozess aufrechterhalten werden kann. Grundlage dafür ist ein internes Notfall-Management.

Passwort
Mit der Eingabe eines Passwortes weist der Benutzer/die Benutzerin nach, dass er/sie zu dem geschlossenen System eine Zugangsberechtigung hat. Dies kann zum Beispiel die Anmeldung an einem Client oder die Eingabe der Geheimzahl am Geldautomaten sein. „Passwort“ stellt dabei einen Oberbegriff dar und beinhaltet Passwörter, PINs oder auch Passphrasen (Folge von aneinandergereihten Wörtern).

Qualitätsmanagement (QM)
Unter QM versteht man alle Maßnahmen zur Verbesserung und Erhaltung der Qualität als legitime Erwartung der Patient*innen und der Volkswirtschaft insgesamt. Qualitätsmanagement umfasst die Dokumentation, die Analyse, das Controlling und auch alle Maßnahmen zur Qualitätssicherung.

Qualitätsmanagementsystem (QMS)
Das QMS ist ein Kompendium zur Umsetzung von Qualitätsmanagement in der Organisation. Im Bereich der Medizin wird ein QMS nach SGB V (Sozialgesetzbuch) GBA (Gemeinsamer Bundesausschuss) QM RL (Richtlinie) für Praxen und Kliniken vorausgesetzt. Es existieren parallel verschiedene System wie z.B. QEP (Qualität und Entwicklung in Praxen) der KBV oder nach der Norm ISO 9001:2015.

Ransomware
Ransomware hat innerhalb eines Bereiches der Cyberkriminalität gefährlich an Bedeutung gewonnen. Mit ihr verschlüsselt ein Angreifer die Daten der Opfer und verlangt ein Lösegeld für den privaten Schlüssel. Ransomware wird unter anderem via E-Mail-Anhänge, infizierte Programme und kompromittierte Websites verteilt. Security-Experten bezeichnen diese Form der Malware je nach Verbreitungsart auch als Kryptovirus, Kryptotrojaner oder Kryptowurm.

Risiko
Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit bzw. Unwägbarkeit.

Spamfilter
Software, die Computer vor unerwünschten Informationen (Spam) schützen, werden als Spamfilter bezeichnet.

TI
Telematikinfrastruktur zur Umsetzung digitaler Anwendungen im Gesundheitswesen und in der Sozialwirtschaft

TOM
Technische und organisatorische Maßnahmen nach DSGVO Artikel 32 für Datenschutz und Informationssicherheit

Virus
In der Computersprache eine Schadsoftware, die IT-Systeme stören oder zerstören kann.

Webinar
Schulungsangebote im Internet, die auch für die Bereiche Datenschutz und Informationssicherheit in ärztlichen Praxen, Kliniken und Krankenhäusern angeboten werden. Sie erfüllen die Anforderung nach ISO Standards (z.B. ISO 9001 etc.).

Wissenstests
Das Wissen aller Mitarbeitenden zur Informationssicherheit und Datenschutz ist die Grundlage einer rechtskonformen Organisation. Um die Kenntnisse eines Teams zu evaluieren, können digitale Wissenstests genutzt werden.

Registrierung/Onboarding

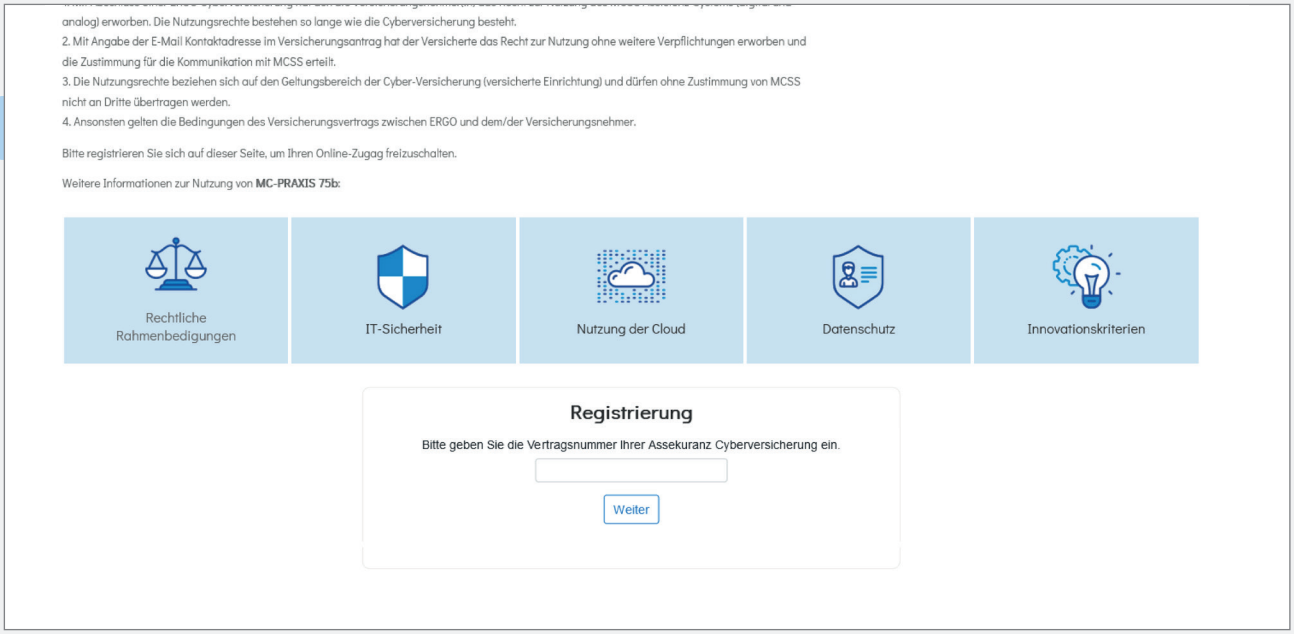
Beschreibung des Prozesses für den Administratorzugang und den Zugang zu MC-SMARTLEARN

Der Zugang zum digitalen Assistenz-System für Cyber-Versicherte ist durch die Versicherungsprämie lizensiert.
MCSS stellt den sicheren Zugangs-Code den Versicherten unter der im Versicherungsvertrag angegebene E-Mail-Adresse zur Verfügung.

Achtung: Wenn der Code bislang nicht eingegangen ist, bitte auch im SPAM Ordner des Postfachs nachschauen.

Ansonsten Nachfrage an: anwenderservice@mcss-ag.de mit Angabe von Cyber-Versicherungs-Nr. und Adressdaten.

1



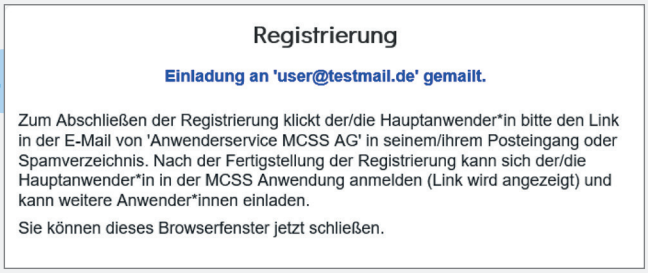
2

In dem Feld „**Registrierung**“ wird die Vertragsnummer der Cyberpolice eingegeben und anschließend mit einem Klick auf das Feld „**Weiter**“ bestätigt.

3

Nun kann in dem Feld „Registrierung“ die E-Mailadresse des Hauptverantwortlichen (Administratorzugang, der für das Projekt Verantwortliche) eingegeben werden. Anschließend wird diese Eingabe mit dem Feld „**Akzeptieren und weiter**“ bestätigt.

4

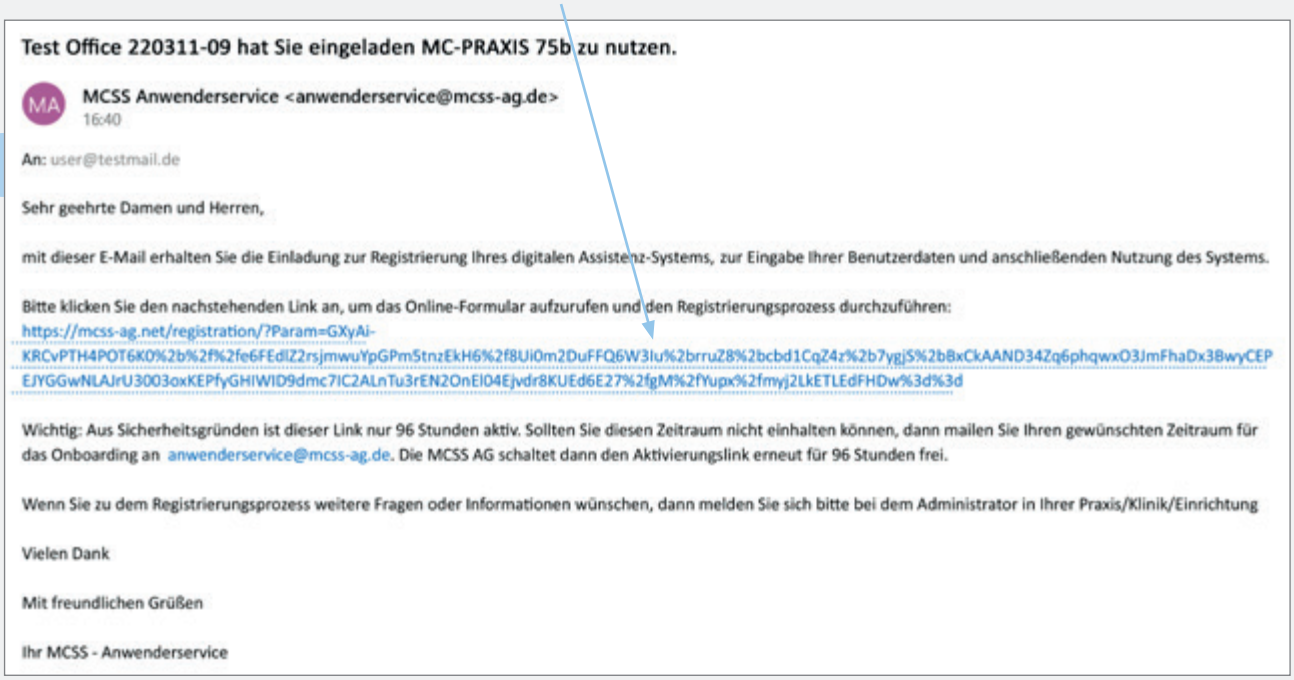


Es folgt die Bestätigung, dass eine Einladung zur finalen Registrierung an die eingegebene E-Mail-Adresse versendet worden ist.
Diese E-Mail ist im Mailaccount abrufbar und wurde von anwenderservice@mcss-ag.de versendet.

Bitte diese Adresse freischalten, damit wichtige Informationen nicht im Spamfilter verloren gehen.

In der erhaltenen E-Mail ist der entsprechende Link anzuklicken, um das Onlineregistrierungsformular aufzurufen.

5



Test Office 220311-09 hat Sie eingeladen MC-PRAXIS 75b zu nutzen.

MA **MCSS Anwenderservice <anwenderservice@mcss-ag.de>**
16:40

An: user@testmail.de

Sehr geehrte Damen und Herren,

mit dieser E-Mail erhalten Sie die Einladung zur Registrierung Ihres digitalen Assistenz-Systems, zur Eingabe Ihrer Benutzerdaten und anschließenden Nutzung des Systems.

Bitte klicken Sie den nachstehenden Link an, um das Online-Formular aufzurufen und den Registrierungsprozess durchzuführen:
https://mcss-ag.net/registration/?Param=GXyAi-KRCvPTH4POT6K0%2b%2f%2fe6FEdlZ2rsjmwuYpGPm5tnzEkH6%2f8Ui0m2DuFFQ6W3Iu%2brruZ8%2bcbd1CqZ4z%2b7ygjS%2bBxCkAAND34Zq6phqwxO3JmFhaDx3BwyCEPEJYGGwNLAJrU3003oxKEPfyGHIWID9dmc7IC2ALnTu3rEN2OnElO4Ejvdr8KUEd6E27%2fgM%2fYupx%2fmyj2LkETLEdFHDw%3d%3d

Wichtig: Aus Sicherheitsgründen ist dieser Link nur 96 Stunden aktiv. Sollten Sie diesen Zeitraum nicht einhalten können, dann mailen Sie Ihren gewünschten Zeitraum für das Onboarding an anwenderservice@mcss-ag.de. Die MCSS AG schaltet dann den Aktivierungslink erneut für 96 Stunden frei.

Wenn Sie zu dem Registrierungsprozess weitere Fragen oder Informationen wünschen, dann melden Sie sich bitte bei dem Administrator in Ihrer Praxis/Klinik/Einrichtung

Vielen Dank

Mit freundlichen Grüßen

Ihr MCSS - Anwenderservice

6

Bitte die Administratordaten eintragen mit Vorname, Nachname, Anzeigename und Passwort.

Danach mit dem Feld „**Weiter**“ bestätigen.

7

Der **MC-SMARTLEARN** Zugang (siehe Seite 23) wird mit Eingabe eines Loginnamens und eines Passwort eingerichtet. Anschließend die Eingabe mit „**Registrierung abschließen**“ beenden.

8

Die Registrierung ist damit erfolgreich abgeschlossen.

Jetzt kann mit dem System sofort gearbeitet oder über die Admin-Verwaltung weitere Zugänge angelegt werden.

Hierzu ist eine Anleitung im Admin-Zugang verfügbar.

Einführung MC-SMARTLEARN

Beschreibung des Prozesses für den MC-SMARTLEARN Zugang und Anwendungshinweise

MC-SMARTLEARN ist eine Schulungsplattform für alle Mitarbeitenden, die sich ortsungebunden und flexibel zu den Themen Informationssicherheit, Datenschutz und Cybersicherheit schulen möchten.
Dazu stehen Erklär- und Schulungsvideos, Wissenstests und Checklisten zur Verfügung. Nach erfolgreicher Schulung sind Nachweisdokumente abrufbar. Alle Inhalte sind für Smartphones optimiert.

So ist es möglich, die vielfältigen Inhalte überall zu nutzen, auch unterwegs im Bus, Zug, der Straßenbahn oder als Mitfahrer im Auto.

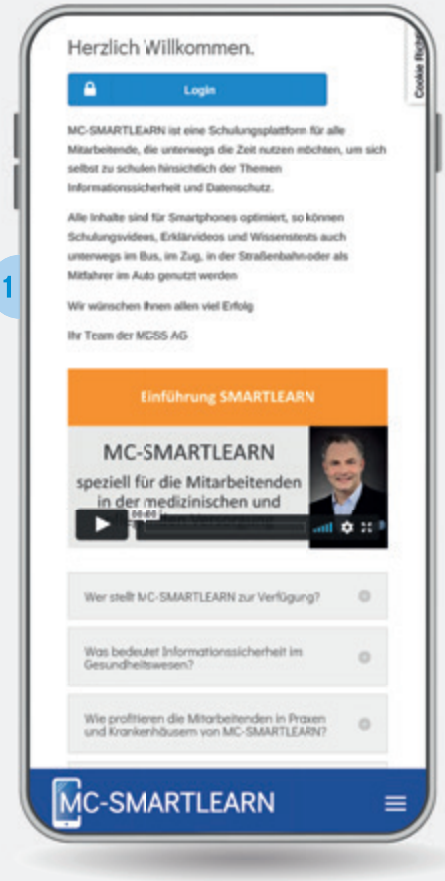
Anmelden können Sie sich unter der Webadresse mc-smartlearn.de

MC-SMARTLEARN ist für Cyber-Versicherte durch die Versicherungsprämie lizenziert.

Den für den Zugang erforderlichen Benutzernamen und das Passwort legt der Administrator (der/die Verantwortliche für das Assistenz-System) fest und stellt dies allen verantwortlichen Mitarbeitenden zur Verfügung.

Achtung: MC-SMARTLEARN ist für **SMARTPHONES** entwickelt.
Auf anderen Computern ist eine Ansicht nur mit angepasstem Bildschirmausschnitt möglich, z.B. durch Verringern der Breite des Browserfensters.

1



Nach Eingabe der Domain https://mc-smartlearn.de in einem beliebigen Browser eines Smartphones erscheint der **„Willkommens-Bildschirm“**.

Dort stehen viele Informationen und ein Erklärvideo zur Einführung zur Verfügung.

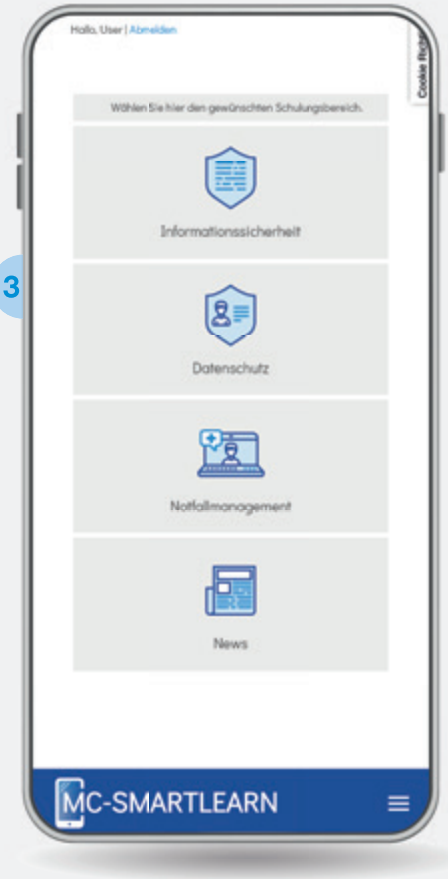
Mit einem Klick auf den Button **„Login“** geht es zur Anmelde-Maske von **MC-SMARTLEARN**.

2

In dem Anmeldebildschirm wird der Benutzername in das Feld **„Benutzername“** und das Kennwort in das Feld **„Kennwort“** eingetragen.

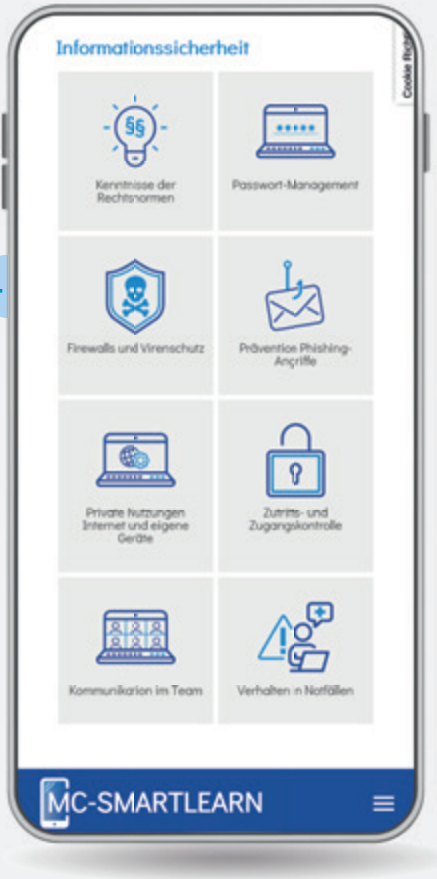
Anschließend mit dem Button **„Anmelden“** bestätigen und schon geht es los.

Tipp: Bitte auf Groß- und Kleinschreibung achten.



3

Nach der Anmeldung in **MC-SMARTLEARN** ist die Auswahl zu den Schulungsbereichen Informationssicherheit, Datenschutz und Notfallmanagement möglich, sowie der Aufruf von News aus den genannten Fachbereichen.



4

In den Schulungsbereichen gibt es unterschiedliche Schulungsblöcke, wie z.B. **„Kenntnisse der Rechtsnormen“,** die die Mitarbeitenden Schritt für Schritt abarbeiten können.

Mit einem „Klick“ auf den Schulungsbereich kann die Fortbildung beginnen.

5

In jedem Schulungsblock sind zu dem jeweiligen Thema ein **SMARTLEARN-** und ein **Erklärvideo** verfügbar, in denen die ausgesuchten Themen erklärt werden.

Zusätzlich bietet ein **Informationsblatt** weitere Inhalte an.

Mit dem **Wissenstest** prüfen Mitarbeitende, ob das jeweilige Thema inhaltlich verstanden wurde. Nach erfolgreich absolviertem Wissenstest kann ein **Schulungsnachweis** angefordert werden.

Alle Bausteine sind mit einem „Klick“ ansteuerbar.

Tipp: Zur besseren Konzentration und für unterwegs empfehlen sich Kopfhörer.