CDQM-PRAXIS Kompendium

Cyber-Sicherheit, Datenschutz & Qualitätsmanagement (ISMS-DSMS-QMS) für kleine und mittlere Arzt-, Zahnarztpraxen und Kliniken

Entwickelt nach aktuellen Rechtsnormen:

Informationssicherheit nach § 75b SGB V (VdS RL 10000)
Datenschutz nach DSGVO (VdS RL 10010)
Qualitätsmanagement nach GBA QM RL § 4

Stand 11-2022

MCSS AG
MioCloud
Solution Systems

Inhalt

Informationssicherheits-, Datenschutz- und Qualitätsmanagementsystem für kleine und mittlere Arztpraxen und Kliniken

1 Allgemeine Grundlagen

Die vorliegenden Richtlinien legen Mindestanforderungen an die Informationssicherheit, den Datenschutz und das Qualitätsmanagement fest und beschreiben ein auf kleine und mittlere Arztpraxen (KMAP) zugeschnittenes Informationssicherheits-Managementsystem (ISMS), Datenschutz-Managementsystem (DSMS) und Qualitätsmanagementsystem (QMS).

1.1 Anwendungsgrundlagen

Aus Gründen der leichteren Lesbarkeit wird in diesen Richtlinien auf eine geschlechtsspezifische Differenzierung, wie z.B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form verwendet. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten.

1.1.1 Anwendungsgrundlagen Informationssicherheit

Das für die Umsetzung der geforderten Maßnahmen erforderliche Fachwissen beruht auch auf Erfahrungen auf den Gebieten der Informationssicherheit (DVG, BSI Grundschutz) und den Grundlagen des Qualitätsmanagements.

1.1.2 Anwendungsgrundlagen Datenschutz

Das für die Umsetzung der geforderten Maßnahmen erforderliche Fachwissen beruht auch auf Erfahrungen auf den Gebieten des Datenschutzes (DSGVO/BDSG) und den Grundlagen des Qualitätsmanagements.

1.2 Anwendungs- und Geltungsbereich

Diese Richtlinien sind für KMAP, kleinere Kliniken und MVZ Organisationen anwendbar.

1.3 Gültigkeit und Anwendungsbereiche

Diese Richtlinien gelten ab dem (Datum) für die Bereiche Informationssicherheit (Cyberschutz), Datenschutz und Qualitätsmanagement.

1.4 Anleitung zur Anwendung

Das vorliegende IS-DS-QM Kompendium (Handbuch) wurde für eine langfristige und umfassende Umsetzung der Informationssicherheit, des Datenschutzes und des Qualitätsmanagements in medizinischen Versorgungseinheiten entwickelt. Es steht in einem analogen Format (gedrucktes Handbuch) und digital als cloudbasiertes System zur Verfügung.

1.4.1 Analoges Handbuch

Das analoge Handbuch wird zu Beginn des Einführungsprozesses zur Verfügung (Bestandteil des Leistungsumfangs)gestellt. Es repräsentiert den Regulierungsstand zum Zeitpunkt der Einführungsphase. Die Verantwortlichen können das analoge Handbuch parallel zum digitalen System pflegen und jeweils aktuelle Unterlagen ausdrucken und im Kompendium austauschen.
Bei Audits und Begehungen durch Behörden dient das Handbuch auch als Nachweisdokument.

1.4.2 Digitales Kompendium

Das digitale Kompendium entspricht strukturell dem analogen Handbuch (identische Gliederung). Es befindet sich in der Cloud und kann mit einem lizensierten Zugang zur Umsetzung von IS, DS und QM im Team genutzt werden. Der Zugang ist mit verschiedenen Endgeräten wie PCs, Tabletts und Smartphones möglich.
Die digitale Version repräsentiert jeweils den aktuellen Regulierungsstand für Informationssicherheit (incl. Cyberschutz), Datenschutz und QM.

1.4.3 Einführung und Sensibilisierung

Die Komplexität der Rechtskonformität in den Bereichen IS, DS und QM in medizinischen Versorgungseinrichtungen setzen eine strukturierte Vorbereitung und Planung voraus. Im Regelfall ist eine erste Phase zur Sensibilisierung und

Orientierung der beteiligten Teams umzusetzen. Diese erste Phase, die durch Informationsmaßnahmen gekennzeichnet ist, ist mit 3-6 Monaten einzuplanen.

Die einzelnen Regelungen ergeben sich aus den folgenden Kapiteln:

Kapitel 4.3.2 und 4.6.2
Kapitel 8.2.1 und 8.2.2

1.4.4 Planung

Die umfassende Planung erfolgt im Team unter Berücksichtigung der individuellen Ausgangssituation der medizinischen Versorgungseinheit. Dabei sind sowohl die personellen Kapazitäten wie auch die vorhandenen Qualifikationen zu berücksichtigen.

Hinweise zu Planungsregelungen:

- Kapitel 4.5.1 und 4.5.2
- Kapitel 8.1.2
- Kapital 27.1 und 28.3

Wesentliche Elemente der Planung:

- Rollen und Verantwortungsbereiche im Team für IS, DS und QM
- Zeitkapazitäten der Verantwortlichen und Mitarbeitern
- Strukturen, z.B. IT-Infrastruktur

Die Planungsphase kann teilweise parallel zur Informationsphase mit 6-12 Monaten angesetzt werden.

1.4.5 Umsetzung mit Curriculum (Einführungs- und Zielplanung)

Alle technischen und organisatorischen Maßnahmen (TOM) für IT-Sicherheit, Datenschutz und QM sind in einem übergeordneten Curriculum (Umsetzungsplan mit Zieldefinition) zu erfassen. Der gesamte Umsetzungszeitraum richtet sich wiederum nach den vorhandenen Qualifikationen und Personalkapazitäten.

Die allgemeinen rechtlichen Rahmenbedingungen bedeuten:

- Der Versorgungsauftrag für alle Patienten hat höchste Priorität
- Die technischen und organisatorischen Maßnahmen (TOM) müssen sich an Wirtschaftlichkeit und Machbarkeit orientieren
- Die Orientierung an den Risiken bestimmen die Reihenfolge der TOM

In diesem Kontext können (analog zur Erst-Einführung des Qualitätsmanagements in Arztpraxen) folgende Umsetzungszeiträume geplant werden:

- 12- 24 Monate Orientierung, Sensibilisierung, Planung und Umsetzung von Schutzmaßnahmen gegen hohe Risiken
- 24-36 Monate Umsetzung der Elementar-Prozesse
- 12-24 Monate „Fine-Tuning“ und Optimierung (PDCA)

1.4.6 Modulare Anwendung

Das vorliegende Managementsystem ist modular aufgebaut und kann deshalb an die jeweils bestehenden Rahmenbedingungen der Praxis / Klinik angepasst werden:

Kapitel 1. – 9.	Allgemeine Regelungen für Informationssicherheit und Datenschutz
Kapitel 10.- 19.	Regelungen für Informationssicherheit (DVG und IT-Richtlinien
Kapitel 20. - 28.	Regelungen für Datenschutz (DSGVO und BDSG)
Kapitel 29.	Qualitätsmanagement (SGB V 135 ff mit QM RL §4)

Die Curriculum Strategie (Einführungskonzept nach Zeitplan) richtet sich nach den bereits bestehenden Voraussetzungen:

Fall 1: Die Praxis setzt bereits ein QMS und ein DSMS nach DSGVO/BDSG ein:
Priorität hat dann die Einführung nach Kapitel 10.- 19. mit der Umsetzung der Informationssicherheit in der Praxis.

Fall 2: Bislang wird kein Management System in der Praxis/Klinik eingesetzt (Neugründung/Übernahme):
Es ist dann das Komplettsystem einzuführen mit Kapitel 1. - 29

Fall 3: Die Praxis setzt bereits ein QMS (z.B. nach QEP oder ISO 9001:2015) ein:
Priorität haben dann die Kapitel 1. – 28. mit der Kombination Informationssicherheit nach DVG und Datenschutz nach DSGVO.

1.4.7 Grundsätze der Anwendung

Nach dem Willen des Gesetzgebers haben die medizinischen Versorger eine hohe Mitwirkungspflicht bei der Anwendung der individuellen Maßnahmen für IS, DS und QM. Die Leitung (also in medizinischen Versorgungseinheiten der Arzt) ist verantwortlich dafür, dass alle Personen die relevanten Regelungen kennen, nach Schulungen diese beherrschen und rechtskonform anwenden. Die angebotenen analogen und digitalen Systeme (ISMS, DSMS, QMS) sind qualifizierte Instrumente, die vom ganzen Team mit Leben zu erfüllen sind. Motivation und Eigeninitiative sind die zentralen Elemente einer erfolgreichen Professionalisierung in der medizinischen Versorgung.

2 Normen

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.

2.1 Normen Informationssicherheit

DIN EN ISO 9001:2015	Qualitätsmanagementsysteme – Anforderungen
ISO/IEC 27001	Information technology – Security techniques – Information security management systems - Requirements
BSI-Standard 100-4	Notfallmanagement
BSI-Standard 200-2	IT-Grundschutz-Vorgehensweise
BSI-Standard 200-3	Risikomanagement
ISO 31000	Risk Management – Principles and guidelines

2.2 Normen Datenschutz

BSI-Standard 200-1	Managementsysteme für Informationssicherheit
BSI-Standard 200-3	Risiko-Management
DIN 66398:2016-05	Leitlinie Löschkonzept
DIN EN ISO 9001:2015	Qualitätsmanagementsysteme – Anforderungen
ISO 31000	Risk Management – Principles and guidelines
ISO / IEC 27001	Information technology – Security techniques – Information security management systems – Requirements
ISO / IEC 29134	Risk Management – Principles and guidelines
VdS 3473	Cyber-Security für kleine und mittlere Unternehmen (KMU), Anforderungen

3 Glossar

Administrativer Zugang:
Zugang, der einen Nutzer dazu befähigt, ein IT-System zu verwalten, d.h. der einem Nutzer umfangreiche Rechte in einem IT-System einräumt.

Administrator:
Person, die für Einrichtung, Betrieb, Überwachung und/ oder Wartung eines IT-Systems oder Netzwerks zuständig ist.

Aktive Netzwerkkomponente:
Netzwerkkomponente, die über eine eigene Logik verfügt, wie z.B. Hub, Switch, Repeater, Bridge, Medienkonverter, Gateway, Firewall usw. Eine aktive Netzwerkkomponente benötigt in aller Regel eine Stromversorgung. Eine aktive Netzwerkkomponente ist ein IT-System.

Angriff:
Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteil zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Archivierung:
Entfernen aus der operativen Umgebung und Langzeitspeicherung bis zum Erreichen der Aufbewahrungsfrist.

Aufgabe:
Dauerhaft wirksame Aufforderung an Handlungsträger, festgelegt Handlungen wahrzunehmen.

Ausfall:
Erliegen eines Prozesses, weil notwendige Ressourcen nicht in ausreichender Menge und / oder in ausreichender Qualität zu Verfügung stehen.

Authentizität:
Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit.

Authentifizierungsmerkmal:
Merkmal, mit dessen Hilfe eine anfragende Instanz ihre Identität nachweisen kann. Authentifizierungsmerkmale können Wissen (z.B. Passwort oder PIN), Besitz (z.B. Chipkarte oder Token) oder biometrische Merkmale (z.B. Fingerabdruck oder Iris) sein.

Autorisierung:
Bei der Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtig ist.

Basis-Absicherung:
Die Basis-Absicherung ermöglicht es, als Einstige in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen.

Basis-Anforderung:
Siehe Sicherheitsanforderung.

Beauftragter für IT-Sicherheit
Person mit Fachkompetenz zur IT-Sicherheit, die in großen Institutionen für Aspekte rund um die IT-Sicherheit zuständig ist, in enger Abstimmung mit dem IT-Betrieb. Der ISB gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben., ein Beauftragter für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Ein Beauftragter für die IT-Sicherheit ist somit typischerweise im IT-Betrieb tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Bedrohung:
Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

Benutzerkennung (häufig auch Benutzerkonto)
Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben beziehungsweise Ziffern.

Biometrie
Unter Biometrie ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Diese kann genutzt werden, um Benutzer auf Grundlage besonderer Merkmale eindeutig zu authentisieren. Ein oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

BSI
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine in der Bundesstadt Bonn ansässige zivile obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat, die für Fragen der IT-Sicherheit zuständig ist. Der Leitsatz des BSI lautet: „Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.“. Für 2017 waren dem BSI 180 neue Stellen zugesprochen worden. Mitte 2018 waren im BSI rund 940 Mitarbeiter beschäftigt. Für 2019 waren im Bundeshaushalt weitere 349,5 Stellen für das BSI vorgesehen.

Business Continuity Management (BCM):
Ganzheitlicher Managementprozess für die systematische Vorbereitung auf das Bewältigen von Schadensereignissen mit dem Ziel, zentrale Geschäftsprozesse auch beim Eintreten von Notfällen, Krisen oder Katastrophen weiter zu betreiben, bzw. schnellstmöglich wieder in Gang zu setzen.

Business Impact Analyse (BIA)
Eine Business Impact Analyse (Folgeschäden-Abschätzung) ist eine Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden. Es ist ein Verfahren, um kritische Ressourcen und Wiederanlaufanforderungen sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen zu identifizieren.

Client:
Als Client wird Soft- oder Hardware bezeichnet, die bestimmt Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Cloud Computing:
Technologie, die es erlaubt über ein Netz auf einem geteilten Pool von konfigurierbaren IT-Ressourcen zuzugreifen.

Curriculum

Schulungsplan u.a. zur Einführung von Managementsystemen zum Datenschutz, zur Informationssicherheit und zum Qualitätsmanagement. Ein Curriculum ist Bestandteil der Planung bei der Einführung eines DSMS, ISMS und QMS.

Cyber-Sicherheit:
Der Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. 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. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Daten:
Gebilde aus Zeichen, die aufgrund bekannter Abmachungen Informationen darstellen.

Datenleitung:
Physischen Medium, über das Daten ausgetauscht werden können.

Datenschutz:
Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigen Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datenschutz-Management:
Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Datenschutz-Managementsystem (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.

Datensicherheit:
Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist „Informationssicherheit“.

Datensicherung (englisch „Backup“):
Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen 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.

DICOM
Digital Imaging and Communication in Medicine: internationaler Standard für Bildverarbeitung in medizinischen Einrichtungen. DICOM Server waren in der Vergangenheit Schwachstellen einiger Kliniken im Internet.

Digitale Signatur:
Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat und
- Es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde.

DVG
Digitale Versorgung Gesetz (DVG) definiert die neuen Rahmenbedingungen für Arztpraxen und Kliniken im Internet. Es macht ebenfalls Maßnahmen zur Informationssicherheit verpflichtend. Die entsprechenden Richtlinien werden von der KBV herausgegeben.

Echtzeitbetrieb:
Elektronische Datenverarbeitung, die (nahezu) simultan mit den entsprechenden Prozessen in der Realität abläuft.

Externer:
Natürliche Person, die kein Mitarbeiter ist. Externe sind z.B. Geschäftspartner oder Gäste.

Firewall:
Eine Firewall (oft auch als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway).

Funktion:
Bündel von Aufgaben, durch die ein Teil der Ziele der Organisation erreich werden soll.

Gefahr:
Möglichkeit einer Schadwirkung auf ein zu schützendes Objekt.
„Gefahr“ wird oft als übergeordneter Begriff gesehen, wohingegen unter „Gefährdung“ eine genaue beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. Die Gefährdungen sind dann „defekter Datenträger“ und „Diebstahl von Datenträgern“. Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, „Gefahr“ und „Gefährdung“ als gleichbedeutend aufzufassen.

Gefährdung:
Bedrohung, die konkret über eine Schwachstelle auf ein zu schützendes Objekt einwirkt (Bedrohung plus Schwachstelle).

Grundwerte der Informationssicherheit:
Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.
Jedem Anwender des IT-Grundschutzes steht es natürlich frei, bei der Schutzbedarfserstellung weitere Grundwerde zu betrachten, wenn dies in seinem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.

HL7
Health Level 7, internationaler Standard für administrative Schnittstellen im Gesundheitswesen. Der Standard wird auch zur EPA Strukturierung von klinischen Patientendaten verwendet: CDA = Clinical Document Architecture.

IHE
Das Projekt „Integrating the Healthcare Enterprise“ hat sich die Realisierung von standardisierten Abläufen in der Medizin-Informatik zum Ziel gesetzt. Im IHE-Projekt arbeiten bereits seit fast sechs Jahren Software-Unternehmen und Hersteller von Medizin-Technik eng zusammen, um Standards in allen Bereichen zu erproben und im Rahmen der Qualitäts- und Investitions-Sicherung zu realisieren.

Information:
Sinn und Bedeutung, die der Empfänger aus erhaltenen Daten interpretiert.

Informationssicherheit:
Schutz von Informationen hinsichtlich gegebener Sicherheitsanforderungen (beispielsweise Vertraulichkeit, Verfügbarkeit oder Integrität).

Informationssicherheitsbeauftragter (ISB):
Ein Informationssicherheitsbeauftragter (kurz IS-Beauftragter oder ISB) ist für die operative Erfüllung der Aufgabe „Informationssicherheit“ zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM). Die Rolle des ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde wahrgenommen werden.

Informationssicherheitsmanagement (IS-Management):
Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen

kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

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.

Informationssicherheitsmanagementeam (IS-Managementteam):
In größeren Institutionen ist es sinnvoll, ein IS-Management-Team (häufig auch IT-Sicherheitsmanagement-Team) aufzubauen, das den ISB unterstützt, beispielsweise indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

Informationssicherheitsteam (IST):
Gremium, das die Aufgaben gemäß Abschnitt 4.4. wahrnimmt.

Informationstechnik (IT):
Oberbegriff für die Informations- und Datenverarbeitung sowie -übertragung inklusive der dafür benötigten Hard- und Software.

Infrastruktur:
Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT-genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.

Integrität:
Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmt Attribute, wie z.B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Intranet:
Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Institution) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch eine Firewall abgesichert.

Inventarisierung:
Bestandsaufnahme zu einem definierten Zeitpunkt.

IS-Leitlinie:
Leitlinie zur Informationssicherheit, die die Anforderungen gemäß Kapitel 5 erfüllt.

IS-Richtlinie:
Sammlung von Regelungen zur Informationssicherheit, die die Anforderungen gemäß Kapitel 6 erfüllt.

IT-Grundschutz-Check:
Der Begriff bezeichnet im IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Institution bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch fehlen (früher: Basis-Sicherheitscheck).

IT-Infrastruktur:
Alle langlebigen Einrichtungen materieller und institutioneller Art für den Betrieb von Anwendungssoftware.

IT-Ressource:
Betriebsmittel für die elektronische Informationsverarbeitung. Hierzu zählen u.a. IT-Systeme, Datenträger, Verbindungen, Daten, Informationen sowie Mitarbeiter.

IT-System:
IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.

IT-Verantwortlicher:
Leiter der IT-Abteilung, bzw. das für die Informationstechnik zuständige Management.

IT-Outsourcing:
Auslagerung von IT-Aufgaben an einen von der Organisation rechtlich unabhängigen Anbieter.

IT-System:
Technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit aus Hard- und Software bildet. Typische IT-Systeme sind z.B. Server (physisch und virtuell), Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets und aktive Netzwerkkomponenten.

Katastrophaler Schaden:
Schaden, auf den eines der folgenden Kriterien zutrifft:

1. Auswirkungen auf Leib und Leben von Personen: Es werden Menschen schwer verletzt oder kommen ums Leben.
2. Auswirkung auf zentrale Prozesse: Zentrale Prozesse der Organisation werden zum Erliegen gebracht und die Rückkehr zum Regelbetrieb ist (innerhalb eines akzeptablen Zeitraums) nicht möglich.
3. Auswirkung auf zentrale Werte: Zentrale Werte der Organisation gehen verloren oder werden zerstört und ihre Wiederherstellung ist (mit den Ressourcen der Organisation) nicht mehr möglich.
4. Auswirkung auf die Rechtskonformität: Gesetze, Verträge oder Normen werden gebrochen und die daraus resultierende Haftung ist für die Organisation oder für die Verantwortlichen ruinös.

Komponenten:
Eine Komponente ist in der Softwarearchitektur eine eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die mit anderen Komponenten verbunden werden kann. Sie ist sowohl fachlich als auch technisch unabhängig und besitzt eine gewisse Größe (im Sinne eines wirtschaftlichen Wertes).

Konnektor
Intelligente Hardware-Schnittstelle, mit der die Arztpraxis mit der Telematikinfrastruktur (TI) verbunden wird. Der Anschluss erfolgt durch Fachleute vor Ort (DLO=Dienstleister vor Ort) und muss nach den genauen technischen Anweisungen erfolgen. Bei einem nicht fachgerechten Anschluss besteht die Gefahr von Störangriffen von außen.

Kritische Individualsoftware:
Software, die für den Betrieb von kritischen IT-Systemen zwingend benötigt wird und individuell für die Organisation erstellt oder angepasst wurde.

Kritische Informationen:
Informationen, die die Bedingungen gemäß Abschnitt 9.2. erfüllen.

Kritisches IT-System:
IT-System, das die Bedingungen gemäß Abschnitt 9.3. erfüllt.

Kritischer mobiler Datenträger:
Mobiler Datenträger, der die Bedingungen gemäß Abschnitt 9.3 erfüllt.

Kritische Verbindung:
Verbindung, die die Bedingungen gemäß Abschnitt 9.3. erfüllt.

Kronjuwelen:
Als Kronjuwelen werden solche Assets bezeichnet, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde.

Leitlinie:
Dokument des Topmanagements, das ein Ziel der Organisation und seine Priorität definiert sowie Verantwortlichkeiten zu seiner Erreichung festlegt.

Leitlinie zur Informationssicherheit:
Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. IN ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

Maximal tolerierbare Ausfallzeit (MTA):
Zeit, bis zu der eine definierte Leistung (z.B. ein Notbetriebsniveau) wieder verfügbar sein muss.

Maximal tolerierbarer Datenverlust (MTD):
Zeitspanne, die als noch akzeptierbar für einen Datenverlust erachtet wird.

Mitarbeiter:
Natürliche Person, die in einem Vertragsverhältnis oder in einem öffentlich-rechtlichen Dienst- und Treueverhältnis mit der Organisation steht und eine oder mehrere Positionen in der Organisation einnimmt. Mitarbeiter sind z.B. Angestellt, Arbeiter, Beamte, freier Mitarbeiter, Dienstleister oder deren Mitarbeiter bzw. Erfüllungsgehilfen.

Mobiler Datenträger:
Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z.B. Speichersticks und -karten sowie externe Festplatten, aber auch Speichermedien wie CD-ROMs, DVDs und Disketten.

Mobiles IT-System:
IT-System, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile IT-Systeme sind z.B. Notebooks, Smartphones, Tablets oder Digitalkameras.

Netzplan:
Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Netzwerkkomponente:
Technische Anlage, die der Weiterleitung von Daten dient. Es werden aktive und passive Netzwerkkomponenten unterschieden.

Netzübergang:
Schnittstelle zwischen zwei unterschiedlichen Netzwerken. Dabei können sich die Netzwerke durch die physikalischen Übertragungsmedien, durch die verwendeten Protokolle oder durch eine unterschiedliche administrative Hoheit voneinander unterscheiden.

Notbetrieb:
Auf ein Minimum reduzierte Funktionstüchtigkeit, mit der ein Prozess aufrechterhalten werden kann.

Notbetriebsniveau:
Definition, welche Funktionen von einer IT-Ressource erbracht werden müssen, damit ein Notbetrieb aufrechterhalten werden kann.

Organisationseinheit:
Einheit, in der artverwandet (Teil-)Aufgaben oder Tätigkeiten zusammengefasst sind.

Passive Netzwerkkomponente:
Netzwerkkomponente ohne eigene Logik z.B. Kabel, Patchfeld, Dose, Stecker usw. Eine passive Netzwerkkomponente benötigt in aller Regel keine Stromversorgung.

Passwort:
Mit der Eingabe eines Passwortes weist der Benutzer nach, dass er 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).

Patientendatenschutzgesetz (PDSG)
Das Patientendatenschutzgesetz ist die nächste Stufe der Gesetzgebung zur digitalen Versorgung in Deutschland. Es regelt die Voraussetzungen der Elektronischen Patientenakte im Internet. Für die EPA ist ein Einführungsplan bis 2022 veröffentlicht worden, der verschiedene Stufen der EPA Nutzung vorsieht. Die EPA stellt hohe Anforderungen an Informationssicherheit und Datenschutz und wird in den Praxen sehr hohe Anforderungen an die geschützten Datenprozesse stellen.

Patch:
Ein Patch (vom englischen „patch“, auf Deutsch „Flicken“) ist ein kleines Programm, das Softwarefehler, wie z.B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Position:
Platz, den ein Mitarbeiter in der Hierarchie einer Organisation einnimmt.

Privilegierte Berechtigungen:
Privilegierte oder administrative Berechtigungen umfassen weitergehende Zugriffsmöglichkeiten auf IT-Systeme oder Software-Komponenten, als für normale Benutzer erforderlich sind. In der Regel werden privilegierte Berechtigungen nur solchen Rollen, Gruppen oder Personen zugewiesen, die überwiegend mit der Administration von Informationstechnik betraut sind. Dazu gehört unter anderem die betrieblich sowie sicherheitstechnische Konfiguration.

Projektverantwortlicher:
Person, die für die ordnungsgemäße Durchführung eines Projekts verantwortlich ist.

Proxy:
Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Prozess:
System von Tätigkeiten, das Eingaben mit Hilfe von Ressourcen in Ergebnisse umwandelt.

Prozess mit hohem Schadenspotential:
Prozess, bei dessen Fehlfunktionen oder kurzzeitigem Ausfall ein katastrophaler Schaden entstehen kann.

Prozessverantwortlicher:
Person, die inhaltlich für einen oder mehrere Prozesse verantwortlich ist. Sie besetzt den Über blick über die für diese Prozesse benötigten Ressourcen und über die an sie gestellten Anforderungen.

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.

Regelung:
Verbindliche Vorgabe.

Ressource:
Betriebsmittel, das der Organisation gehört oder ihr zu Verfügung steht.

Revision:
Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Die Revision sollte unabhängig und neutral sein.

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 oder besser Unwägbarkeit.
In der ISO wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings al gängiger in der Praxis durchgesetzt.
Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse:
Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in den Dokumenten zum IT-Grundschutz weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Risikomanagement:
Als Risikomanagement werden alle Aktivtäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren:
Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen zw. Aufeinander abgestimmt sein.

Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus:

- Identifikation von Risiken,
- Einschätzung und Bewertung von Risiken,
- Behandlung von Risiken,
- Überwachung von Risiken und
- Risikokommunikation

Schaden / Konsequenz:
Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden“ genannt). Hierbei kann es sich grundsätzlich um eine positive oder negative Abweichung handeln.
Eine positive Konsequenz beziehungsweise positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet.
Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z.B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z.B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.

Schadfunktion:
Mit Schadfunktion wir eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst besteuert gefährden kann.

Schadprogramm / Schadsoftware / Malware:
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware oder Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious Software“ und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Schnittstelle:
Teil eines IT-Systems, das der Kommunikation dient, wie z.B. Ethernet- und Wireless-LAN-Adapter, ISDN-Karten, Modems, USB-Ports, NVD- und Infrarot-Schnittstellen, SD-Slots oder Tastaturen.

Schutzbedarf:
Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schutzbedarfsfeststellung:
Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen, der IT-Systeme, Räume und Kommunikationsverbindungen bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet. Die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit) entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“.

Schwachstelle:
Umstand, der es ermöglicht, dass eine Bedrohung mit einem zu schützenden Objekt räumlich und / oder zeitlich zusammentreffen kann.

Server:
Zentrales IT-System, über das funktionale und / oder infrastrukturelle Netzdienste realisiert werden.

Sicherheitsanforderung:
Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. Dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben (siehe dort). Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff „control“ verwendet.
Der IT-Grundschutz unterscheidet zwischen Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegen sprechen. Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Sicherheitskonzept:
Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess

eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Sicherheitsmaßnahme:
Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Sicherheitsmaßnahmen dienen zur Erfüllung von Sicherheitsanforderungen (siehe dort). Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaß0nahme benutzt. Als englische Übersetzung wurde „safeguard“, „security measure“ oder „measure“ gewählt.

Sicherheitsrichtlinie (englisch „Security Policy“)
In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsanforderungen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Sicherheitsvorfall:
Unerwünschtes Ereignis, das Auswirkung auf die Informationssicherheit hat und große Schäden nach sich ziehen kann. Was genau als Sicherheitsvorfall eingestuft wird, wird von der Organisation selbst definiert.

Speicherort:
Ort, an dem Nutzer bzw. Applikationen ihre Daten speichern.

Spyware:
Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines IT-Systems sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

Standard-Absicherung:
Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise des BSI-Standards 100-2. Mit der Standard-Absicherung kann ein ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.

Standardsoftware:
Unter Standardsoftware wird Software (z.B. Programme, Programm-Module oder Tools) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich dadurch aus, dass Institutionen sie selbst installieren und mit wenig Aufwand anpassen können.

Störung:
Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Die Beseitigung einer Störung kann im allgemeinen Tagesgeschäft vorbenommen werden.

Strukturanalyse:
In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützten.

Systemsoftware:
Firmware, Betriebssystem und systemnahe Software, Systemsoftware verwaltet die internen und externen Hardwarekomponenten eines IT-Systems.

Telematikinfrastruktur (TI)
Telematikinfrastruktur, das gesicherte Netz der Kassenärztlichen Bundesvereinigung. Der Anschluss an die TI ist für Kassenärzte in Deutschland seit 2020 verpflichtend.

Topmanagement:
Oberste Führungsebene, wie z.B. Vorstände, Geschäftsführer oder Behördenleiter.

Trojanisches Pferd:
Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

VdS
Die VdS Schadenverhütung GmbH ist Europas größtes Institut für Unternehmenssicherheit und eine 100%ige Tochter des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV). VdS bietet Dienstleistungen mit den Schwerpunkten Brandschutz, Security, Cyber-Security, Datenschutz, Naturgefahren, Organisation und Bildung und veröffentlicht Richtlinien für Sicherheitstechniken, die die Basis von EN-Normen bildeten. Am Unternehmenssitz in Köln und in den Außenbüros der Technischen Prüfstellen in Deutschland, im europäischen Ausland sowie in der Niederlassung Shanghai beschäftigt das Institut rund 500 Mitarbeiter.

Verbindung:
Kanal, über den Daten ausgetauscht werden können.

Verfahren:
Festgelegt Art und Weise, wie ein Prozess (oder auch eine einzelne Tätigkeit innerhalb eines Prozesses) auszuführen ist.

Verfügbarkeit:
Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. Die Ressource kann wie vorgesehen genutzt werden.

Verschlüsselung
Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation, also die Zurückgewinnung des Klartextes aus dem Geheimtext, wird Entschlüsselung genannt.

Vertraulichkeit:
Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Es ist auch die Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.

VLAN:
Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende IT-Systeme zu einem virtuellen Netz verbunden werden.

VPN:
Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder IT-Systeme über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.
Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Webinar:
Schulungsangebote im Internet, die auch für die Bereiche Datenschutz und Informationssicherheit in Arztpraxen und Kliniken angeboten werden. Sie erfüllen die Anforderung nach ISO Standards (z.B. ISO 27001, ISO 9001 etc.).

WLAN
Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IOEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Wurm:
Bei (Computer-, Internet-, E-Mail) Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

Zentraler Prozess:
Prozess, der mitentscheidend für die Aufgabenerfüllung der Organisation ist. Dies kann z.B. ein Prozess für die Wertschöpfung oder für den Erhalt bzw. die Verbesserung der Wettbewerbsfähigkeit sein.

Zertifikat:
Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterschieden sind vor allem:

- ISO 27001-Zertifikate: Der ISO-Standard 27001 „Information technology – Security techniques – Information security management systems requirements specification" ermöglicht eine Zertifizierung des Informationssicherheitsmanagements.
- ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-IT-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-IT-Grundschutz-Auditor gehören eine Sichtung der von der Institution erstellten Referenzdokument, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsanfor4derungen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es auf Wunsch des Antragstellers.
- Schlüsselzertifikat: Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten Kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.
- Zertifikate für IT-Produktsicherheit: Zertifiziert wird nach international anerkannten Sicherheitskriterien, wie z.B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung ist jedoch, dass die am Ende des

Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen

Ein digitales Zertifikat ist ein Datensatz, der bestimmt Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann Ein digitales Zertifikat ermöglicht unter anderem die Verwendung elektronischer Signaturen.

Zugang:
Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme oder System-Komponenten und Netze zu nutzen.

Zugriff:
Mit Zugriff wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt:
Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z.B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

4 Organisation

Um mit möglichst geringem Aufwand das notwendige Sicherheitsniveau zu definieren, umzusetzen und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage anzupassen, ist es notwendig, eine entsprechende Organisation zu etablieren.

4.1 Verantwortlichkeiten

Verantwortlichkeiten werden eindeutig und widerspruchsfrei zugewiesen.

4.1.1 Verantwortlichkeiten Informationssicherheit

Die Verantwortlichkeiten für Informationssicherheit (IS) und Cyberschutz (CS) werden unter Berücksichtigung der erforderlichen Qualifikationen festgelegt. Grundsätzliche Kenntnisse zu den IT-Anwendungen sind erforderlich.

4.1.2 Verantwortlichkeiten Datenschutz

Die Verantwortlichkeiten für Datenschutzaufgaben werden in Abhängigkeit von der Qualifikation festgelegt. Grundlagenkenntnisse der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) werden nachgewiesen.

4.1.3 Zuweisung Dokumentation

4.1.3.1 Zuweisung und Dokumentation Informationssicherheit

Es wird für jede Verantwortlichkeit dokumentiert:

1. Welche Ziele für IS erreicht werden sollen
2. Für welche Ressourcen die Verantwortlichkeit für IS besteht
3. Welche Aufgaben erfüllt werden müssen, damit die IS-Ziele erreicht werden
4. Welche Berechtigungen an die IS-Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können
5. Welche Ressourcen für die Wahrnehmung der IS-Verantwortlichkeit zur Verfügung stehen
6. Wie und durch welche Position(en) die Erfüllung der IS-Verantwortlichkeit überprüft wird
7. Welche Positionen die IS-Verantwortlichkeit wahrnehmen

4.1.3.2 Zuweisung und Dokumentation Datenschutz

Es wird für jede Verantwortlichkeit dokumentiert:

1. Welche Ziele für DS erreicht werden sollen
2. Für welche Ressourcen die Verantwortlichkeit für DS besteht
3. Welche Aufgaben erfüllt werden müssen, damit die DS-Ziele erreicht werden
4. Welche Berechtigungen an die DS-Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können
5. Welche Ressourcen für die Wahrnehmung der DS-Verantwortlichkeit zur Verfügung stehen
6. Wie und durch welche Position(en) die Erfüllung der DS-Verantwortlichkeit überprüft wird
7. Welche Positionen die DS-Verantwortlichkeit wahrnehmen

4.1.4 Funktionstrennungen

Bei der Verteilung der Verantwortlichkeiten wird das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten dürfen nicht von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

4.1.4.1 Funktionstrennungen Informationssicherheit

Um Zuständigkeitslücken oder Überschneidungen von Verantwortlichkeiten zu vermeiden, müssen die entsprechenden Regelungen jährlich vom Informationssicherheitsbeauftragten (ISB) überprüft werden.

4.1.4.2 Funktionstrennungen Datenschutz

Es müssen jährliche Überprüfungen des Datenschutzbeauftragten vorgenommen werden, um die Lücken oder Überschneidungen von Verantwortlichkeiten im Bereich Datenschutz zu vermeiden.

4.1.5 Zeit-Ressourcen

4.1.5.1 Zeit-Ressourcen Informationssicherheit

Um zugewiesene IS-Verantwortlichkeiten wahrzunehmen, müssen die entsprechenden Mitarbeiter im erforderlichen Umfang von anderen Tätigkeiten freigestellt werden.

4.1.5.2 Zeit-Ressourcen Datenschutz

Um zugewiesene Datenschutz-Verantwortlichkeiten wahrzunehmen, müssen die entsprechenden Mitarbeiter im erforderlichen Umfang von anderen Tätigkeiten freigestellt werden.

4.1.6 Aufgaben-Delegierung

Aufgaben können dann delegiert werden, wenn die Personen, die delegierte Aufgaben übernehmen, über die entsprechenden Qualifikationen in der Informationssicherheit und / oder Datenschutz nach DSGVO verfügen.

Die Verantwortung für delegierte Aufgaben verbleibt jedoch bei ihnen, so dass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen müssen.

4.1.6.1 Aufgaben-Delegierung Informationssicherheit

Verantwortliche für Informationssicherheit können Aufgaben an andere Personen delegieren soweit diese über IT-Grundkenntnisse generell und in der Informationssicherheit verfügen. Dazu sind im Regelfall IT-Ausbildungen oder spezifische Schulungen zu dokumentieren.

4.1.6.2 Aufgaben-Delegierung Datenschutz

Die Datenschutz-Verantwortlichen können dann Aufgaben auch an andere Personen delegieren, wenn diese eine Grundausbildung in der DSGVO und im BDGS absolviert haben.

4.2 Praxisleitung

Die Praxisleitung verpflichtet sich zur Wahrnehmung folgender Verantwortlichkeiten:

1. Übernehmen der Gesamtverantwortung für die Informationssicherheit und den Datenschutz
2. In Kraft setzen von Richtlinien für die Informationssicherheit (IS-Richtlinien) und Datenschutzrichtlinien
3. Bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit und den Datenschutz
4. Einbetten der Informationssicherheit und des Datenschutzes in die Strukturen, Hierarchien und Arbeitsabläufe der Organisation

4.3 Beauftragte

Die Leitung benennt Beauftragte für Informationssicherheit und Datenschutz nach den rechtlichen Rahmenbedingungen.

4.3.1 Informationssicherheitsbeauftragter (ISB)

Die Praxisleitung weist die Verantwortlichkeiten eines Informationssicherheitsbeauftragten (ISB) einem Mitarbeiter zu.
Dieser Mitarbeiter stellt sicher, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit erreicht werden.

Hierfür wird er insbesondere die folgenden Verantwortlichkeiten wahrnehmen:

1. Steuern, Koordinieren und Prüfen der technischen und organisatorischen Maßnahmen, kontinuierliches Verbessern der Informationssicherheit, insbesondere Anpassen der Informationssicherheit an neue Bedrohungen, Änderungen im technischen und organisatorischen Umfeld und an neue gesetzliche, betriebliche und vertragliche Anforderungen.
2. Jährliches Berichten an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle.

Es wird sichergestellt, dass die Verantwortlichkeiten des ISB auch in seiner Abwesenheit wahrgenommen werden.

Dies dann z.B. durch eine Stellvertreterregelung umgesetzt werden.

4.3.2 Datenschutzbeauftragter

Die Leitung weist die Verantwortlichkeiten eines Datenschutzkoordinators oder / und eines Datenschutzbeauftragten einem qualifizierten Mitarbeiter zu. Der Datenschutzkoordinator und / oder -beauftragte (je nach rechtlicher Anforderung) nimmt die folgenden Verantwortlichkeiten war:

1. Initiieren, Planen, Umsetzen und Steuern des Datenschutzmanagementsystems (DSMS)
2. Erarbeiten konkreter Verbesserungsvorschläge (siehe PDCA)
3. Unterstützen der Leitung bei der Erarbeitung und jährlichen Überprüfung sowie bei der Anpassung der DS-Leitlinie (siehe Kapitel 5)
4. Unterstützen der Leitung in zentralen Fragen des Datenschutzes, insbesondere nach DSGVO und BDSG
5. Erarbeiten und jährliches Überprüfen und Anpassen aller DS-Richtlinien (PDCA)
6. Untersuchen von Datenschutz-relevanten Ereignissen aller Art
7. Einleiten und Steuern von Sensibilisierungs- und Schulungsmaßnahmen gegebenenfalls mit externer Unterstützung

8. Beteiligung als Ansprechpartner bei Projekten mit Auswirkungen auf den Datenschutz, sowie bei der Einführung neuer Software und IT-Systeme.
9. Jährliches Berichten an die Leitung oder den Datenschutzbeauftragten (DSB) (falls bestellt) über den aktuellen Stand des Datenschutzes.
10. Wahrnehmen der Rolle des zentralen Ansprechpartners für Datenschutz, sofern kein Datenschutzbeauftragter bestellt ist.

4.4 Teams

Die Praxisleitung bestellt in großen Praxen ein Informationssicherheitsteam (IST) und ein Datenschutzteam.

In diesen werden folgende Organisationseinheiten bzw. Positionen persönlich oder durch einen Repräsentanten vertreten sein:

1. Praxisleitung
2. ISB oder DSB
3. IT-Verantwortliche
4. Mitarbeiter
5. Verantwortliche für den Datenschutz (z.B. Datenschutzmanager und / oder Datenschutzbeauftragter)

Das Team unterstützt den ISB oder DSB, insbesondere bei den folgenden Tätigkeiten:

1. Erkennen und Bewerten neuer Bedrohungen und Schwachstellen
2. Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit und Datenschutz
3. Organisationsweites Steuern und Koordinieren der Maßnahmen zur Informationssicherheit und zum Datenschutz

4.5 Verantwortliche

4.5.1 IT-Verantwortliche

Die Aufgaben eines IT-Verantwortlichen werden von der Praxisleitung mindestens einem Mitarbeiter zugewiesen.

IT-Verantwortliche übernehmen folgende Aufgaben:

1. Umsetzen der IS-Richtlinien in ihrem Verantwortungsbereich durch entsprechende technische und organisatorische Maßnahmen (TOM)

2. Abstimmen aller Maßnahmen mit dem ISB, die aus ihrer Sicht zur Verbesserung und Erhaltung der Informationssicherheit in ihrem Verantwortungsbereich ergriffen werden müssen sowie deren Planung, Koordination und Umsetzung.

4.5.2 Datenschutz-Verantwortliche

Von der Praxisleitung werden die Aufgaben eines DS-Verantwortlichen an mindestens einen Mitarbeitern gewiesen:

1. Umsetzen der DS-Richtlinien in ihrem Verantwortungsbereich durch entsprechende technische und organisatorische Maßnahmen (TOM)
2. Abstimmen aller Maßnahmen mit dem DSB, die aus ihrer Sicht zur Verbesserung und Erhaltung des Datenschutzes in ihrem Verantwortungsbereich ergriffen werden müssen sowie deren Planung, Koordination und Umsetzung.

4.6 Besondere Verantwortungsbereiche

In der IT-Sicherheit und dem Datenschutz sind spezielle Verantwortungsbereiche definiert:

- Administratoren als besondere Verantwortliche für IS
- Eigentümer einer Datenverarbeitung im Datenschutz

4.6.1 Administratoren Informationssicherheit

Administratoren werden in Abstimmung mit dem IT-Verantwortlichen die technischen Maßnahmen für die Informationssicherheit implementieren.

Die Verantwortlichkeiten eines Administrators werden mindesten einem Mitarbeiter zugewiesen.

4.6.2 Eigentümer einer Datenverarbeitung im Datenschutz

Für jede Datenverarbeitung sind die Verantwortlichkeiten eines Eigentümers einem Mitarbeiter zugewiesen (beispielsweise Datenverarbeitung in der Abrechnung).

Der Eigentümer einer Datenverarbeitung nimmt folgende Verantwortlichkeiten war:

1. Unterstützen bei Fragen zur Verarbeitung, insbesondere bei personenbezogenen Daten

2. Untersuchen von Datenschutzvorfällen (siehe Kapitel 23)
3. Melden des Bedarfs an Sensibilisierungs- und Schulungsmaßnahmen an die Leitung bzw. die Datenschutzverantwortlichen.

4.7 Team-Leiter / Vorgesetzte

Vorgesetzte, die Verantwortung für Mitarbeiter tragen, müssen sicherstellen, dass die getroffenen technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter umgesetzt werden.

4.8 Mitarbeiter

Mitarbeiten sind in allen Fragen zu IS und DS zu sensibilisieren und zu schulen, damit sie ihre Aufgaben erfüllen können:

4.8.1 Mitarbeiteraufgaben Bereich Informationssicherheit

Mitarbeiter übernehmen folgende Aufgaben:

1. Einhalten und Umsetzen aller sie oder ihre Tätigkeit betreffenden Maßnahmen zur Informationssicherheit
2. Melden von Störungen, Ausfällen und Sicherheitsvorfällen

4.8.2 Mitarbeiteraufgaben Bereich Datenschutz

Mitarbeiter übernehmen folgende Aufgaben:

1. Einhalten und Umsetzen aller sie oder ihre Tätigung betreffenden Regelungen zum Datenschutz
2. Melden von Datenschutzvorfällen

4.9 Projektverantwortliche

4.9.1 Projektverantwortliche Informationssicherheit

Projektverantwortliche werden den ISB bei allen Projekten mit Auswirkung auf die Informationsverarbeitung konsultieren, um sicherzustellen, dass sicherheitsrelevante Aspekte ausreichend beachtet werden.

4.9.2 Projektverantwortliche Datenschutz

Der DSB wird von den Projektverantwortlichen einbezogen, wenn Projekte Auswirkungen auf die Verarbeitung personenbezogener Daten haben. Dadurch wird sichergestellt, dass datenschutzrelevante Aspekte ausreichend beachtet werden.

4.10 Externe Partner

Die Leitung ist auch für alle Handlungen und Maßnahmen externer Partner verantwortlich. Deshalb kommt der Auswahl vertrauenswürdiger Partner und Prüfung deren Qualifikation eine hohe Bedeutung zu.

4.10.1 Externe Partner Informationssicherheit

Externe müssen verpflichtet werden, die sie betreffenden Maßnahmen und Regelungen zur Informationssicherheit einzuhalten bzw. umzusetzen, sofern sie Zugriff auf kritische Informationen besitzen oder sie nichtöffentliche Bereiche der Informationstechnologie (IT) der Organisation nutzen.

4.10.2 Externe Partner Datenschutz

Im Datenschutz sind die externen Auftragsverarbeiter nach DSGVO besonders zu führen und zu kontrollieren. In der DSGVO bestehen dazu die ausführlichen Regelungen für Auftragsverarbeiter. Die entsprechend definierten Verpflichtungen werden im Abschnitt 22.1.4 nach DSGVO und BDSG dokumentiert.

5 Leitlinien

5.1 Anforderungen allgemein

Die Leitlinie wird von der Praxisleitung erstellt und in Kraft gesetzt.
Die Praxisleitung wird die Leitlinie jährlich auf Aktualität prüfen und bei Bedarf aktualisieren.
Die Leitlinie wird nach jeder Aktualisierung zeitnah bekannt gegeben und in der jeweils aktuellen Form allen Betroffenen zur Verfügung stehen.

5.1.1 Anforderungen Informationssicherheit (IS-Leitlinie)

Die Leitlinie zur Informationssicherheit (IS-Leitlinie) ist das zentrale Dokument für die gesamte Informationssicherheit. In ihr werden die zu erreichenden Ziele durch die Praxisleitung vorgegeben und Verantwortlichkeiten definiert.
Für IS

5.1.2 Anforderungen Datenschutz

Die Datenschutz-Leitlinie ist analog zur IS-Leitlinie das zentrale Dokument für alle Datenschutzprozesse nach DSGVO und BDSG. Sie enthält die zu erreichende Ziele, die durch die Leitung vorgegeben werden. In ihr werden die Verantwortlichkeiten und Befugnisse für DS definiert.

5.2 Inhalte

Die Inhalte der Leitlinien werden frei gestaltet. Wichtig ist, dass alle relevanten Ziele und Elemente enthalten sind.

5.2.1 Inhalte Informationssicherheit

Die Leitlinie erfüllt folgende Anforderungen:

1. Sie definiert die Ziele und den Stellenwert der Informationssicherheit in der Organisation.
2. Sie definiert sämtliche erforderlichen Positionen (siehe Abschnitte 4.2. bis 4.10) und weist auf deren Aufgaben hin.

5.2.2 Inhalte Datenschutz

Die Datenschutz-Leitlinie erfüllt speziell folgende Anforderungen:

1. Die DS-Leitlinie definiert den Stellenwert des Datenschutzes und die konkreten Ziele.
2. Die Leitlinie verpflichtet die Organisationseinheit alle rechtlichen Anforderungen des Datenschutzes jeweils aktuell umzusetzen.
3. Die DS-Leitlinie definiert alle Positionen für die Datenschutzprozesse und stellt die verbundenen Aufgaben heraus.
4. Die DS-Leitlinie enthält auch Hinweise auf die Konsequenzen bei Nichteinhaltung bzw. Nichtbeachtung.

5.3 Beispiel Leitlinie

5.3.1 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 (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein.
Negative finanzielle und immaterielle Folgen für die Praxis/Klinik 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.

5.3.2 Beispiel Leitlinie zum Datenschutz

Der Schutz der personenbezogenen Daten hat höchste Priorität für alle Personen in der Praxis / Klinik. Es gelten insbesondere auch alle rechtlichen Rahmenbedingungen zur Einhaltung der ärztlichen Schweigepflicht.
Der Datenschutz 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

Die Ärztliche Schweigepflicht und der damit verbundene Schutz aller personenbezogener Daten ist integraler Bestandteil der Praxispolitik und leistet einen unverzichtbaren Beitrag zum Erfolg der Praxis. Datenschutz und Schweigepflicht sind an den Geschäftszielen ausgerichtet und werden von der Praxisleitung verantwortet.

Die Standard-Datenschutzmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis Sensibilität der schützenswerten Daten und Informationen zu Patienten stehen. Datenpannen mit hohen Schäden im Hinblick auf die ärztliche Schweigepflicht müssen verhindert werden. Alle Mitarbeiter der Praxis/Klinik halten die einschlägigen Gesetze (z. B. Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG), Patientendatenschutzgesetz (PDSG) Strafgesetzbuch, Sozialgesetzbuch V), und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für die Praxis/Klinik sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeiter und die Praxisleitung sind sich ihrer Verantwortung beim Umgang mit personenbezogenen Daten bewusst und unterstützen die Datenschutzstrategie nach besten Kräften. Die Praxis-/Klinikleitung und alle Mitarbeiter der Praxis/Klinik sind zur Einhaltung der technischen und organisatorischen Maßnahmen (TOM)verpflichtet. Externe Vertragspartner sind in rechtskonformen Verträgen (siehe AV) ebenso zu verpflichten.

6 Richtlinien

Zur Unterstützung und Konkretisierung der Leitlinien ist es notwendig, weitere Regelungen für die Informationssicherheit und Datenschutz zu verabschieden und in einzelnen Dokumenten, den IS- und DS-Richtlinien, zu sammeln.

6.1 Anforderungen allgemein

6.1.1 Anforderungen Informationssicherheit

Jede IS-Richtlinie muss vom ISB unter Mitarbeit des IST erstellt und von der Praxisleitung in Kraft gesetzt werden.

Der ISB muss jede IS-Richtlinie jährlich auf Aktualität prüfen und ggf. aktualisieren. Bei der Erstellung und Anpassung on IS-Richtlinien müssen alle gesetzlichen, behördlichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.

Die IS-Richtlinien müssen nach jeder Aktualisierung den Zielgruppen zeitnah bekannt gegeben werden.

Dies wird in einer für die Zielgruppe zugänglichen und verständlichen Form geschehen, beispielsweise im Zuge einer Schulung.
IS-Richtlinien müssen umgesetzt oder von der Praxisleitung aufgehoben werden.

6.1.2 Anforderungen Datenschutz

Die Datenschutz-Richtlinie wird von allen Verantwortlichen gemeinsam entwickelt und erstellt. Die Leitung setzt sie anschließend nach den entsprechenden Regeln in Kraft. Es wird in dem Erstellungsprozess geprüft, dass alle gesetzlichen, behördlichen und vertraglichen Anforderungen vollständig umgesetzt werden.

Nach der Verabschiedung bzw. Aktualisierung werden die DS-Richtlinien den beteiligten Zielgruppen zeitnah bekannt gegebenen. Dies erfolgt in einer für die Zielgruppe zugänglichen Form (digital oder analog).

6.2 Inhalte

Die Inhalte der Richtlinien stehen im Vordergrund. Es existieren keine formalen Bedingungen. Die Inhalte entsprechen den Kommunikationsvorgaben in der Praxis (verständliche, positive Formulierungen).

6.2.1 Inhalte Informationssicherheit

Jede IS-Richtlinie erfüllt folgende Anforderungen:

1. Sie enthält, für wen sie verbindlich ist (Zielgruppe)
2. Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll.
3. Sie verstößt nicht gegen Leitlinien oder andere Richtlinien
4. Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

IS-Richtlinien können begründete Ausnahmen ermöglichen, sofern diese im Vorfeld genehmigt und dokumentiert werden.

IS-Richtlinien können auf weitere mitgeltende Dokumente verweisen.

6.2.2 Inhalte Datenschutz

Für die Datenschutz-Richtlinien nach DSGVO und BDSG gelten die folgenden Anforderungen:

1. Sie enthält den Hinweis, für welche Zielgruppen die DS-Richtlinie verbindlich ist.
2. Die DS-Richtlinie enthält eine Begründung für die Erstellung und definiert die Ziele.
3. Die DS-Richtlinien verstoßen nicht gegen andere Leitlinien und Richtlinien
4. Es wird auf die Konsequenzen und Sanktionen bei Nichteinhaltung der Richtlinien nach DSGVO und BDSG hingewiesen.

6.3 Regelungen für Anwender

Die Regelungen für Anwender stellen zentrale Schulungsinhalte für das Team in der Praxis dar. Sie sind deshalb entsprechend verständlich zu formulieren und regelmäßig in ausreichendem Umfang zu schulen (siehe 8.2).

6.3.1 Regelungen für Anwender Informationssicherheit

Es müssen Regelungen für den Umgang mit der IT getroffen werden, die in ihrer Gesamtheit für alle Nutzer (inkl. aller Führungsebenen) sowie für die gesamt IT verbindlich sind:

1. Generelle Nutzungsbedingungen:

    a. Das unrechtmäßige Abrufen oder Verbreiten von urheberrechtlich geschützten Inhalten wird untersagt.

b. Das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten wird untersagt.

2. Privatnutzung:

    a. Es wird definiert, ob die private Nutzung der IT erlaubt ist.
    b. Wenn die private Nutzung der IT erlaubt ist, so wird sie im Sinne der Praxis/Klinik ausgestaltet.

3. Grundlegende Verhaltensweisen:

    a. Es wird nur freigegebene Hard- und Software in der IT-Infrastruktur installiert, genutzt oder betrieben.
    b. Es wird untersagt, eigenmächtig Netzübergänge (wie z.B. Zugänge zum Internet, Fernwartungszugänge oder VPN-Verbindungen) zu installieren; es werden ausschließlich die von der Praxis / Klinik bereitgestellten Netzübergänge genutzt.
    c. Die in der IT-Infrastruktur installierten Sicherheitseinrichtungen werde nicht eigenmächtig deinstalliert, deaktiviert oder in ihrer Konfiguration verändert bzw. mutwillig umgangen.
    d. Authentifizierungsmerkmale werden nicht weitergeben.

4. Umgang mit den Informationen der Praxis / Klinik:

    a. Informationen der Praxis / Klinik werden nicht eigenmächtig verschlüsselt oder vor lesendem Zugriff geschützt; hierfür werden die von der Praxis / Klinik explizit freigegebenen technischen Verfahren genutzt.

5. Informationsfluss bei Abwesenheit:

    a. Es wird geregelt, ob neu eintreffende Nachrichten für einen abwesenden Nutzer weitergeleitet werden.
    b. Es wird geregelt, ob und wann auf den Datenbestand eines Abwesenden zugegriffen werden darf.

6. Missbrauchskontrolle:

    a. Es werden Mechanismen zur Missbrauchskontrolle definiert und den Betroffenen mitgeteilt.

Bei der Umsetzung von Überwachungs- und Protokollierungsmaßnahmen sollten die gesetzlichen Vorgaben, insbesondere die des Datenschutzes, beachtet werden.

Ausnahmen müssen vom ISB genehmigt werden.

6.3.2 Regelungen für Anwender Datenschutz

Die Regelungen gelten für alle Mitarbeiter einschließlich Leitung und Stellvertretung. Im Einzelnen:

1. Personenbezogene Daten werden nur nach Anweisung verarbeitet. Es werden ausschließlich die von der Leitung bereitgestellten Verarbeitungsabläufe genutzt.
2. Besteht ein Bedarf für weitergehende Verarbeitung, so werden die Verantwortlichen, je nach Anforderung, einbezogen.
3. Die Mitarbeiter halten alle Anforderungen und betreffenden Maßnahmen zur Sicherheit personenbezogener Daten ein und setzen diese gemäß der Regelungen um.
4. Mögliche Datenschutzvorfälle werden von den Mitarbeitern umgehend an die Verantwortlichen für den Datenschutz gemeldet.

Bestehen begründete Anforderungen für Ausnahmen, so sind diese im Vorfeld von den Verantwortlichen zu genehmigen und mit entsprechender Begründung zu dokumentieren.

6.4 Regelungen allgemein

Es wird sichergestellt, dass für alle relevanten Verarbeitungen und Prozesse gültige Regelungen zur Verfügung stehen und für alle Mitarbeiter verfügbar sind.

6.4.1 Regelungen allgemein Informationssicherheit

Im Rahmen dieser Richtlinien müssen gegebenenfalls weitere themenspezifische Richtlinien und Verfahrensanweisungen erarbeitet werden.

1. Mobile IT-Systeme (siehe Abschnitt 10.4)
2. Mobile Datenträger (siehe Abschnitt 12.1)
3. IT-Outsourcing und Cloud Computing (siehe Abschnitt 14.1)
4. Datensicherung (siehe Abschnitt 16.1)
5. Störungen und Ausfälle (siehe Abschnitt 17.1)
6. Sicherheitsvorfälle (siehe Abschnitt 18.1)
7. Telematikinfrastruktur Anwendung
8. Medizintechnik Nutzung

Der Bedarf für weitere Richtlinien muss jährlich vom ISB ermittelt werden.

6.4.2 Regelungen allgemein Datenschutz

Die Datenschutz-Richtlinien werden für alle Verarbeitungen festgelegt und gelten in der gesamten Organisationseinheit:

1. Die personenbezogenen Daten werden nur auf der Grundlage einer Einwilligung der Betroffenen oder einer anderen gültigen Rechtsgrundlage verarbeitet (Prinzip der Rechtmäßigkeit)
2. Die personenbezogenen Daten werden ausschließlich für eindeutige und genau festgelegte Zwecke verarbeitet. Wenn der Verwendungszweck geändert wird, wird vorab die rechtliche Zulässigkeit geprüft und falls notwendig die Einwilligung der Betroffenen eingeholt (Zweckbindung)
3. Die Verarbeitung wird nur durchgeführt, wenn der Prozess zu Zielerreichung geeignet, erforderlich und angemessen ist (Prinzip der Verhältnismäßigkeit)
4. Betroffene Personen werden über die Verwendung der personenbezogenen Daten umfassend und verständlich informiert (Transparenz).
5. Nur die tatsächlich benötigten personenbezogenen Daten werden verarbeitet (Datenminimierung)
6. Um unrichtige personenbezogene Daten zu vermeiden und zu erkennen werden geeignete Maßnahmen etabliert. Unkorrekte Daten werden korrigiert oder gelöscht (Richtigkeit der Daten).
7. Sobald personenbezogene Daten nicht mehr benötigt werden, sind diese zu löschen. Dabei ist eine eventuell bestehende Aufbewahrungspflicht (z.B. bei personenbezogenen medizinischen Daten) unbedingt zu beachten (Speicherbegrenzung).
8. Im Rahmen einer Risikoanalyse werden Maßnahmen zur Sicherstellung der Vertraulichkeit, der Integrität und der Verfügbarkeit der personenbezogenen Daten umgesetzt (Vertraulichkeit, Integrität und Verfügbarkeit der Daten).
9. Eingesetzte Systeme, Produkte (z.B. Software und Prozesse werden unter dem Gesichtspunkt der Datenschutzfreundlichkeit ausgewählt und implementiert (Datenschutz by Design, Privacy by Default).
10. In einer Dokumentation wird die Einhaltung aller Datenschutz-Richtlinien festgeschrieben und für Jahresberichte bzw. Audits vorgehalten.

6.5 Weitere Regelungen und Richtlinien

Weitere Regelungen und Richtlinien gelten in Abhängigkeit der Besonderheiten der Organisationseinheiten. Dies gilt beispielweise dann, wenn besondere Risiken bestehen.

6.5.1 Weitere Richtlinien Informationssicherheit

Für bestimmt Branchen und Zielgruppen gelten spezielle Richtlinien. Sie orientieren sich an branchenspezifischen Regelungen, Vorschriften und Empfehlungen.

Dies gilt für die Informationssicherheit z.B. für:

1. Besondere digitale Kommunikationsstrukturen (z.B. Telematikinfrastruktur in der medizinischen Versorgung)
2. Anwendung von Medizintechnik mit Risiken für die Informationssicherheit
3. Einsatz cloudbasierten Software-Applikation z.B. Gesundheits-Apps.

6.5.2 Weitere Richtlinien und Regelungen für den Datenschutz

Für den Datenschutz gelten besondere Regelungen z.B. für:

1. Zutritts- und Zugangsprozesse
2. Private Nutzung von IT-Einrichtungen
3. Abwesenheitsregelungen
4. Datenschutz im Home-Office
5. Integration private IT-Systeme (BYOD = Bring your own device)

7 Human Ressources

Die Mitarbeiter sind der zentrale Faktor für die Implementierung und Aufrechterhaltung der Informationssicherheit und des Datenschutzes. Es ist deshalb notwendig, folgende Anforderungen der Informationssicherheit und des Datenschutzes zu berücksichtigen und im Rahmen der wirtschaftlichen und personellen Kapazitäten zu erfüllen.

7.1 Vor Tätigkeitsaufnahme

7.1.1 Vor Tätigkeitsaufnahme Informationssicherheit

Wenn eine für die Informationssicherheit relevante Position besetzt wird, muss die Praxis / Klinik sicherstellen, dass der Bewerber über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.

7.1.2 Vor Tätigkeitsaufnahme Datenschutz

Der Faktor Mensch spielt im Datenschutz eine zentrale Rolle. Bevor eine Position besetzt wird, ist sicher zu stellen, dass der Bewerber über die notwendige Eignung, die erforderliche Vertrauenswürdigkeit und die Kenntnisse zum Datenschutz (Grundlagen DSGVO/BDSG) verfügt.

7.2 Tätigkeitsaufnahme

Für die Einstellung neuer Mitarbeiter gelten besondere Prozesse zur Einhaltung der Informationssicherheit und des Datenschutzes.

7.2.1 Tätigkeitsaufnahme Informationssicherheit

Es muss ein Verfahren (siehe Anhang) implementiert werden, welches im Zuge der Aufnahme der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:

1. Mitarbeiter verpflichten sich mittels einer schriftlichen Erklärung zur Vertraulichkeit; die Erklärung definiert auch die Pflichten in Bezug auf Informationssicherheit, die nach Beendigung oder Veränderung des Arbeitsverhältnisses fortbestehen.
2. Mitarbeiter werden in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit (wie z.B. in die Inhalte entsprechender Richtlinien und Verfahren) eingewiesen.
3. Mitarbeiter werden im Umgang mit den für sie relevanten Sicherheitsmaßnahmen geschult (siehe Abschnitt 8.2)

4. Mitarbeiter erhalten die benötigten IT-Ressourcen, Zugänge und Zugriffsrechte und werden in deren Nutzung geschult.

7.2.2 Tätigkeitsaufnahme Datenschutz

Im Rahmen der Einstellung und Einarbeitung von neuen Mitarbeitern besteht ein strukturiertes Verfahren zur Sicherstellung der folgenden Anforderungen:

1. Neue Mitarbeiter verpflichten sich mit einer schriftlichen Erklärung zur Vertraulichkeit. Diese definiert insbesondere die Pflichten in Bezug auf den Datenschutz, die auch nach Beendigung des Arbeitsverhältnisses fortbestehen.
2. Die neuen Mitarbeiter werden in die Datenschutz-Leitlinie und alle DS-Richtlinien eingewiesen.
3. Die neuen Mitarbeiter erhalten Schulungen, die sie befähigen alle Regelungen zum Datenschutz qualifiziert umzusetzen.

7.3 Tätigkeitsbeendigung oder -wechsel

Bei der Beendigung eines Arbeitsverhältnisses sind besondere Prozesse durchzuführen, um auch nachvertraglich die Informationssicherheit und den Datenschutz zu gewährleisten.

7.3.1 Tätigkeitsbeendigung oder – wechsel Informationssicherheit

Es ist ein Verfahren (siehe Anhang A1) implementiert, das bei Beendigung oder Wechsel der Tätigkeit eines Mitarbeiters folgende Punkte sicherstellt:

1. Soweit erforderlich werden Mitarbeiter, Kunden sowie relevante externe Stellen über die Änderung informiert.
2. Die zur Verfügung gestellten IT-Ressourcen, Zugänge und Zugriffsrechte des Mitarbeiters werden umgehend überprüft und bei Bedarf angepasst.

7.3.2 Tätigkeitsbeendigung oder -wechsel Datenschutz

Es ist ein Verfahren implementiert, dass bei Beendigung oder Wechsel einer Anstellung folgende Regelungen implementiert:

1. Über die Beendigung einer Anstellung werden andere Mitarbeiter, Kunden / Patienten, Lieferanten und Auftragsverarbeiter über Änderungen im betrieblichen Bereich informiert.
2. Die Zugriffmöglichkeiten des ausscheidenden Mitarbeiters auf personenbezogene Daten werden umgehend überprüft und technisch und organisatorisch ausgeschlossen.

8 Wissensmanagement

Viele Gefährdungen entstehen aus Unkenntnis oder mangelndem Problembewusstsein oder werden zumindest durch diese Faktoren verstärkt. Deshalb ist es notwendig, dass die Praxis / Klinik über aktuelles Wissen in Bezug auf Informationssicherheit verfügt, die Mitarbeiter ihre Verantwortlichkeiten verstehen und für ihre Aufgaben geeignet und qualifiziert sind.

8.1 Aktualität des Wissens

8.1.1 Aktualität des Wissens Informationssicherheit

Es ist ein Verfahren (siehe Anhang A1) implementiert, mit dem alle relevanten Stellen der Praxis / Klinik sowie gegebenenfalls relevante externe Stellen in geeigneter Weise über geänderte rechtliche und technische Bedingungen im Bereich der Informationssicherheit informiert werden.

Das Verfahren stellt folgende Punkte sicher:

1. Es werden regelmäßig aus verlässlichen Quellen Informationen über die aktuellen technischen und rechtlichen Entwicklungen im Bereich der Informationssicherheit, insbesondere über neue Gefährdungen und mögliche Gegenmaßnahmen bezogen.

2. Die Informationen werden im Hinblick auf die Bedeutung für die Informationssicherheit zeitnah ausgewertet, um geänderte Gefahrenlagen zu erkennen.

3. Die jeweils Verantwortlichen werden über relevante Entwicklungen zeitnah informiert.

   Es stehen Newsletter und Notfall-Informationen mit aktuellen Informationen zur Verfügung.

8.1.2 Aktualität des Wissens Datenschutz

Für den Datenschutz stellen die eingerichteten Verfahren folgendes sicher:

1. Aus verlässlichen Quellen stehen regelmäßig aktuelle Informationen zu technischen, organisatorischen und rechtlichen Entwicklungen für den Datenschutz zur Verfügung. Dies bezieht sich beispielsweise auf Informationen der Datenschutzbehörden

2. In Abhängigkeit von der Bedeutung neuer Entwicklungen werden diese von den Verantwortlichen zeitnah ausgewertet und dem gesamten Team zur Verfügung gestellt.
3. Die jeweils Verantwortlichen werden in den Informationsprozess einbezogen.

Es empfiehlt sich für die Verantwortlichen im Datenschutz ständig Kontakte zu Interessensgruppen zu pflegen und auch geeignete Schulungsmaßnahmen in die Trainingsplanung einzubeziehen (z.B. Webinare).

8.2 Sensibilisierung und Schulung

Nach allgemein anerkannten Statistiken und Umfrageergebnissen werden Verstöße gegen die Informationssicherheit und des Datenschutzes zu mehr als 70% durch den „Faktor Mensch“ ausgelöst. Der gezielten Schulung und Sensibilisierung aller Beteiligten kommt deshalb die höchste Priorität zu.

In einem Curriculum werden die geeigneten Schulungs- und Fortbildungsmaßnahmen zur Informationssicherheit und zum Datenschutz geplant und für alle Beteiligten transparent festgelegt.

8.2.1 Sensibilisierung und Schulung Informationssicherheit

Es besteht ein Verfahren (siehe Anlage A1) für Schulungs- und Sensibilisierungsmaßnahmen, das folgende Punkte sicherstellt:

1. Sie werden regelmäßig nach dem Praxis-Curriculum sowie bei Bedarf durchgeführt.

2. Ihre Art und ihr Intervall werden zielgruppenorientiert festgelegt (Patientenversorgung, Verwaltung etc.)

3. Sie vermitteln in ihrer Gesamtheit die Inhalte der IS-Leitlinie und sämtlicher für die Zielgruppe relevanter Regelungen zur Informationssicherheit (wie z.B. die Inhalte entsprechender IS-Richtlinien und Verfahren).

4. Sie klären über Gefährdungen auf und schulen den Umgang mit den vorhandenen Sicherheitsmaßnahmen sowie das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen.

5. Sie vermitteln den Teilnehmern ihre Verantwortung für die Informationssicherheit und fördern bei ihnen die Akzeptanz der Sicherheitsmaßnahmen.

6. Ihre Inhalte und die Teilnahme an ihnen werden dokumentiert.

Schulungs- und Sensibilisierungsmaßnahmen schließen mit einer Lernerfolgskontrolle, um das Verständnis der Teilnehmer und den Bedarf weiterer Schulungs- oder Sensibilisierungsmaßnahmen zu ermitteln, ab.

Schulungs- und Sensibilisierungsmaßnahmen werden von den Teilnehmern bewertet, um ihren Inhalt, ihre Form und ihren Ablauf verbessern zu können.

8.2.2 Sensibilisierung und Schulung Datenschutz

Auch für den Bereich des Datenschutzes (siehe Anlage A1) bestehen Verfahren zur Sicherstellung aller geeigneter Sensibilisierungs- und Schulungsmaßnahmen mit den folgenden Punkten:

1. Alle Mitarbeiter werden regelmäßig (siehe Curriculum) und zielgruppenorientiert über ihre gesetzlichen und betrieblichen Pflichten bei der Anwendung der vorhandenen Datenschutzmaßnahmen geschult.
2. Inhalte der Leitlinien und den Datenschutz-Richtlinien werden regelmäßig oder bei aktuellem Bedarf zeitnah und qualifiziert vermittelt.
3. Mitarbeiter werden über die Konsequenzen bei Zuwiderhandlung gegen verbindliche Vorgaben informiert und aufgeklärt.

8.3 Curriculum und Fortbildung

8.3.1 Curriculum und Fortbildung Informationssicherheit

Der Schulungsplan zur Umsetzung der Informationssicherheit wird in einem Curriculum zentral für Praxis / Klinik umgesetzt. Das Curriculum richtet sich nach der aktuellen Situation der Organisationseinheit und wird aus der Qualifikation der Mitarbeiter, der freien Kapazitäten und der zeitlichen Ziele abgeleitet.

Die Mitarbeiterqualifikation wird in regelmäßigen Abständen überprüft. Das Fortbildungscurriculum wird nach den Ergebnissen der internen bzw. externen Audits festgelegt und für einen Zeitraum von 2 – 3 Jahren geplant.

8.3.2 Curriculum und Fortbildung Datenschutz

Der übergeordnete Schulungsplan synchronisiert in einem Curriculum alle Schulungsmaßnahmen und enthält alle wesentlichen Elemente zur Aktualisierung des Wissen im Datenschutz nach DSGVO und BDSG.

9 Ressourcen IT-Infrastruktur

Der ISB ermittelt die kritischen IT-Ressourcen der Praxis / Klinik und prüft jährlich mindestens einmal, ob die Aufstellung der kritischen IT-Ressourcen aktuell ist und wird sie bei Bedarf anpassen.

Die Praxis / Klinik führt bei Bedarf eine Informationsklassifizierung auf Basis eines anerkannten Standards wie ISO / IEC 27001 oder eine Schutzbedarfsanalyse gemäß BSO-Standard 200-2 durch.

Wenn eine andere Vorgehensweise gewählt wird, so wird hierfür ein Verfahren (siehe Anhang A1) implementiert, welches die Anforderungen folgender Abschnitte erfüll.

9.1 Prozesse

9.1.1 Prozesse Informationssicherheit

Die Praxis / Klinik muss ihre zentralen Prozesse und ihre Prozesse mit hohem Schadenspotential identifizieren und dokumentieren.

Die Dokumentation muss folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung des Prozesses (Verfahrensanweisung)
2. Sie begründet, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohem Schadenspotential ist.
3. Sie enthält, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).
4. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) des Prozesses.

Die Aufstellung der Prozesse und deren Dokumentation wird von der Praxisleitung geprüft und freigegeben.

9.1.2 Prozesse Datenschutz

Alle in der Praxis/Klinik vorkommenden relevanten Prozesse mit personenbezogenen Daten sind zu identifizieren und zu dokumentieren.

Die Dokumentation muss folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung des Prozesses (Verfahrensanweisung)

2. Sie begründet, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohen Datenschutzanforderungen ist.

3. Sie enthält, wer für den Prozess verantwortlich ist (Prozessverantwortlicher).

Die Aufstellung der Prozesse und deren Dokumentation wird von der Praxisleitung geprüft und freigegeben.

9.2 Informationen und Daten

Die Praxis / Klinik ermittelt, welche kritischen Informationen und Daten sie verarbeitet, überträgt und / oder speichert und dokumentiert diese.

Kritische Informationen sind Informationen, bei denen folgende Faktoren zu sehr hohen Schäden führen können.

1. Unberechtigte Einsicht, Kenntnisnahme oder Weitergabe (Kriterium „Vertraulichkeit“)

2. Verfälschung (Kriterium „Integrität“)

3. Datenverlust von weniger als 24 Stunden (Kriterium „maximal tolerierbarer Datenverlust – MTD“)

4. Nichtverfügbarkeit im Echtzeitbetrieb (Kriterium „unmittelbare Verfügbarkeit“)

Hierfür werden die zentralen Prozesse und die Prozesse mit hohem Risikopotential (siehe Abschnitt 9.1.) untersucht.

Die Dokumentation soll folgende Anforderungen erfüllen:

1. Sie enthält die Kriterien, anhand derer die Informationen als kritisch eingestuft wurden.
   Kritische Informationen sollten anhand ihrer qualitativen und quantitativen Merkmale beschrieben werden. Qualitative Merkmale definieren die Eigenschaften der kritischen Informationen. Quantitative Merkmale definieren, ab welcher Menge die Informationen mit den genannten Eigenschaften kritisch sein. Die Erfassung quantitativer und qualitativer Merkmale bietet die Möglichkeit, kritische Informationen zuverlässig zu erfassen.

2. Sie begründet, warum die Informationen kritisch sind.

Die Aufstellung der kritischen Informationen und deren Dokumentation muss von der Praxisleitung geprüft und freigegeben werden.

9.3 Ressourcen

9.3.1 IT-Ressourcen

Die Praxis / Klinik ist verpflichtet, ihre kritischen IT-Ressourcen (insbesondere die kritischen IT-Systeme, mobilen Datenträger, Verbindungen sowie die kritische Individualsoftware) zu bestimmen und diese zu dokumentieren.

Kritische IT-Ressourcen sind IT-Ressourcen, die kritische Informationen (siehe Abschnitt 9.2) verarbeiten, speichern oder übertragen oder die für den Betrieb von kritischen IT-Ressourcen zwingend benötigt werden.

Die Dokumentation soll folgende Anforderungen erfüllen:

1. Sie enthält eine kurze Beschreibung der kritischen IT-Ressource

2. Sie begründet, warum die IT-Ressource kritisch ist

3. Sie enthält die maximal tolerierbare Ausfallzeit (MTA) der IT-Ressource.

Die MTA soll ebenso kurz oder kürzer sein, als die kürzeste MTA aller zentralen Prozesse und Prozesse mit hohem Schadenspotential (siehe Abschnitt 9.1), die von der kritischen IT-Ressource direkt oder indirekt abhängig sind.

Die Aufstellung der kritischen IT-Ressourcen und deren Dokumentation wird vom IT-Verantwortlichen freigegeben.

9.3.2 Personenbezogene Daten Datenschutz

Die Praxis/Klinik ermittelt für jede Verarbeitung (siehe 9.2) welche Kategorie personenbezogener Daten verarbeitet werden.
Es wird geprüft, ob die Ergebnisse mit dem Verarbeitungsverzeichnis übereinstimmen.
Alle bereits vorliegenden Dokumentationen in der Praxis/Klinik werden in die Ermittlung einbezogen.

10 IT-Systeme

Die Informationsverarbeitung einer Praxis / Klinik geschieht zum größten Teil elektronisch. Es ist deshalb notwendig, IT-Systeme strukturiert zu verwalten und abzusichern.

10.1 Bestandsaufnahme und Inventarisierung

Es muss eine Inventarisierung vorhanden sein, in der alle IT-Systeme der Praxis / Klinik verzeichnet sind.

Die Inventarisierung muss durch entsprechende Verfahren (siehe Abschnitte 10.2.1 und 10.2.2) vollständig und aktuell gehalten werden.

In ihr sollen folgende Informationen für jedes IT-System verzeichnet sein:

1. Eindeutiges Identifizierungsmerkmal
2. Informationen, die eine schnelle Lokalisierung erlauben
3. Einsatzzweck

Darüber hinaus sollten für jedes IT-System weitere Informationen erhoben und aktuell gehalten werden, wie z.B. Namen, Versionen und Lizenzinformationen der installierten System- und Anwendungssoftware, Seriennummern von Hardwarekomponenten sowie Informationen über Garantieren und Serviceverträge.

Besonderheiten der Installation und Konfiguration sollten in einer Dokumentation verzeichnet sein.

10.2 Lebenszyklus der Systeme

IT-Systeme bilden eine abgeschlossene Funktionseinheit aus Hard- und Software (siehe Abschnitt 10.3). Sie unterliegen einem Lebenszyklus, der sich üblicherweise von der Inbetriebnahme bis zu deren Ausmusterung erstreckt.

10.2.1 Inbetriebnahme und Änderung

Es soll ein Verfahren (siehe Anhang A1) für die Inbetriebnahme und Änderung der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:

1. Es wird ermittelt, ob das IT-System kritisch ist (siehe Abschnitt 9.3)

2. Der Basisschutz (siehe Abschnitt 10.3) wird umgesetzt.

3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.

4. Bei Inbetriebnahme werden die Arbeitsschritte dokumentiert.

10.2.2 Ausmusterung und Wiederverwendung

Es muss ein Verfahren (siehe Anhang A1) für das Ausmustern und Wiederverwenden der IT-Systeme implementiert werden, das folgende Punkte sicherstellt:

1. Die auf dem IT-System gespeicherten Informationen werden bei Bedarf gesichert bzw. archiviert.

2. Alle Informationen werden vor unrechtmäßigem Zugriff geschützt, indem sie z.B. zuverlässig gelöscht, überschrieben, aus dem IT-System entfernt werden oder indem das IT-System insgesamt zerstört wird.

3. Die Inventarisierung der IT-Systeme (siehe Abschnitt 10.1) und der Netzwerkplan (siehe Abschnitt 11.1) werden aktualisiert.

4. Bei Ausmusterung werden die Arbeitsschritte dokumentiert.

10.3 Basisschutz

Die Maßnahmen der folgenden Abschnitte müssen, sofern eine entsprechende Funktionalität gegeben ist, für alle IT-Systeme implementiert werden.

Wenn eine entsprechende Funktionalität nicht gegeben ist. Sollte dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Abschnitt A2) begegnet werden.

10.3.1 Software

System- und Anwendungssoftware darf ausschließlich aus vertrauenswürdigen Quellen bezogen werden.

Es darf ausschließlich System- und Anwendungssoftware eingesetzt werden, die Sicherheitsupdates des Herstellers enthält.

Es darf nur Software auf IT-Systemen installiert werden, die zur Aufgabenerfüllung benötigt wird; nicht benötigte Software sollte deinstalliert werden.

Sämtliche Zugriffsrechte und Privilegien der Anwendungssoftware werden auf ein Mindestmaß reduziert.

Vom Hersteller zur Verfügung gestellte Sicherheitsupdate für die System- und Anwendungssoftware müssen nach einem implementierten Verfahren (siehe Anhang A1) getestet, bei Eignung freigegeben und nach ihrer Freigabe umgehend installiert werden.

10.3.2 Beschränkung des Netzwerkverkehrs

Der Netzwerkverkehr von und zu IT-Systemen muss auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden, wenn eines der folgenden Kriterien zutrifft:

1. Es existieren über das Netzwerk ausnutzbare Schwachstellen, die nicht behoben werden (z.B., wenn keine Sicherheitsupdates installiert werden können, Authentifizierungsmerkmale nicht geändert werden können oder unsichere technische Verfahren eingesetzt werden).

2. Es handelt sich um besonders exponierte IT-Systeme (z.B. um IT-Systeme, die aus dem Internet erreichbar, oder die in öffentlich zugänglichen Räumen platziert sind oder die in weniger vertrauenswürdigen Umgebungen eingesetzt werden).

Zusätzlich sollte der Netzwerkverkehr von und zu IT-Systemen, für die die Praxis / Klinik keinen administrativen Zugang besetzt, auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden.

Die Beschränkung des Netzwerkverkehrs kann beispielsweise durch eine geeignete Segmentierung des Netzwerks (siehe Abschnitt 11.4.2), lokale Filtermechanismen oder durch das Deaktivieren nicht benötigter Dienste erfolgen.

10.3.3 Protokollierung und Dokumentation

Jedes IT-System muss erfolgreiche und erfolglose Anmeldeversuche, Fehler und Informationssicherheitsereignisse protokollieren.

Protokolldaten sollten zentral gespeichert werden.

Protokolldaten müssen 6 Monate lang aufbewahrt werden, sofern keine gesetzlichen Lösch- oder Aufbewahrungspflichten entgegenstehen.

Die Uhren aller IT-Systeme müssen auf eine gemeinsame Zeit synchronisiert sein, um Auswertungen von Logeinträgen zu ermöglichen.

10.3.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, werden ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht.

10.3.5 Schadsoftware

Alle IT-Systeme müssen über einen Schutz vor Schadsoftware verfügen.

Jedes IT-System muss mit Hilfe geeigneter Software täglich vollständig auf Anwesenheit von Schadsoftware untersucht werden.

Darüber hinaus sollten alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien bei Zugriff auf Schadsoftware prüft.

Bei IT-Systemen mit einem Echtzeitschutz kann die vollständige Untersuchung auf Schadsoftware auf einen wöchentlichen Rhythmus reduziert werden.

Das Ausführen erkannter Schadsoftware muss verhindert werden.

Die Software zum Schutz gegen Schadsoftware muss automatisch in kurzen zeitlichen Abständen (z.B. stündlich oder täglich) nach den neuesten Suchmustern der Hersteller suchen und diese verwenden.

10.3.6 Starten von fremden Medien

Es muss sichergestellt werden, dass IT-Systeme nur von autorisierten Medien gestartet werden können.

Dies kann z.B. über BIOS-Passwörter oder über einen Zutrittsschutz umgesetzt werden.

10.3.7 Authentifizierung

Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme muss durch geeignete Anmeldeverfahren abgesichert werden, die eine Authentifizierung verlangen.

Die Anmeldeverfahren müssen folgende Punkte sicherstellen:

1. Das systematische Ausprobieren von Anmeldeinformationen wird erschwert.

2. Interaktive Sitzungen werden beendet oder gesperrt, wenn der Nutzer innerhalb einer vorgegebenen Zeitspanne keine Eingaben tätigt.

3. Erfolgt die Anmeldung über ein Netzwerk, so wird die Vertraulichkeit und Integrität der Anmeldeinformationen (z.B. mit Hilfe entsprechender Authentifizierungsprotokolle) sichergestellt.

Damit die Anmeldeverfahren zuverlässig arbeiten können, müssen folgende Punkte sichergestellt werden:

1. Zugänge werden strukturiert verwaltet (siehe Kapitel 15)

2. Es werden zuverlässige Authentifizierungsmechanismen verwendet.

3. Es werden keine trivialen Authentifizierungsmerkmale (z.B. Standard-Passwörter oder einfach zu erratende Passwörter) verwendet.

Es sollte Mehr-Faktor-Authentifizierung eingesetzt werden, um die Gefahr eines unberechtigten Zugangs zu verringern, insbesondere wenn Nutzer umfangreiche Zugriffsrechte besitzen.

10.3.8 Zugänge und Zugriffe

Es wird sichergestellt, dass Nutzer keine administrativen Arbeiten durchführen können.

Dies kann mit Hilfe getrennter Zugänge und geeigneter Zugriffsrechte umgesetzt werden.
Darüber hinaus sollten folgende Anforderungen erfüllt werden:

1. Nutzer können nur auf Informationen lesend zugriefen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Need-to-Know“)
2. Nutzer können nur auf Informationen schreibend zugreifen, wenn dies für die Erfüllung ihrer Aufgaben notwendig ist („Least-Privileges“).

10.4 Mobile IT-Systeme

Mobile IT-Systeme sind in besonderer Weise Gefährdungen durch Diebstahl, unautorisiertem Zutritt oder unsichere Netze ausgesetzt, die zusätzliche Maßnahmen erforderlich machen.

Folgende Maßnahmen müssen für alle mobilen IT-Systeme umgesetzt werden.

10.4.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3. müssen in einer IS-Richtlinie Regelungen für den Umgang mit mobilen IT-Systemen getroffen werden:

1. Es wird festgelegt, welche Informationen auf den mobilen IT-Systemen erhoben, verarbeitet, gespeichert und übertragen werden dürfen.

2. Die Verantwortung für die Datensicherung wird definiert.

3. Die Nutzer werden über die spezifischen Risiken mobiler IT-Systeme (z.B. Gefahren durch Ausspähung bei der Nutzung in der Öffentlichkeit, Verlust oder Diebstahl) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.

4. Es wird untersagt, mobile IT-Systeme an unberechtigte Dritte weiterzugeben.

5. Es wird definiert, ob und welche Software auf den mobilen IT-Systemen von den Nutzern installiert werden darf.

6. Es wird definiert, ob und unter welchen Bedingungen ein Administrator das mobile IT-System orten darf.

7. Es wird definiert, ob und unter welchen Bedingungen ein Administrator die auf einem mobilen IT-System gespeicherten Informationen aus der Ferne löschen darf.

10.4.2 Schutz der Informationen

Die auf dem mobilen IT-System gespeicherten Informationen der Praxis / Klinik vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

Der Schutz der Vertraulichkeit kann z.B. durch eine Verschlüsselung der Datenträger erreicht werden.

10.4.3 Verlust der Informationen

Es müssen Verfahren (siehe Anhang A1) implementiert werden, die festlegen, wie Nutzer und Administratoren bei Verlust eines mobilen IT-Systems vorzugehen haben.

Die Verfahren müssen insbesondere festlegen, wie und an wen der Verlust zu melden ist und welche Sofortreaktion erfolgt.

Die Verfahren müssen sicherstellen, dass die auf dem gerät hinterlegten Zugänge der Praxis / Klinik nach der Verlustmeldung nicht unberechtigt genutzt werden können (z.B. indem die entsprechenden Authentifizierungsmerkmale umgehend zurückgesetzt oder indem Anrufweiterleitungen modifiziert sowie Sprachnachrichten gelöscht werden).

Der Verlust eines mobilen IT-Systems muss als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

10.5 Kritische IT-Systeme

Folgende Maßnahmen müssen zusätzlich für alle kritischen IT-Systeme umgesetzt werden.
Wenn Maßnahmen nicht umgesetzt werden, muss dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A2) begegnet werden.

10.5.1 Risikoanalyse und Behandlung

Für kritische IT-Systeme muss eine Risikoanalyse und –Behandlung etabliert werden (siehe Anhang A2)

10.5.2 Notbetriebsmanagement

Für jedes kritische IT-System sollte ein Notbetriebsniveau definiert werden.

10.5.3 Robustheit

Auf kritischen IT-Systemen dürfen keine Entwicklungen oder Tests durchgeführt werden.

Auf kritischen IT-Systemen müssen alle Netzwerkdienste, die nicht zur Aufgabenerfüllung benötigt werden, deinstalliert, abgeschaltet oder durch geeignete Filtermechanismen unzugänglich gemacht werden.

10.5.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, müssen ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden.

10.5.5 Änderungsmanagement

Änderungen, die auf kritischen IT-Systemen umgesetzt werden sollen, müssen zuvor in einer Testumgebung getestet und freigegeben worden sein.

Für kritische IT-Systeme muss ein Mechanismus vorhanden sein, der sicherstellt, dass bei einer Fehlfunktion oder einem Ausfall des IT-Systems aufgrund einer Änderung sein ursprünglicher Zustand innerhalb seiner MTA wiederhergestellt werden kann, sofern keine Ersatzsysteme oder -verfahren verfügbar sind (siehe Abschnitt 10.5.9).

10.5.6 Dokumentation

Für jedes kritische IT-System muss eine Dokumentation vorhanden sein.

Anhand der Dokumentation muss es fachlich versierten Personen möglich sein, folgende Punkte nachzuvollziehen:

1. Wer für das IT-System verantwortlich ist
2. Wie und mit welchen Zugängen und Authentifizierungsmerkmalen der administrative Zugang zum IT-System möglich ist.
3. Welche grundlegenden Designerentscheidungen bei der Installation getroffen wurden
4. Welche Änderungen vorgenommen wurden
5. Wann sie vorgenommen wurden
6. Wer sie vorgenommen hat
7. Warum sie vorgenommen wurden

10.5.7 Datensicherung und -rekonstruktion

Alle kritischen IT-Systeme müssen über eine Datensicherung (Abschnitt 16.6)

10.5.8 Überwachung und Kontrolle

Es muss überwacht werden, ob sich kritische IT-Systeme im Regelbetrieb befinden. Dabei muss sichergestellt werden, dass der Ausfall eines kritischen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden.

Darüber hinaus werden die Ressourcen kritischer IT-Systeme überwacht, um Engpässe zu erkennen, bevor sie akut werden.

10.5.9 Ersatzsysteme und Verfahren

Wenn ein kritisches IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, muss die Praxis / Klinik über ein Ersatzsystem oder -verfahren verfügen, das es ermöglicht, die vom kritischen IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential weiter zu betreiben.

Das Ersatzsystem oder -verfahren sollte das Notbetriebsniveau (siehe Abschnitt 10.5.2) des kritischen IT-Systems sicherstellen.

10.5.10 Kritische Individualsoftware

Die Praxis / Klinik muss durch vertragliche und / oder organisatorische Regelungen sicherstellen, dass sie kritische Individualsoftware auch in Zukunft verwenden und ihren Bedürfnissen anpassen kann.

10.6 IT-Spezialanwendungen in Arztpraxen

In der Praxis / Klinik werden umfangreiche Softwareanwendungen eingesetzt, die ca. 90% aller IT-Applikationen ausmachen. Die Anwendungen sind in der Inventarisierung dokumentiert. Es handelt sich dabei um Software, häufig mit Zertifizierung, und Hardware-Komponenten wie beispielsweise Konnektoren, Chipkarten-Lesegeräte.

10.6.1 Telematikinfrastruktur (TI)

Die TI-Einführung wurde 2020 zur Pflicht und stellt hohe Anforderungen an die Informationssicherheit. Die Praxis ist verantwortlich für die Anwendung innerhalb der Praxis / Klinik bis zum Konnektor, der die Verbindung zum TI-Netzwerk nach außen herstellt. Für die TI-Informationssicherheit selbst ist die Gematik als Partner der Kassenärztlichen Bundesvereinigung (KBV) zuständig und verantwortlich.

Die Betreuung vor Ort erfolgt über den DLO (Dienstleister vor Ort). Dieser muss nachweislich über die Qualifikation, die von KBV vorausgesetzt wird, verfügen. Der Grundlagenvertrag DLO Kooperation befindet sich im Anhang.

10.6.2 Abrechnungsprogramme

In der Praxis / Klinik erfolgt die Abrechnung mit Patienten im Regelfall papierlos. Es werden drei Abrechnungspatientengruppen unterschieden.

10.6.2.1 KV-Abrechnung

Die Patienten, die nach der GKV versorgt werden (Kassenpatienten), werden über die Kassenärztlichen Vereinigungen in den Bundesländern abgerechnet. Die für die GKV Patienten erbrachten Leistungen werden digital über die Telematik Infrastruktur kommuniziert. Die Patienten selbst identifizieren sich mit einer GKV Chipkarte, deren Daten mit einem lokalen Lesegerät erfasst und in das PVS (Praxisverwaltungssystem) übertragen werden. Die datenschutzrechtlichen und Informationssicherheits-relevanten Abläufe werden in Verfahrensanweisungen dokumentiert.

10.6.2.2 Privatliquidation

Privatpatienten, die nach der Gebührenordnung für Privatliquidation (GOÄ) abgerechnet werden, erhalten ihre Rechnungen direkt postalisch oder digital. In der Mehrzahl erfolgt die Abrechnung über Privatärztliche Verrechnungsstellen (PVS), die die Abrechnungsdaten elektronisch übermittelt bekommen. Für die Informationssicherheit werden die Abläufe in Richtlinien und Verfahrensanweisungen verwaltet.

10.6.2.3 IGeL Abrechnung

Patienten, die die sogenannte Individuelle Gesundheitsleistungen (IGeL) in Anspruch nehmen, erfolgt die Abrechnung lokal in der Praxis über elektronische Zahlungssysteme (EC-Karten, Kreditkarten, PayPal etc.).

10.6.3 Elektronische Patientenakte (EPA / PVS)

Die Elektronische Patientenakte wird auf der rechtlichen Grundlage des PDSG (Patientendatenschutzgesetz) in den Jahren 2020 – 2022 eingeführt. Danach werden ausgewählte Patientendaten in standardisierten Datenformaten in die Systeme Telematik-Infrastruktur (TI) übertragen. Die Übertragung aus der lokalen elektronischen Patientenakte erfolgt in einem standardisierten Verfahren. Die Sicherheitsrelevanten Rahmenbedingungen basieren auf den Richtlinien der Gematik, verantwortlich für die TI.

10.6.4 Medizintechnik

Medizintechnik besteht zum größten Anteil aus Diagnose- oder Therapiesystemen, die digitale Daten erzeugen und exportieren. Je nach Funktionalität der medizintechnischen Systeme können diese auch Patientendaten aus dem lokalen IT-Netzwerk empfangen (bidirektionale Kommunikation). Die Schnittstellen zwischen Medizintechnik und EPA lokal basieren auf Standards wie z.B. HL7 und GDT.

10.6.4.1 Medizintechnik mit Speicherung von Patientendaten

Der Anteil der Medizintechnik, der auch Patientendaten speichert, steigt an. Die auf lokalen Datenträger im Gerät gespeicherten Daten können als kritisch hinsichtlich des Datenschutzes und der Informationssicherheit angesehen werden. Für Neuanschaffungen und Ausmusterungen müssen in der Praxis / Klinik ausführliche Dokumentationen und Verfahrensanweisungen / Arbeitsanweisungen zur Verfügung stehen.

10.6.4.2 Medizintechnik ohne Speicherung von Patientendaten

Einfache Medizintechnik Geräte ohne Speicherung von Patientendaten werden entweder per Kabel (serielle Schnittstelle) oder drahtlos an Empfangsstationen des lokalen IT-Netzwerks angeschlossen. Für Kabelanschlüsse und Schnittstellen sind besondere Standards und Sicherheitsmaßnahmen vorgeschrieben.

10.6.5 Terminmanagement-SW

Die Verwaltung von Patiententerminen in der Praxis oder zur Videosprechstunde werden in unterschiedlichen IT-Umgebungen verwaltet. Da im Regelfall zusammen mit den personenspezifischen Daten auch medizinische Informationen (Besuchsgründe, Diagnosen, Untersuchungsmethoden) übertragen werden, sind diese Kommunikationen datenschutzrechtlich sensibel. Es werden deshalb entsprechende Maßnahmen in den Richtlinien und Verfahrensanweisungen dokumentiert.

10.6.5.1 Lokaler Terminkalender

Das herkömmliche Terminmanagement erfolgt in einem lokalen, digitalen Terminkalender. Die Termine werden im Regelfall telefonisch aufgenommen und dann in das Terminmanagementsystem, verbunden mit der EPA, eingegeben.

Terminbestätigungen erfolgen immer häufige über E-Mail-Kommunikation zwischen Praxis / Klinik und Patienten. Die entsprechenden Verfahrensanweisungen sind deshalb Bestandteil des IS-Konzepts.

10.6.5.2 Web-Terminkalender

Terminmanagement über das Internet erfolgt mit unterschiedlichen Kommunikationskonzepten. Bei einer einfachen Peer-to-Peer Kommunikation überträgt der Patient seine Wünsche und erhält seine Bestätigung über einen dedizierten Rechner in der Praxis. Nach anderen Konzepten erfolgt die Terminkommunikation direkt mit dem EPA-Netzwerk.

Die entsprechenden IT-Konstellationen sind in der Inventarisierung aufzunehmen und zu beschreiben (Termin-Kommunikationsschnittstelle).

Die Dokumentation des Providers ist Bestandteil der IT-Inventarisierung mit entsprechender Risikoanalyse.

10.6.6 Web-Anwendungen

Im Digitale Versorgung Gesetz (DVG) werden zusätzliche Möglichkeiten der Versorgung über das Internet ermöglicht. Die jeweiligen Anwendungen im Web sind von der Praxis / Klinik unabhängig vom lokalen IT-Netzwerk zu dokumentieren und in eine separate Risikoanalyse aufzunehmen.

10.6.6.1 Homepage / Portal

Die Auftritte der Arztpraxen / Kliniken im Web reichen von einer einfachen Homepage bis zu einem regionalen Gesundheitsportal. Die Informationssicherheits-relevanten Anwendungen sind ausführlich zu dokumentieren. Solche Anwendungen sind z.B.: Patientenbefragungen, Web-Shops für Medizinprodukte, Anmeldeformulare für Informationsveranstaltungen etc. Die entsprechenden Richtlinien nach DSGVO und DVG werden dokumentiert und eingehalten.

10.6.6.2 Videosprechstunde nach DVG

Ab 2020 werden Videosprechstunden unter bestimmten Bedingungen gefördert und honoriert. Eingesetzt werden speziell entwickelte Software-Systeme für Videosprechstunden. Diese Applikationen laufen entweder „Stand-Alone“ oder sind mit dem EPA-Netzwerk verbunden. In letzterem Fall werden sensible Patientendaten, beispielsweise Bildaufnahmen, mit dem Patienten über seinen Internet-Zugang ausgetauscht. Verfahrensanweisungen für die organisatorische und technische Abwicklung von Videosprechstunden liegen im ISMS vor.

10.6.6.3 Gesundheits-APPS nach DVG

Ebenfalls seit 2020 kann der Arzt sogenannte Gesundheits-Apps nach dem EBM Gebührenkatalog abrechnen. Dazu ist es notwendig das die Gesundheits-Apps auch

in der Praxis / Klinik über eine Internet-Verbindung demonstriert und eingewiesen werden können. Dazu werden Richtlinien und Verfahrensanweisungen erstellt und dokumentiert.

10.6.7 Datenschnittstellen medizinische Anwendungen

Der Austausch medizinischer Daten wird dem Gesetzgeber gefördert. Um sensible Patientendaten zwischen behandelnden Ärzten auszutauschen, sind digitale Schnittstellen zwischen den verschiedenen Systemwelten erforderlich. Diese sind im Regelfall standardisiert bzw. zertifiziert.

10.6.7.1 DICOM Schnittstellen

DICOM steht für Digital Imaging and Communication in Medicine, definiert Schnittstellen zum Austausch von Bilddaten in unterschiedlichen Formaten. Die bildgebenden Systeme (beispielsweise Radiologie, Laserdiagnostik, etc.) werden über einen internen oder externen DICOM Server ausgetauscht. Die im Rahmen der Informationssicherheit relevanten Informationen werden im DICOM Standard beschrieben. Wegen eines relativ hoher Störfall-Risikos (Störvorfälle in der Vergangenheit) sind DICOM Kommunikationen ausführlich im ISMS beschrieben.

10.6.7.2 HL7 Schnittstellen

Die HL7 Standards regeln Datenaustausch von administrativen, aber auch medizinischen Daten. Der HL7-CDA (Clinical Data Architecture) ist der Import-Standard innerhalb der TI zum Befüllen der individuellen EPA der Patienten (Patientendatenschutzgesetz / PDSG).

10.6.7.3 GDT-Schnittstellen

Der Standard der GDT-Schnittstellen (Gerätedatenaustausch) wurde von der Kassenärztlichen Bundesvereinigung (KBV). Er basiert auf dem KV-DT Schnittstellenprotokoll für die Abrechnung kassenärztlicher Leistungen. Der GDT-Schnittstellen-Verbund ist ausschließlich lokal im Einsatz und wird im Rahmen der IT-Inventarisierung beschrieben.

10.6.7.4 Andere Schnittstellen

Neben den standardisierten Schnittstellen (DICOM, HL7, GDT) existieren in der Praxis auch individuelle Schnittstellen. Im Rahmen des ISMS werden solche proprietären Schnittstellen (beispielsweise zum Datenaustausch von Praxen untereinander) ausführlich dokumentiert und mit Priorität in die Risikoanalyse aufgenommen.

10.6.8 Qualitätssicherungs- und Forschungsprojekte

Ein zentrales Ziel der digitalen Versorgung im Gesundheitswesen ist die Nutzung medizinischer Daten für Zwecke der Qualitätssicherung und der wissenschaftlichen Auswertung. Die einzelnen Projekte, wie beispielswese Gesundheitsregister, basieren auf individuellen IT-Architekturen. Die Schnittstellen und Anwendungen sind als hohes Risiko innerhalb der Informationssicherheit zu bewerten und entsprechend zu dokumentieren.

10.6.9 Schnittstellen zu Gesundheits-Apps nach DVG

Nach DVG werden sogenannte Gesundheits-Apps gefördert. Diese Förderung setzt voraus, dass die Apps zertifiziert sind und auf der Website der Kassenärztlichen Bundesvereinigung veröffentlicht sind. Die Zertifizierungs-Dokumentation ist über die KBV im Internet zu beziehen und in das ISMS zu integrieren.

11 Netzwerke und Verbindungen

Netzwerke und Verbindungen übertragen Informationen und vernetzen IT-Systeme miteinander. Deshalb ist es notwendig, sie angemessen abzusichern.

11.1 Netzwerkplan

Die Netzwerke der Praxis / Klinik müssen so erfasst sein, dass fachlich versierte Personen folgende Punkte nachvollziehen können:

1. Physikalische Netzwerkstruktur
    a. Aktive Netzwerkkomponenten und deren Verbindungen untereinander
    b. Physikalisches Medium der Verbindungen
2. Logische Netzwerkstruktur
    a. Netzwerksegmente (siehe Abschnitt 11.4.2) deren Einsatzzweck und deren Verbindungen untereinander
    b. Fernzugänge (siehe Abschnitt 11.4.3)
    c. Netzwerkkopplungen (siehe Abschnitt 11.4.4)
    d. Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken (siehe Abschnitt 11.3)

11.2 Aktive Netzwerk-Komponenten

Aktive Netzwerkkomponenten sind IT-Systeme und müssen gemäß Kapitel 10 behandelt werden.

11.3 Netzübergänge

Folgende Maßnahmen müssen für alle Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken umgesetzt werden.

1. Der Netzwerkverkehr wird auf das für die Funktionsfähigkeit notwendige Minimum beschränkt.
2. Der Inhalt erlaubter Verbindungen wird auf Schadsoftware und Angriffe untersucht; erkannte Schadsoftware und Angriffe werden blockiert.

3. Hinweise auf Schadsoftware in der IT-Infrastruktur der Praxis / Klinik und Angriffe aus der IT-Infrastruktur der Praxis / Klinik heraus werden als Sicherheitsvorfall (siehe Kapitel 18) behandelt.

Wenn Maßnahmen nicht umgesetzt werden, muss dem dadurch entstehenden Risiko durch eine Risikoanalyse und -Behandlung (siehe Anhang A2) begegnet werden.

Weitere Sicherheitsmaßnahmen sollten im Zuge einer Risikoanalyse und -Behandlung (siehe Anhang A2) ermittelt und umgesetzt werden.

Die Konfiguration der Netzwerkkomponenten, die einen Netzwerkübergang zu weniger oder nicht vertrauenswürdigen Netzwerken implementieren, muss jährlich überprüft werden und folgende Anforderungen erfüllen:

1. Für die sicherheitsrelevanten Einstellungen sind folgende Punkte dokumentiert:

    a. Wer sie implementiert hat
    b. Wann sie implementiert wurden was sie bewirken
    c. Warum sie benötigt werden

2. Die angestrebten Verkehrsbeschränkungen werden wirksam umsetzt.

11.4 Basis-Schutz

Die Maßnahmen der folgenden Abschnitte müssen, sofern eine entsprechende Funktionalität gegeben ist, für alle Netzwerke implementiert werden.

Wenn eine entsprechende Funktionalität nicht gegeben ist, sollte dem dadurch entstehenden Risiko durch eine Risikoanalyse und -Behandlung (siehe Anhang A2) begegnet werden.

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, muss dem dadurch entstehenden Risiko durch eine Risikoanalyse und -Behandlung (siehe Anhang A2) begegnet werden.

11.4.1 Netzwerkanschlüsse

Dauerhaft nicht genutzte Netzwerkanschlüsse müssen vor unberechtigter Nutzung gesichert werden.

Dies kann beispielsweise durch eine Zutrittsbeschränkung, eine Deaktivierung der Netzwerkanschlüsse oder durch eine Netzwerkzugangskontrolle geschehen.

11.4.2 Segmentierung

Die Notwendigkeit einer Segmentierung der Netzwerke der Praxis / Klinik muss geprüft und die Entscheidung dokumentiert werden.

Die Umsetzung der Segmentierung muss eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.

11.4.3 Fernzugang

Der Zugang zu nichtöffentlichen Bereichen von OT-Systemen der Praxis / Klinik über weniger oder nicht vertrauenswürdige Netzwerke muss abgesichert werden.

Dabei müssen folgende Anforderungen erfüllt werden:

1. Die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen werden geschützt.

2. Der Zugang wird so gestaltet, dass über ihn nur IT-Systeme erreichbar sind, die der jeweilige Nutzer für seine Aufgabenerfüllung benötigt.

Darüber hinaus sollten folgende Anforderungen erfüllt werden:

1. Der Zugang wird so gestaltet, dass der Nutzer und das zugreifende IT-System authentifiziert werden und sichergestellt ist, dass das IT-System grundlegende Sicherheitsanforderungen erfüllt oder der Zugang erfolgt über eine Remote-Desktop-Verbindung, die sicherstellt, dass Informationen nicht auf die zugreifenden IT-Systeme kopiert werden können.

2. Der Nutzer wird, vor allem wenn er umfangreiche Zugriffsrechte besitzt, mit Hilfe einer Mehr-Faktor-Authentifizierung authentifiziert, um die Gefahr eines unberechtigten Zugangs zu verringern.

11.4.4 Netzwerkkopplung

Die Kopplung von Netzwerken der Praxis / Klinik über weniger oder nicht vertrauenswürdige Netzwerke hinweg muss abgesichert werden.

Dabei müssen die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen gewährleistet werden.

11.5 Kritische Verbindungen

Für alle kritischen Verbindungen muss eine Risikoanalyse und -Behandlung (siehe Anhang A2) etabliert werden.

12 Mobile Datenträger

Mobile Datenträger sind aufgrund ihrer exponierten Nutzungsart besonders gefährdet. Deshalb ist es notwendig, die damit verbundenen Risiken angemessen zu behandeln.

12.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3. müssen in einer IOS-Richtlinie Regelungen für den Umgang mit mobilen Datenträgern getroffen werden:

1. Es wird festgelegt, welche Informationen der Praxis / Klinik gespeichert werden dürfen.

2. Die Nutzer werden über die spezifischen Risiken mobiler Datenträger (z.B. Gefahren durch Verlust oder Diebstahl oder durch das Einschleppen von Schadsoftware) informiert und zur Ergreifung entsprechender Gegenmaßnahmen verpflichtet.

3. Mobile Datenträger, auf denen Daten der Praxis / Klinik gespeichert sind, werden grundsätzlich vertraulich behandelt; sie werden nicht an unberechtigte Dritte weitergegeben oder verliehen und nicht für andere Personen zugänglich aufbewahrt.

12.2 Schutz der Informationen

Die auf den mobilen Datenträgern gespeicherten Informationen der Praxis / Klinik sollten vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden.

Der Schutz der Vertraulichkeit kann z.-B. durch eine Verschlüsselung der Datenträger erreicht werden.

12.3 Kritische mobile Datenträger

Für alle kritischen mobilen Datenträger muss eine Risikoanalyse und -Behandlung (siehe Anhang A2) etabliert werden.

13 Umgebung / Infrastruktur

Die Praxis / Klinik muss ihre IT-Systeme und Datenleitungen gegen negative Umwelteinflüsse absichern.

Dies sollte auf Basis eines anerkannten Standards, wie z.B. VdS 2007 erfolgen.

Wenn eine andere Vorgehensweise gewählt, wird, so muss hierfür ein Verfahren (siehe Anhang) implementiert werden, dass die Anforderungen folgender Abschnitte erfüllt.

13.1 Server und aktive Netzwerk-Komponenten

Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen /z.B. Patchfelder) müssen vor Beschädigung und unberechtigtem Zutritt geschützt werden.

Dies kann z.B. durch bauliche Maßnahmen (Serverraum) oder durch abschließbare Schränke (Server- oder Netzwerkschränke) umgesetzt werden.

Insbesondere sollten folgende Bedrohungen bewertet und behandelt werden:

1. Ungeeignete Umgebungsbedingungen (wie, z.B ungeeignete Temperatur oder Luftfeuchtigkeit, Staub oder Rauch)

2. Negative Umwelteinflüsse (wie z.B. Feuer, Wasser, Blitzschlag)

3. Unzuverlässige Stromversorgung (wie z.B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)
   Fest installierte Niederspannungsanlagen sollten gemäß gängiger Normen und Standards wie z.B. der DIN VDE 0100-Reihe errichtet sein.

4. Beschädigung und Verlust (wie z.B. Löschmittel, Vandalismus, Diebstahl)

13.2 Datenleitungen

Sämtliche Datenleitungen sollten gemäß gängiger Normen und Standards wie z.B. DIN EN 50173/4-Reihe installiert werden.
Wenn eine andere Vorgehensweise gewählt wird, müssen fest installierte Datenleitungen durch entsprechende baulich Maßnahmen vor Beschädigung geschützt werden.
Dies kann z.B. durch das Verlegen der Datenleitungen in Kabelkanälen umgesetzt werden.

13.3 Kritische IT-Systeme

Im Zuge der Risikoanalyse und -Behandlung (siehe Abschnitt 10.5.1) müssen für alle kritischen IT-Systeme folgende Bedrohungen behandelt werden.

1. Ungeeignete Umgebungsbedingungen (wie z.B. ungeeignete Temperatur oder Luftfeuchtigkeit, Staub, Rauch)

2. Negative Umwelteinflüsse (wie z.B. Feuer, Wasser, Blitzschlag)

3. Unzuverlässige Stromversorgung (wie z.B. Unter- oder Überspannung, Spannungsspitzen, Unterbrechung)

4. Beschädigung und Verlust (wie z.B. Löschmittel, Vandalismus, Diebstahl)

5. Unautorisierter Zutritt

6. Ausspähen vertraulicher Informationen

Insbesondere sollte geprüft werden, kritische IT-Systeme in zusätzlich abgesicherten Gebäuden oder Gebäudeteilen unterzubringen (Sicherheitszonen).

14 IT-Outsourcing und Cloud-Computing

Wenn IT-Ressourcen ausgelagert werden, ist es notwendig, dass die Sicherheitsinteressen der Praxis / Klinik berücksichtig werden.

14.1 IS-Richtlinie

In Ergänzung zu Schnitt 6.2 werden in einer IS-Richtlinie die Bedingungen, unter welchen IT-Ressourcen ausgelagert werden dürfen, festgelegt.

14.2 Vorbereitung

Für jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, müssen folgende Punkte dokumentiert werden:

1. Welche IT-Ressourcen ausgelagert werden sollen

2. Welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen, insbesondere in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität der ausgelagerten IT-Ressourcen, erfüllt werden müssen.

3. Ob die auszulagernden IT-Ressourcen kritisch sind.

Wenn IT-Ressourcen ausgelagert werden, muss die Organisation darauf vorbereitet werden:

1. Kompetenzen für die Steuerung der auszulagernden IT-Ressourcen werden aufgebaut

2. Die IT-Infrastruktur wird auf das Zusammenspiel mit den auszulagernden IT-Ressourcen vorbereitet.

14.3 Vertragsgestaltung

Wenn IT-Ressourcen ausgelagert werden soll, so muss mit dem Anbieter ein Vertrag geschlossen werden, der die Anforderungen aus Abschnitt 14.2 enthält und den Anbieter zu deren Erfüllung verpflichtet (siehe Richtlinien für Dienstleister vor Ort (DLO) im Anhang).

Darüber hinaus werden folgende Punkte sichergestellt:

1. Ansprüche aus Vertragsverletzungen können durchgesetzt werden, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Praxis / Klinik befindet.

2. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz sind vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen der Praxis / Klinik sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.

14.4 Kritische IT-Ressourcen

Wenn kritische IT-Ressourcen ausgelagert werden, müssen die Anforderungen aus Abschnitt 14.2 an ihre Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoanalyse (siehe Anhang A 2.1) ermittelt und folgende Punkte vertraglich geregelt werden:

1. Leistungen:

    a. Die vom Anbieter zu erbringenden Leistungen werden definiert und deren Messung und Überwachung werden vereinbart.

    b. Die Standorte, an denen Leistungen erbracht werden, werden festgelegt.

    c. Die Sicherheitsmaßnahmen, die der Anbieter zum Schutz der ausgelagerten IT-Ressourcen treffen muss, werden vereinbart.

    d. Eine Beschreibung der Schnittstellen zwischen der IT-Infrastruktur der Praxis / Klinik und den ausgelagerten IT-Ressourcen wird definiert.

Es sollten Konsequenzen bei Nichteinhaltung der vertraglich vereinbarten Leistungen vereinbart werden.

2. Kommunikation

    a. Die Ansprechpartner auf Seiten der Praxis / Klinik und des Anbieters werden benannt.

    b. Eine Vertraulichkeitsvereinbarung wird getroffen.

    c. Es wird vereinbart, ob und unter welchen Bedingungen der Anbieter dazu berechtig ist, Daten an Dritte weiterzugeben.

d. Eine Informationspflicht des Anbieters bei Sicherheitsvorfällen, die die ausgelagerten IT-Ressourcen betreffen, wird vereinbart.

3. Leistungsänderungen und Vertragsauflösung

   a. Die Mitwirkungspflichten des Anbieters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, insbesondere die vollständige Herausgabe der IT-Ressourcen der Praxis / Klinik sowie die aktive Unterstützung des Migrationsprozesses durch den Anbieter.

   b. Eine schriftliche Dokumentation und Meldung bei Änderungen an einem der oben genannten Punkte wird vereinbart.

Es muss sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Anbieter nicht im gleichen Rechtsraum wie die Praxis / Klinik befindet.

15 Zugänge und Zugriffsrechte

Zugänge und Zugriffsrechte erlauben es, auf die nichtöffentliche IT der Praxis / Klinik ihre Daten zuzugreifen. Deshalb ist es notwendig, beide strukturiert zu verwalten.

15.1 Managementzugänge und -zugriffe

Es müssen Verfahren (siehe Anhang A1) für das Anlegen und Ändern von Zugängen und Zugriffsrechten sowie für das Zurücksetzen von Authentifizierungsmerkmalen implementiert werden, die folgende Punkte sicherstellen:

1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt.

2. Zugänge und Zugriffsrechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe der Praxis / Klinik notwendig sein.

3. Wen nein Nutzer administrative Zugänge oder Zugriffsrechte erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden.

4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert.
   Wenn Zugänge und Zugriffsrechte entzogen werden, kann auf das Informieren des Nutzers verzichtet werden.

5. Vor dem Löschen eines Zugangs werden die Daten, die mit ihm verknüpft sind, weitergegeben, gelöscht oder gesichert bzw. archiviert.

6. Die jeweiligen Vorgänge werden dokumentiert.

15.2 Kritische IT-Systeme und Informationen

Alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen müssen jährlich erfasst und daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.1 angelegt wurden und benötigt werden.

Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte müssen als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.

16 Datensicherung, Sicherungstransport, Archivierung

Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit der Datensicherzustellen.

Die Datensicherung sollte auf Basis eines anerkannten Standards wie z.B. BSI-Standard 200-2 unter Berücksichtigung der IT-Grundschutz-Kataloge des BSO implementiert werden.

Wenn eine andere Vorgehensweise gewählt wird, müssen die Anforderungen folgender Abschnitte erfüllt werden.

16.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 müssen in einer IS-Richtlinie die Speicherorte für die Daten der Praxis / Klinik festgelegt werden.

16.2 Archivierung

Die Praxis / Klinik muss prüfen, welche Daten archiviert werden müssen, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen.
Die Liste der Aufbewahrungsfristen für personenbezogene medizinische Daten befindet sich im Anhang.

16.3 Planung und Verfahren

Für die Datensicherung, -wiederherstellung und -archivierung müssen Verfahren (siehe Anhang A1) implementiert werden, die die folgenden Punkte sicherstellen:

1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt.

   Der Schutz der Vertraulichkeit kann z.B. durch eine Verschlüsselung der Daten oder der Sicherungsmedien erreicht werden.

2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-System aufbewahrt.

   Ein eigener Brandabschnitt kann durch geeignete Datensicherungsschränke umgesetzt werden. In Bereichen mit Brandmeldesystemen sollten Datensicherungsschränke nach DIN EN 1047-1, Ausführung S 60 DIS, und in

Bereichen ohne Brandmeldesysteme nach DIN EN 1047-1, Ausführung S 120 DIS zertifiziert sein.

3. Die Datensicherung und -wiederherstellung wird jährlich oder bei einer Änderung des Verfahrens getestet, indem ein betroffenes IT-System nach dem Zufallsprinzip ausgewählt, gesichert und in einer Testumgebung wiederhergestellt wird.

   Die Tests sollten ohne Unterstützung durch den jeweiligen Verantwortlichen für die Datensicherung erfolgen. Vielmehr sollten sie von einem anderen Mitarbeiter anhand der vorliegenden Dokumentation durchgeführt werden.

4. Die Durchführung und die Ergebnisse der Tests werden dokumentiert.

Die Verfahren sollten darüber hinaus die folgenden Punkte sicherstellen:

1. Einzelne Datensicherungen werden in festen zeitlichen Abstünden (z.B. wöchentlich) an einen entfernten Standort ausgelagert, damit die gesicherten Daten auch bei größeren Schadenereignissen verfügbar bleiben.

2. Die Datensicherung wird nach dem Mehr-Generationen-Prinzip durchgeführt, um die Wahrscheinlichkeit eines umfangreichen Datenverlusts weiter zu verringern.

16.4 Weiterentwicklung

Der ISB muss jährlich prüfen, ob Änderungen an IT-Systemen sowie an betrieblichen, gesetzlichen oder vertraglichen Rahmenbedingungen eine Anpassung der Sicherungs- Wiederherstellungs- und / oder Archivierungsverfahren erforderlich machen.
Notwendige Anpassungen müssen zeitnah implementiert werden.

16.5 Basis-Schutz

Die Maßnahmen der folgenden Abschnitte müssen, sofern eine entsprechende Funktionalität gegeben ist, für Speicherorte (siehe Abschnitte 16.1), Server, aktive Netzwerkkomponenten und mobile IT-Systeme implementiert werden.

Wenn eine entsprechende Funktionalität nicht gegeben ist, sollte dem dadurch entstehenden Risiko durch eine Risikoanalyse und -Behandlung (siehe Anhang A2) begegnet werden.

Wenn Maßnahmen nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, muss dem dadurch entstehenden Risiko durch eine Risikoanalyse und -Behandlung (siehe Anhang A2) begegnet werden.

16.5.1 Speicherorte

Speicherorte müssen so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist.

16.5.2 Server

Server müssen so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.) nicht älter als 24 Stunden ist.

16.5.3 Aktive Netzwerk-Komponenten

Systemsoftware und Konfiguration der aktiven Netzwerkkomponenten müssen erstmalig und nach jeder Änderung gesichert werden.

16.5.4 Mobile IT-Systeme

Es muss eine Vorgehensweise für die Datensicherung von einem Administrator vorgegeben werden.

16.6 Kritische IT-Systeme

Jedes kritische IT-System muss über eine Datensicherung verfügen, die in Ergänzung zu Abschnitt 16.5 folgende Anforderungen erfüllt.

16.6.1 Risikoanalyse

Im Zuge der Risikoanalyse und -Behandlung (siehe Abschnitt 10.5.1) müssen die Folgen eines Datenverlusts analysiert und dabei der MTD bestimmt werden.

16.6.2 Verfahrensanweisungen

Die Verfahren zur Datensicherung und -wiederherstellung müssen in Ergänzung zu Abschnitt 16.3 folgende Punkte sicherstellen:

1. Kritische IT-Systeme werden vollständig gesichert (Systemsoftware, Konfigurationen, Anwendungssoftware, Anwendungs-, Logdaten, usw.)

2. Der MTD wird nicht überschritten.

3. Die Wiederherstellung innerhalt der MTA wird gewährleistet, sofern keine Ersatzsysteme oder -verfahren verfügbar sind (siehe Abschnitt 10.5.9)

17 Störungen und Ausfälle

Eine angemessene Reaktion auf Störungen und Ausfälle ermöglicht, zügig den Regelbetrieb wieder aufzunehmen und so Schäden zu minimieren.

Zu diesem Zweck sollte die Praxis / Klinik ein Business Continuity Management (BCM) auf Basis eines anerkannten Standards wie BSO-Standard 100-4 oder DIN EN ISO 22301 implementieren.

Wenn eine andere Vorgehensweise gewählt wird, müssen die Anforderungen folgender Abschnitt erfüllt werden.

17.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 müssen in einer IS-Richtlinie Regelungen für den Umgang mit Störungen und Ausfällen getroffen werden:

1. Begriffe „Störung“ und „Ausfall“ werden klar definiert.

   Hierbei wird aufgezählt, welche Auffälligkeiten zur Meldung einer möglichen Störung bzw. eines möglichen Ausfalls führen müssen.

2. Jeder Mitarbeiter meldet mögliche Störungen und Ausfälle an einen Administrator.

3. Administratoren untersuchen, gegebenenfalls in Zusammenarbeit mit den jeweiligen Prozessverantwortliche, dem IT-Verantwortlichen und dem ISB, Störungen und Ausfälle vordinglich.

4. Es wird definiert, in welchen Fällen die Praxisleitung über Störungen und Ausfälle informiert wird.

5. Es wird definiert, wie die Praxis / Klinik intern und nach außen über akute und bewältigte Störungen und Ausfälle kommuniziert.

17.2 Reaktionen

Es muss ein Verfahren (siehe Anhang) implementiert werden, das beim Auftreten einer Störung oder eines Ausfalls folgende Reaktionen zeitnah sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
4. Der Schaden wird dokumentiert.
5. Beweismittel werden gesichert.
6. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Störungen oder Ausfällen können einzelne Punkte ausgelassen und / oder das Verfahren vorzeitig beendet werden.

17.3 Kritische IT-Systeme

Folgende Maßnahmen müssen zusätzlich für alle kritischen IT-Systeme umgesetzt werden.

17.3.1 Wiederanlaufpläne

Für jedes kritische IT-System muss ein Verfahren (siehe Anhang A1) für den Wiederanlauf implementiert werden (Wiederanlaufplan), das folgende Anforderungen erfüllt:

1. Es enthält alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, das IT-System innerhalb der MTA soweit wiederherzustellen, dass zumindest das Notbetriebsniveau (siehe Abschnitt 10.5.2) erreicht ist.
2. Wenn das IT-System innerhalb seiner MTA nicht wiederhergestellt werden kann, enthält der Wiederanlaufplan alle Informationen, Arbeitsschritte und deren Reihenfolge, die es fachlich versierten Personen ermöglichen, die entsprechenden Ersatzsysteme oder -verfahren (siehe Abschnitt 10.5.9)

soweit in Betrieb zu nehmen, dass die vom IT-System abhängigen zentralen Prozesse und Prozesse mit hohem Schadenspotential betrieben werden können.

3. Er enthält eine Aufstellung der für die Wiederherstellung zwingend benötigten Ressourcen, wie z.B. Mitarbeiter und deren Kontaktdaten, Hardware, Software, Netzwerke, Dienste und Authentifizierungsmerkmale.

4. Er ist verständlich und übersichtlich strukturiert.

5. Er ist im Bedarfsfall schnell verfügbar.

6. Er wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

17.3.2 Abhängigkeiten IT-Systeme

Es müssen die Abhängigkeiten der kritischen IT-Systeme untereinander dokumentiert werden.

Darüber hinaus sollten die Abhängigkeiten der kritischen IOT-systeme von sämtlichen kritischen IT-Ressourcen dokumentiert und dabei die Notwendigkeit weiterer Wiederanlaufpläne geprüft werden

Die Dokumentation muss folgende Anforderungen erfüllen:

1. Aus ihr geht eindeutig hervor, in welcher Reihenfolge die kritischen IT-Systeme wiederhergestellt werden müssen.

2. Sie ist verständlich und übersichtlich strukturiert.

3. Sie ist im Bedarfsfall schnell verfügbar.

4. Sie wird in einem anderen Brandabschnitt als das betreffende IT-System aufbewahrt.

18 Sicherheitsvorfälle

Eine angemessene Reaktion auf Sicherheitsvorfälle ermöglichet es, Schäden schnelleinzudämmen und beheben zu können. Deshalb ist es notwendig, angemessen auf Sicherheitsvorfälle vorbereitet zu sein.

18.1 IS-Richtlinie

In Ergänzung zu Abschnitt 6.3 müssen in einer IS-Richtlinie Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden:

1. Der Begriff des Sicherheitsvorfalls wird klar definiert.

   Hierbei sollte aufgezählt werden, welche Auffälligkeiten zur Meldung eines potentiellen Sicherheitsvorfalles führen müssen.

2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle an den ISB

3. Der ISB untersucht, gegebenenfalls in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und den Administratoren, Sicherheitsvorfälle vordringlich.

4. Es wird definiert, in welchen Fällen die Praxisleitung über Sicherheitsvorfälle informiert wird.

5. Es wird definiert, wie die Praxis / Klinik intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.

18.2 Erkennen von Sicherheitsvorfällen

Es sollten Maßnahmen implementiert werden, die es ermöglichen, Sicherheitsvorfälle zu erkennen, wie z.B.:

1. Intrusion Detection Systeme (IDS)

2. Integritätsprüfungen auf Prüfsummenbasis

3. Sensor-Systeme (Honeypots)

4. Überwachen der Zugriffe auf besonders sensible Dateien
5. Erfassen und Auswerten von Logmeldungen

Das Melden von Sicherheitsvorfällen sollte durch eine positive Fehlerkultur und / oder anonyme Meldewege gefördert werden.

18.3 Reaktionen auf Sicherheitsvorfälle

Es muss ein Verfahren (siehe Anhang A1) implementiert werden, das beim Auftreten eines Sicherheitsvorfalls folgende Reaktionen zeitnah sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen.
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen.
3. Der Schaden wird durch Sofortmaßnahmen eingedämmt.
4. Der Schaden wird dokumentiert.
5. Beweismittel werden gesichert.
6. Der Schaden wird behoben und der Regelbetrieb wieder aufgenommen.
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden.

Bei geringfügigen Sicherheitsvorfällen können einzelne Punkte ausgelassen und /(oder das Verfahren vorzeitig beendet werden.

Das Verfahren sollte so gestaltet werden, dass auch bei Abwesenheit des ISB eine zeitnahe Reaktion gewährleistet ist.

19 Individualdokumentation

19.1 Verfahrensanweisungen

Die Praxis / Klinik plant, steuert und verbessert die in diesen Richtlinien geforderten Verfahren stetig (siehe PDCA)
Dies erfolgt im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z.B. DIN EN ISO 9001:2015 oder QEP.

Wenn eine andere Vorgehensweise gewählt wird, müssen folgende Anforderungen erfüllt sein:

1. Es wird definiert, wer für die Durchführung verantwortlich ist#

2. Verfahren werden in einer für die jeweilige Zielgruppe zugänglichen und verständlichen Form dokumentiert und bekannt gegeben.

3. Verfahren werden verbessert, wenn Mängel in ihrer Umsetzung, Angemessenheit oder Effektivität erkannt werden.

4. Umsetzung, Angemessenheit und Effektivität werden jährlich bei einem Drittel der Verfahren überprüft. Die zu überprüfenden Verfahren werden nach dem Zufallsprinzip ausgewählt. Wenn die Jährliche Überprüfung ergibt, dass mehr als die Hälfte der überprüften Verfahren mängelbehaftet ist, werden alle Verfahren überprüft.

19.2 Risikoanalyse und Behandlung

Die Praxis / Klinik muss die in diesen Richtlinien geforderten Risikoanalysen durchführen und erkannte Risiken zeitnah und angemessen behandeln.

Dies sollte im Rahmen eines Risikomanagements auf Basis eines anerkannten Standards wir BSI-Standard 200-3, ISO / IEC 27005 oder ISO 31000 erfolgen.

Wenn eine andere Vorgehensweise gewählt wird, so muss hierfür ein Verfahren (siehe Anhang) implementiert werden, welches die Anforderungen folgender Abschnitt erfüllt.

19.2.1 Risikoanalyse

Eine Risikoanalyse muss folgende Anforderungen erfüllen:

1. Ihre Dokumentation beinhaltet das Vorgehen für das Identifizieren und Bewerten von Risiken.

2. Die Vorgehensweise gewährleistet, dass Bedrohungen und Schwachstellen zuverlässig erkannt werden können.

3. Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden und deren Eintrittswahrscheinlichkeit.

4. Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

19.2.2 Risikobehandlung

Identifizierte Risiken müssen zeitnah und priorisiert behandelt werden, indem geeignete Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken (z.B. durch den Abschluss einer Versicherung) definiert, dokumentiert und umgesetzt werden.

Die Umsetzung muss kontrolliert und auf Wirksamkeit geprüft werden.

Wenn Risiken nicht angemessen behandelt werden können, müssen sie von der Praxisleitung akzeptiert werden. Dies muss dokumentiert werden.

19.2.3 Wiederholung und Anpassung

Risikoanalysen müssen jährlich auf ihre Aktualität geprüft und bei Bedarf wiederholt werden.

Risikoanalysen müssen darüber hinaus zeitnah überarbeitet werden, wenn eine der folgenden Faktoren auftritt:

1. Der Gegenstand der Risikoanalyse hat sich wesentlich verändert (z.B. die Hardware, die Software oder die Konfiguration eines IT-Systems).
2. Der Einsatzzweck des untersuchten Gegenstands hat sich wesentlich geändert.
3. Die Gefährdungslage hat sich erhöht (z.B. wenn eine neue Gefährdung bekannt wurde oder sich eine bestehende Gefährdung wesentlich erhöht hat).

20 Verarbeitungen im Rahmen des Datenschutzes

Für alle Verarbeitungen werden die Maßnahmen der folgenden Abschnitte implementiert.

20.1 Verarbeitungsprozesse

Die Praxis/Klinik wird ein Verzeichnis seiner Verarbeitungen führen (Verarbeitungsverzeichnis). Dieses Verzeichnis enthält alle internen und alle ausgelagerten Verarbeitungen (siehe Kapitel 22).
Das Verarbeitungsverzeichnis enthält den Namen und die Kontaktdaten der Organisationseinheit, der Leitung, des DSB (falls benannt) und ggf. auch die der gemeinsam Verantwortlichen (siehe Abschnitt 10.5). Es dokumentiert für jede Verarbeitung die Abschnitte 20.3 bis 20.11.

Das Verarbeitungsverzeichnis wird im Rahmen eines Qualitätsmanagements auf Basis eines anerkannten Standards wie z.B. DIN EN ISO 9001:2015 gelenkt.

20.2 Lebenszyklus

20.2.1 Etablierung und Änderungen

Es wird ein Verfahren für die Etablierung und Änderung einer Verarbeitung implementiert, das folgende Punkte sicherstellt:

1. Die Anforderungen der Abschnitte 20.3 bis 20.11. werden umgesetzt.
2. Das Datenmanagement (siehe Kapitel 24) wird bei Bedarf angepasst.
3. Das Verarbeitungsverzeichnis (siehe Abschnitt 20.1) wird aktualisiert und vom DSM /DSB freigegeben.

20.2.2 Einstellung / Beendigung

Es wird ein Verfahren für die Einstellung einer Verarbeitung implementiert, das folgende Punkte sicherstellt:

1. Die Einstellung der Verarbeitung werden die nicht mehr benötigten personenbezogenen Datengelöscht (siehe Abschnitt 24.1.) soweit nicht entsprechende Aufbewahrungspflichten bestehen
2. Die Verarbeitung wird nur aus dem Verarbeitungsverzeichnis gelöscht, wenn alle ihre personenbezogenen Daten gelöscht wurden
3. Das Verarbeitungsverzeichnis (siehe Abschnitt 20.1.) wird aktualisiert und vom DSM / DSB freigegeben.

20.3 Zweck

Der Zweck der Verarbeitung wir konkret definiert.

20.4 Beschreibung

Die Verarbeitung wird beschrieben. Diese Beschreibung ist so gestaltet, dass sie für die Kommunikation mit den Betroffenen (siehe Abschnitt 20.7 und Abschnitt 20.12.2) und den Aufsichtsbehörden verwendet werden kann.

20.5 Gemeinsam Verantwortliche

Wenn personenbezogene Daten gemeinsam von verschiedenen Parteien verarbeitet werden, wird eine Vereinbarung geschlossen, die folgende Anforderungen erfüllt:

1. Sie beschreibt, welche Person für welche Datenschutzaufgaben verantwortlich ist, insbesondere, wer welchen Informationspflichten nachkommt und gegenüber wem die Betroffenen ihre Rechte wahrnehmen können
2. Sie wird auf Nachfrage den Betroffenen zugänglich gemacht.

20.6 Eigentümer

Der Eigentümer der Verarbeitung wird dokumentiert.

20.7 Rechtsgrundlage

Die Rechtsgrundlage der Verarbeitung wird dokumentiert. Wenn die Rechtsgrundlage auf einer Einwilligung beruht, wird eine Vorgehensweise etabliert, die sicherstellt, dass die gesetzlichen Vorgaben eingehalten werden. Insbesondere gewährleistet die Vorgehensweise die Erfüllung der folgenden Anforderungen:

1. Der Betroffene wird vor seiner Einwilligung über den Zweck der Verarbeitung informiert (siehe Abschnitt 20.3)
2. Der Betroffene erhält vor seiner Einwilligung eine Beschreibung, anhand derer er die Datenverarbeitung nachvollziehen kann (siehe Abschnitt 20.4)
3. Der Betroffene wird vor seiner Einwilligung auf seine Rechte (siehe Abschnitt 20.12) hingewiesen.

4. Alle Informationen sind für die Betroffenen verständlich formuliert und übersichtlich strukturiert.
5. Alle Informationen werden nachweislich erbracht.
6. Die Identität des Betroffenen wird geprüft.
7. Der Einwilligungstext, der Zeitpunkt der Einwilligung und die erhobenen personenbezogenen Daten werden protokolliert.
8. Wenn sich der angebotene Dienst direkt an Kinder richtet, werden Anstrengungen unternommen, das Einverständnis der Erziehungsberechtigten einzuholen.

20.8 Personenbezogene Daten

20.8.1 Datenkategorien

Die personenbezogenen Daten der Verarbeitung werden ermittelt und in Kategorien eingeteilt.

Für jede Kategorie wird festgelegt:

1. Für welche Zwecke sie verwendet wird
2. Ob sie zwingend für die Verarbeitung erforderlich ist
3. Welche Kategorien von Personen darin betroffen sind
4. Ab wann ihre Daten nicht mehr benötigt werden
5. Ab wann die Personenbindung ihrer Daten nicht mehr benötigt wird
6. Welche Aufbewahrungsfirsten bestehen
7. Welche Löschristen bestehen
8. Welchen Kategorien von Empfängern die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, sowohl innerhalb als auch außerhalb der Organisationseinheit.

20.8.2 Datenübermittlung

Wenn personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt werden soll, wird eine Vorgehensweise etabliert, die sicherstellt, dass dabei die gesetzlichen Vorgaben eingehalten werden.

Insbesondere gewährleistet die Vorgehensweise die Erfüllung der folgenden Anforderungen:

1. Die Rechtsgrundlage wird festgestellt
2. Es werden Garantien erbracht, dass ein angemessenes Datenschutzniveau bei dem Empfänger existiert.

20.9 IT-Systeme, mobile Datenträger

Für die Verarbeitung wird ermittelt, welche IT-Systeme, mobilen Datenträger und Verbindungen für das Verarbeiten, Speichern oder Übertragen von personenbezogenen Daten verwendet werden.

20.10 Risikoanalyse und -behandlung

Für die Verarbeitung wird eine Risikoanalyse und –behandlung durchgeführt, in der die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen untersucht werden.

Die Praxis/Klinik stellt sicher, dass die Risikoanalyse den gesetzlichen Vorgaben entspricht.

Insbesondere behandelt die Risikoanalyse folgende Risiken:

1. Unberechtigter Zugang zu Verarbeitungsanlagen (Zugangskontrolle)
2. Unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern (Datenträgerkontrolle)
3. Unbefugte Eingabe von personenbezogenen Daten sowie unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)
4. Unbefugte Nutzung von IT-Systemen über Verbindungen (Netzwerke) hinweg (Benutzerkontrolle)
5. Unbefugter Zugang der zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten auf personenbezogene Daten (Zugriffskontrolle)
6. Es kann nicht überprüft und festgestellt werden, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)
7. Es kann nicht nachträglich überprüft und festgestellt werden, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)
8. Verlust der Vertraulichkeit und Integrität bei der Übermittlung personenbezogener Daten sowie beim Transport von entsprechenden Datenträgern (Transportkontrolle)
9. IT-Systeme lassen sich im Störungsfall nicht wiederherstellen (Wiederherstellbarkeit)
10. Funktionen stehen nicht zur Verfügung oder auftretende Fehlfunktionen werden nicht gemeldet (Zuverlässigkeit)

11. Gespeicherte personenbezogene Daten werden durch Fehlfunktionen des Systems beschädigt (Datenintegrität)
12. Personenbezogene Daten, die im Auftrag verarbeitet werden, werden nicht entsprechend den Weisungen des Auftraggebers verarbeitet (Auftragskontrolle)
13. Personenbezogene Daten sind nicht gegen Zerstörung oder Verlust geschützt (Verfügbarkeitskontrolle)
14. Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden nicht getrennt verarbeitet (Trennbarkeit)

Risikoanalysen für vergleichbare Verarbeitungen können zusammen erstellt werden.

20.11 Datenschutz-Folgeabschätzung (DSFA)

Es wird geprüft, ob für die Verarbeitung eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden muss. Die Organisationseinheit stellt sicher, dass die Prüfung den gesetzlichen Vorgaben entspricht.

Insbesondere werden folgende Kriterien geprüft:

1. Vorliegen eines gesetzlichen Regelbeispiels
2. Positiv- und Negativlisten entsprechender Aufsichtsbehörden
3. Vorhandensein eines hohen Risikos für die Rechte und Freiheiten der Betroffenen
4. Gesetzliche Befreiung von der Pflicht zur Durchführung einer DSFA

Die Organisationseinheit führt die notwendigen DSFA durch.

Insbesondere erfüllt die DSFA folgende Anforderungen:

1. Der DSB begleitet die DSFA beratend
2. Es wird überprüft, ob ein im Rahmen der Risikoanalyse zuvor bejahtes voraussichtlich hohes Risiko tatsächlich auch hoch ist.
3. Es wird eine Dokumentation der DSFA erstellt, die folgende Informationen beinhaltet:
    a. Eine systematische Beschreibung der beabsichtigten Verarbeitungen
    b. Deren Zwecke
    c. Die legitimen Interessen des Verantwortlichen an den Verarbeitungen
    d. Eine Bewertung, inwieweit die Verarbeitung zur Erreichung des jeweiligen Zwecks notwendig und verhältnismäßig ist
    e. Eine Bewertung der Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen, die mit den Verarbeitungen verbunden sind
    f. Die beabsichtigten Abhilfemaßnahmen zur Bewältigung der dargestellten Risiken

g. Falls erfolgt das Einbinden der Betroffenen

Wenn die DFSA trotz der beabsichtigten Abhilfemaßnahmen mit hohen Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen verbunden ist, muss die entsprechende Aufsichtsbehörde konsultiert werden.

20.12 Betroffenenrechte

20.12.1 Anfrage und Reaktion

Es ist ein Verfahren für die Entgegennahme und Behandlung von Anfragen implementiert. Die Organisationseinheit stellt sicher, dass mit dem Verfahren die entsprechenden gesetzlichen Anforderungen erfüllt werden.

Insbesondere werden folgende Anforderungen geprüft:

1. Anfragen können von den Betroffenen leicht gestellt werden
2. Die Anfrage wird dokumentiert
3. Die Identität des Betroffenen wird geprüft
4. Es wird geprüft, ob ein Versagungsgrund besteht (z.B. Aufbewahrungspflicht)
5. Jede Auskunftserteilung erfolgt nachweislich und innerhalb der gesetzlichen Fristen
6. Wenn die Auskunft über ein unsicheres Medium wie z.B. E-Mail erfolgt, wird zuvor das Einverständnis des Betroffenen eingeholt

Die Erfüllung der Anforderungen wird durch standardisierte Texte, Tabellen oder Checklisten vereinfacht. Wenn im Zuge der Abarbeitung einer Anfrage Mängel erkannt werden, findet Nachbereitung statt, bei der konkrete Verbesserungen erarbeitet werden mit dem Ziel, zukünftige Anfragen zu vermeiden bzw. die Betroffenenrechte mit möglichst geringem Aufwand zu erfüllen (PDCA Prinzip).

20.12.2 Erfüllung

Für die Verarbeitung wird eine Vorgehensweise zur Erfüllung sämtlicher Betroffenenrechte implementiert und dokumentiert. Die Organisation stellt sicher, dass die Vorgehensweise den gesetzlichen Vorgaben entspricht.

Insbesondere werden folgenden Anforderungen geprüft:

1. Recht auf Auskunft
    a. Es werden sämtliche personenbezogenen Daten des Betroffenen erfasst und in Kopie zur Verfügung gestellt (soweit keine rechtlichen Einschränkungen bestehen)

   b. Die personenbezogenen Daten können in einem gängigen elektronischen Format exportiert werden
   c. Der Betroffene erhält Auskunft über Datenkategorien, Verarbeitungszwecke, Herkunft, Empfänger oder Empfängerkategorien, Speicherdauer oder falls nicht möglich Kriterien für die Festlegung der Dauer
   d. Der Betroffene wird darüber informiert, ob seine personenbezogenen Daten miteinander verknüpft und ausgewertet werden (Profiling) und wenn ja, nach welcher Logik dies geschieht.
2. Recht auf Löschung
   a. Sämtliche personenbezogenen Daten werden aus dem aktiven Datenbestand gelöscht
   b. Es wird vor der Löschung geprüft, ob rechtliche Rahmenbedingungen eingehalten werden (z.B. Aufbewahrungspflicht)
3. Recht auf Berichtigung
   a. Korrekturen werden vor ihrer Umsetzung geprüft
   b. Unrichtige personenbezogenen Daten werden im aktiven Datenbestand berichtigt
4. Recht auf Widerruf und Widerspruch
   a. Die Verarbeitung der betroffenen personenbezogenen Daten wird auf Antrag beendet
   b. Die Beendigung wird rechtskonform dokumentiert
5. Recht auf Einschränkung
   a. Die Verarbeitung der betroffenen personenbezogenen Daten wird auf Antrag ausgesetzt
   b. Vor der Fortsetzung der Verarbeitung wird der Betroffene hierüber informiert.
6. Recht auf Datenmitnahme
   a. Sämtliche personenbezogenen Daten des Betroffenen werden erfasst und in Kopie zur Verfügung gestellt
   b. Die Daten werden in einem strukturierten, gängigen und maschinenlesbaren Format exportiert
   c. Die exportierten Daten werden einem vom Betroffenen benannten Empfänger übermittelt
7. Protokollierung
   a. Jede Durchführung wird nachvollziehbar protokolliert
   b. Die Protokolle werden sicher archiviert.

20.13 Überprüfung

Die Organisation überprüft die Umsetzung und Dokumentation seiner Verarbeitungen und behebt erkannte Mängel. Dies erfolgt im Rahmen eines Qualitätsmanagement auf Basis eines anerkannten Standards wie z.B. DIN EN ISO 9001:2015 (siehe Modul QM).

Wenn eine andere Vorgehensweise gewählt wird, so werden folgende Anforderungen erfüllt:

1. Umsetzung und Dokumentation werden jährlich bei einem Drittel der Verarbeitungen überprüft
2. Die zu überprüfenden Verarbeitungen werden nach dem Zufallsprinzip ausgewählt
3. Wenn die jährliche Überprüfung ergibt, dass bei mehr als der Hälfte der überprüften Verarbeitungen Mängel bestehen, werden alle Verarbeitungen überprüft
4. Erkannte Mängel werden zeitnah behoben

21 Informationssicherheit (Verweis auf Kapitel 1-9)

Die Organisationseinheit stellt die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen auf Dauer sicher (Informationssicherheitsprozess).

Der Informationssicherheitsprozess wird so gestaltet, dass die Anforderungen des Datenschutzes berücksichtigt werden und er sämtliche IT-Systeme, mobilen Datenträger und Verbindungen abdeckt, mit denen personenbezogene Daten verarbeitet, übertragen oder gespeichert werden (Kapitel 1 – 9).

22 Auftragsverarbeitung

Nutzen und Anbieten von Auftragsverarbeitungen setzt bei Patienten und Anbietern ein strukturiertes Vorgehen voraus.

22.1 Als Auftraggeber

Wenn Verarbeitungen ausgelagert werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung hilft der Praxis dabei, Haftungsrisiken vorzubeugen.

22.1.1 Datenschutz-Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 legt die Organisationseinheit in einer DS-Richtlinie fest, unter welchen Bedingungen eine Verarbeitung ausgelagert werden darf.

22.1.2 Vorbereitung

Für jedes Vorhaben, das zur Auslagerung einer Verarbeitung führt, werden folgende Punkte dokumentiert:

1. Welche Verarbeitungen ausgelagert werden sollen
2. Welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen in Bezug auf den Datenschutz der ausgelagerten Verarbeitungen erfüllt werden müssen
3. Ob für die auszulagernden Verarbeitungen eine DSFA (siehe Abschnitt 20.11) durchzuführen ist

22.1.3 Eignung des Auftragsverarbeiters

Wenn eine Verarbeitung ausgelagert werden soll, wir vor der Beauftragung sichergestellt und dokumentiert, dass der Auftragsverarbeiter über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt.
Insbesondere wird geprüft, ob der Auftragsverarbeiter über das notwendige Fachwissen, die Zuverlässigkeit und Ressourcen verfügt, die gesetzlichen, betrieblichen und vertraglichen Anforderungen zu erfüllen. Auftragsverarbeiter können ihre Eignung durch entsprechende Zertifizierungen z.B. nach diesen Richtlinien nachweisen.

22.1.4 Vertragsgestaltung

Wenn Verarbeitungen ausgelagert werden sollen, so wird mit dem Auftragsverarbeiter ein Vertrag geschlossen, der folgende Anforderung erfüllt:

1. Anforderungen an den Datenschutz
    a. Er enthält die Anforderung aus Abschnitt 22.1.2 und verpflichtet den Auftragsverarbeiter zu deren Erfüllung
2. Leistungen
    a. Der Gegenstand und die voraussichtliche Dauer der Verarbeitung werden festgelegt.
    b. Die Zwecke der Auftragsverarbeitung, die Art der verarbeiteten personenbezogenen Daten und die Kategorien der betroffenen Personen werden festgelegt.
    c. Es wird definiert, dass personenbezogene Daten nur auf Weisungen in Textform hin verarbeitet werden (Vertragsbestandteile oder Weisungen während der Dauer der Verarbeitung) und dass der AV entsprechende technische oder organisatorische Maßnahmen in seiner Organisation umsetzen muss
    d. Der AV wird verpflichtet und ermächtigt auf potentielle Rechtsverstöße, die durch eine Weisung entstehen könnten, aufmerksam zu machen
    e. Der AV wird ermächtigt, Weisungen, durch die ein potentieller Rechtsverstoß entstehen kann, bis zur Klärung des Sachverhalts nicht zu befolgen
    f. Der AV stellt sicher, dass die an der Verarbeitung beteiligten Mitarbeiter zur Vertraulichkeit verpflichtet sind
3. Datensicherheit
    a. Die Sicherheitsmaßnahmen, die der Auftragsverarbeiter zum Schutz der personenbezogenen Daten der Organisationseinheit treffen muss, werden vereinbart
    b. Eine Informationspflicht des Auftragsverarbeiters bei Sicherheitsvorfällen, die die externen Verarbeitungen betreffen, wird vereinbart.
4. Unterstützung der Organisation
    a. Es werden technische und organisatorische Maßnahmen definiert, wie der AV die Praxis/Klinik bei der Wahrung der Betroffenenrechte unterstützt, insbesondere bei Erteilung von Auskünften sowie der Korrektur oder der Löschung von personenbezogenen Daten
    b. Die Mitwirkungspflichten des Auftragsverarbeiters im Falle einer Vertragsauflösung oder Insolvenz werden vereinbart, insbesondere die vollständige Herausgabe oder Löschung der personenbezogenen Daten der Praxis/Klinik sowie die aktive Unterstützung des Migrationsprozesses durch den AV
    c. Die Mitwirkungspflichten bei Datenschutzvorfällen werden vereinbart, insbesondere die Unterstützung bei der Meldung an Aufsichtsbehörden und bei der Benachrichtigung von Betroffenen
    d. Die Mitwirkungspflichten bei der Durchführung von Datenschutz-Folgenabschätzungen sowie bei der vorherigen Konsultation der Aufsichtsbehörden werden vereinbart

5. Dokumentation und Kontrolle
    a. Es werden Dokumentationspflichten vereinbart, insbesondere jene, die die Praxis/Klinik zum Nachweis der Einhaltung der oben genannten Punkte benötigt
    b. Es wird vereinbart, dass der AV Inspektionen durch die Organisationseinheit oder einen beauftragten Prüfer bezgl. der Einhaltung der oben genannten Punkte ermöglicht und unterstützt.
    c. Der AV wird verpflichtet, ein Verzeichnis der für die Praxis/Klinik erbrachten Verarbeitungen (siehe Abschnitt 20.1) zu führen und der Praxis/Klinik in der jeweils aktuellen Form zur Verfügung zu stellen
6. Unterauftragnehmer
    a. Eine Genehmigung in Textform bei jeder Einschaltung oder Ersetzung von Unterauftragsnehmern wird vereinbart.
    b. Der AV schließt mit jedem Unterauftragnehmer einen Vertrag, der ihn zur Erfüllung der oben genannten Punkte verpflichtet.

Darüber hinaus sollte sichergestellt sein, dass Ansprüche aus Vertragsverletzungen durchgesetzt werden können, auch wenn sich der Auftragsverarbeiter nicht im gleichen Rechtsraum wie die Organisationseinheit befindet.

22.1.5 Überprüfung

Die Organisation überprüft. Dies kann durch sachverständige Dritte geschehen. Der Nachweis kann durch Zertifikate (z.B. gemäß dieser Richtlinien), Testate oder sonstige Bestätigungen erbracht werden.
Wenn bei einzelnen AV eine andere Vorgehensweise notwendig ist, so werden die folgenden Anforderungen erfüllt:

1. Bei jedem betroffenen AV wird jährlich ein Drittel der zu ihm ausgelagerten Verarbeitungen überprüft.
2. Die zu überprüfenden Verarbeitungen werden nach dem Zufallsprinzip ausgewählt
3. Wenn die Prüfung ergibt, dass bei mehr als der Hälfte der überprüften Verarbeitungen eines AV Mängel bestehen, werden alle an den AV ausgelagerten Verarbeitungen überprüft.
4. Die Verarbeitungen werden anhand der Ergebnisse und Erkenntnisse der Prüfung zeitnah überarbeitet und geprüft, bis sie mängelfrei sind.
5. Die Durchführung und die Ergebnisse der Prüfung werden dokumentiert.

22.2 Als Auftragnehmer

Wenn Verarbeitungen angeboten werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung hilft Haftungsrisiken vorzubeugen.

22.2.1 Datenschutz-Richtlinie

Für jede Verarbeitung wird ein Vertrag mit dem Verantwortlichen gemäß Abschnitt 22.1.4 geschlossen.

22.2.2 Zertifizierungen

Auftragsverarbeiter können ihre Eignung durch entsprechende Zertifizierungen, beispielsweise nach diesen Richtlinien, nachweisen.

23 Datenschutzvorfälle

Eine angemessene Reaktion auf Datenschutzvorfülle ermöglicht es Schäden schnell einzudämmen und beheben zu können sowie gesetzliche Anforderungen zu erfüllen. Deshalb ist es notwendig, angemessen auf Datenschutzvorfülle vorbereitet zu sein.

23.1 Richtlinie

In Ergänzung der Regelungen aus Kapitel 6 wird der Umgang mit Datenschutzvorfüllen in einer Richtlinie festgelegt.

Die DS-Richtlinie stellt folgende Punkte sicher:

1. Der Begriff des Datenschutzvorfalls wird klar definiert
2. Jeder Mitarbeiter meldet mögliche Datenschutzvorfülle an den DSM / DSB.
3. Der DSM untersucht in Zusammenarbeit mit dem DSB (falls bestellt) und ggf. den Eigentümern der betroffenen Verarbeitungen (siehe Abschnitt 4.6) dem IT-Verantwortlichen, den Administratoren und den entsprechenden Auftragsverarbeitern (siehe Kapitel 22), Datenschutzvorfälle vordringlich
4. Es wird definiert, in welchen Fällen die Leitung Datenschutzvorfälle informiert wird
5. Es wird definiert, wie intern und nach außen über akute und bewältigte Datenschutzvorfälle kommuniziert wird.

23.2 Erkennen

Es sind Maßnahmen zu implementieren, die es ermöglichen, Datenschutzvorfälle zu erkennen, wie z.B.

1. Technische Überwachung der IT-Infrastruktur (wie z.B. Intrusion Detection Systeme (IDS), Sensor-Systeme (Honeypots), überwachen der Zugriffe auf besonders sensible Dateien, oder erfassen und auswerten von Logmeldungen)
2. Einrichten von anonymen Meldewegen für Mitarbeiter, Zielgruppen und / oder Öffentlichkeit

23.3 Reaktion

Es ist ein Verfahren implementiert, das beim Auftreten eines Datenschutzvorfalls folgende Reaktionen in der angegebenen Reihenfolge sicherstellt:

1. Es wird ein Überblick über die Situation gewonnen
2. Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen
3. Der Vorfall wird durch Sofortmaßnahmen eingedämmt
4. Der Vorfall wird dokumentiert, insbesondere
    a. Welche Daten von welchen Personenkategorien betroffen sind
    b. Wie hoch die Anzahl der Betroffenen und der Datensätze ist
    c. Eine Beschreibung der wahrscheinlichen Folgen der Verletzung
    d. Eine Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen
    e. Ggf. Maßnahmen für die Abmilderungen der möglichen negativen Folgen
5. Beweismittel werden gesichert
6. Der Schaden wird behoben und die regulären Geschäftsprozesse wieder aufgenommen
7. Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt und konkrete Verbesserungen erarbeitet werden
8. Es wird ermittelt, ob eine gesetzliche Meldepflicht besteht und welche Vorgaben und Fristen hierbei eingehalten werden müssen
9. Es wird geprüft, ob die Betroffenen benachrichtiget werden oder eine öffentliche Bekanntmachung veranlasst werden muss.

Bei geringfügigen Vorfällen ist es möglich, die Punkte 2, 3, 5, 6 und 7 vorzeitig zu beenden oder auszulassen.

24 Datenmanagement

Es besteht die gesetzliche Verpflichtung, nicht mehr benötigte personenbezogene Daten zu löschen. Hierfür ist ein strukturiertes Vorgehen notwendig.

24.1 Löschen

Die Praxis/Klinik erfüllt ihre gesetzlichen Löschpflichten.

Es wird ein Verfahren implementiert, das die folgenden Anforderungen erfüllt:

1. Für jede Datenkategorie wird gemäß der in Abschnitt 20.8.1 definierten Bedingungen eine Vorgehensweise definiert, wie und in welchem Rhythmus nach zu löschenden Daten gesucht wird und wie eine Löschung zu erfolgen hat. Datenkategorien mit gleichen oder ähnlichen Anforderungen können zusammengefasst werden.
2. Es werden der aktive Datenbestand und die archivierten Daten erfasst.
3. Der Suchlauf, das Löschen sowie auftretende Fehler werden, sofern technisch möglich, protokolliert.

24.2 Anonymisieren, Pseudonymisieren, Kryptieren (Verschlüsseln)

Wenn personenbezogene Daten zu ihrem Schutz anonymisiert, pseudonymisiert oder verschlüsselt werden, wird die Vorgehensweise analog zu Abschnitt 24.1 etabliert.

25 Technische + organisatorische Maßnahmen (TOM)

Die Anforderungen an TOM sind konkret in Art. 32 der DSGVO dokumentiert:

Art. 32 DSGVO Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

25.1 Technische Maßnahmen

Alle technischen Maßnahmen werden individuell nach Vorgaben der DSGVO und entsprechenden Standards (z.B. BSI Grundschutz) dokumentiert.

25.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen orientieren sich am eingesetzten Qualitätsmanagementsystem. Dabei werden insbesondere die Anforderungen nach SGB V QM RL § 4 erfüllt (siehe QMS)

26 Datenschutzberichte

Aus verschiedenen Artikeln der DSGVO ergeben sich für die DS-Verantwortlichen Verpflichtungen zu regelmäßigen Dokumentationen.

26.1 Jahresbericht

Nach Art. 24 DSGVO besteht für den/die DS Verantwortlichen die Nachweispflicht: Verantwortung des für die Verarbeitung Verantwortlichen:

1 Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.
2 Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.
Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.
Der DS-Verantwortliche erstellt für die Leitung jährlich einen Bericht nach den Anforderungen der DSGVO.

26.2 Rechenschaftsbericht

Nach Art. 5 (2) macht die DSGVO unter bestimmten Umständen einen Rechenschaftsbericht erforderlich:

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1 auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
2 für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“)
3 dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“); sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
4 in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden
5 in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
6 Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).
7 Der DS- Verantwortliche erstellt regelmäßig oder bei Bedarf den Rechenschaftsbericht. Dieser kann im Datenschutzbericht/Jahresbericht enthalten sein.

27 Optimierungsmanagement (PDCA)

Elementare Bestandteile in der Informationssicherheit, dem Datenschutz und dem allgemeinen Qualitätsmanagement für Praxen und Kliniken sind Optimierungsprozesse. Hierzu wird das PDCA Konzept oder auch der „Demingkreis“ eingesetzt.

27.1 Planung (plan)

In der ersten Phase des PDCA-Zyklus steht die Planung im Fokus. Die Anforderung (z.B. die Datenschutz-Schulung) wird zunächst identifiziert. Anschließend wird eine Ist-Analyse durchgeführt, die ebenfalls Hintergrundinformationen zur aktuellen Anwendung enthält. Mithilfe der Analyse des Ist-Zustandes sowie der Anforderung (z.B. rechtliche Regelungen zur Informationssicherheit) lässt sich im Nachgang ein Ziel bestimmen (Aktualität des Wissens)

27.2 Realisierung (do)

In der zweiten Phase des PDCA-Zyklus werden die Maßnahmen, die in der Planungsphase festgelegt worden sind, umgesetzt. In erster Linie sind hierfür verantwortlichen Mitarbeiter involviert, die an dem Prozess beteiligt sind.
Wichtig ist, dass in der Do-Phase sämtliche Aktivitäten dokumentiert werden.
Es kann sinnvoll sein, die Maßnahmen zunächst in kleinem Rahmen zu testen (Beispielsweise DS Schulung in einer kleinen Gruppe).

27.3 Überprüfung (check)

In der Check-Phase des PDCA-Zyklus liegt der Fokus auf der objektiven Betrachtung. Zentrale Fragen dabei: Wurde das Ziel erreicht? Die zuvor gesammelten Daten werden hierfür ausgewertet und beurteilt. Sind noch Anpassungen erforderlich, um die festgelegten Vorgaben zu erfüllen? Dann ist in dieser Phase die Zeit dafür, bevor die flächendeckende Umsetzung erfolgt (beispielsweise Wissenstest zum Datenschutz).

27.4 Optimierung (act)

In der letzten Phase des PDCA-Zyklus werden die Maßnahmen reflektiert. Die optimierten Abläufe gelten nun als Standard und sollen von allen Mitarbeitern eingehalten werden. Es wird eine Analyse des Soll-Zustands erstellt, die anschließend mit dem Ist-Zustand verglichen wird. Zudem stehen während dieser Phase die Fragen im Vordergrund, was optimiert werden kann und wo sich weitere Potenziale befinden (z.B. beispielsweise digitale Schulungskonzepte). Wird in der Act-Phase festgestellt, dass das Ziel nicht erreicht worden ist, so wird der PDCA-Zyklus erneut durchlaufen (neuer Schulungsplan/Curriculum).

28 Richtlinien für Dienstleister vor Ort (DLO)

28.1 Zweck

Alle Systeme und angebotene Dienstleistungen im Geltungsbereich des ISMS müssen nach anerkanntem Stand der Technik in der Informationssicherheit gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt, in Betrieb genommen, dokumentiert und betrieben werden. Details der vorgesehenen Sicherheitsmaßnahmen sind im Angebot sowohl in technischen als auch organisatorischen Belangen zu beschreiben.
Die Umsetzung der Anforderungen ist zu beschreiben. Alle Abweichungen davon sind im Angebot zu benennen und zu begründen. Der Einsatz von Nachunternehmern und / oder Dritten ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer hat für alle Nachunternehmer wie für sein eigenes Handeln einzustehen.

28.2 Geltungsbereich und Zielgruppen

Dieser Vertragsbestandteil enthält die Anforderungen an Drittunternehmen, um die Sicherheitsanforderungen der Praxis / Klinik zu gewährleisten.
Die nachfolgenden Anforderungen sind verbindlicher Bestandteil der Liefer- und Wartungsverträge. Jegliche Abweichungen von den Anforderungen sind dem Auftraggeber (im Folgenden AG genannt) schriftlich mitzuteilen und von diesem explizit zu genehmigen.
Drittunternehmen (im Folgenden Dienstleister oder DLO genannt), die Dienstleistungen oder Produkte im Geltungsbereich des ISMS erbringen oder liefern, müssen grundlegende Anforderungen an die Sicherheit ihrer informationsverarbeitenden Systeme erfüllen und geeignete organisatorische Abläufe in Bezug auf sichere interne IT-Abläufe zusichern. Der AG behält sich vor, für unten genannte Maßnahmen entsprechende Nachweise anzufordern.
Werden Subdienstleister durch den DLO eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

28.3 Informationssicherheitsprozess

28.3.1 Geregelter Sicherheitsprozess zur Steuerung und Verbesserung der Informationssicherheit

Der Dienstleister muss in seinem Unternehmen einen geeigneten Sicherheitsprozess zur Planung, Steuerung, Kontrolle und Verbesserung der Informationssicherheit etabliert haben, über den die Umsetzung der hier geforderten technischen und organisatorischen Maßnahmen sichergestellt wird.
Dies kann beispielsweise in Form eines Informationssicherheitsmanagementsystems (ISMS) bzw. einer Zertifizierung nach ISO / IEC 27001 oder der Steuerung interner Abläufe bzw. des Betriebs der IT-Infrastruktur, z. B. nach ITIL, erfolgen. Der Nachweis einer Zertifizierung und / oder eines Lieferantenaudits kann in begründeten Einzelfällen erforderlich werden.
Der Dienstleister hat bei Einsatz von Subdienstleistern und Dritthersteller-Produkten diese zu benennen sowie die Umsetzung der Anforderungen aus der Dienstleistungsvereinbarung sicherzustellen und zu dokumentieren.

28.3.2 Ansprechpartner für Informationssicherheit

Der Dienstleister verfügt über einen Ansprechpartner zur Informationssicherheit, der für die Umsetzung und Überprüfung von Informationssicherheitsmaßnahmen verantwortlich und der zu Fragen der Informationssicherheit gegenüber dem Auftraggeber auskunftsfähig und auskunftsberechtigt ist.
Die vollständigen Kontaktdaten des Ansprechpartners sind dem AG mitzuteilen.

28.3.3 Mitarbeiter und Dienstleister

Die Mitarbeiter und Subdienstleister des DLO sind über die sicherheitstechnischen Anforderungen des AG zu informieren.
Die besondere Bedeutung der Informationssicherheit muss durch entsprechende Security-Schulungen für Mitarbeiter des DLO unterstrichen werden. Dabei sind die besondere Sensibilität im Umgang mit vertraulichen und sensiblen Daten sowie die sicherheitstechnischen Anforderungen herauszustellen.
Die Mitarbeiter müssen hinsichtlich des vertraulichen Umgangs mit Informationen, die ihnen im Zuge ihrer Tätigkeit bekannt werden, verpflichtet werden. Dies kann bspw. durch entsprechende Regelungen im Arbeitsvertrag oder eine separate Erklärung erfolgen.

Scheiden Mitarbeiter des DLO aus dem Unternehmen aus oder wechseln ihr Aufgabengebiet, ist durch geeignete Maßnahmen sicherzustellen, dass sicherheitssensitive Zutritts- und Zugriffsberechtigungen zu Systemen und Informationen des AG entzogen werden sowie Einwahlmöglichkeiten dieser Mitarbeiter in das Daten- / Prozessnetz und die Fernwartungsumgebung des AG

ausgeschlossen sind. Die Accounts der betroffenen Mitarbeiter sind zumindest zu deaktivieren.

Der AG behält sich vor, für oben genannte Maßnahmen entsprechende Nachweise anzufordern.

Der AG behält sich vor, Mitarbeiter von Dienstleistern, die in Kontakt mit als besonders sensibel kategorisierten Informationen oder Anlagen kommen, einer Sicherheitsüberprüfung unterziehen zu lassen bzw. für diese einen entsprechenden Sicherheitsnachweis einzufordern.
Werden Subdienstleister durch den DLO eingesetzt, so sind diese Anforderungen ebenfalls für den Subdienstleister bindend. Der Einsatz von Subdienstleistern ist dem AG anzuzeigen.

28.3.4 Anforderungen zum Stand der Technik

Der DLO hat die Verfahren zur Etablierung des Stands der Technik darzustellen, dazu gehört zum Beispiel die Beschreibung der Anforderungserfüllung gemäß des BDEW Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" und das BSI Dokument " Empfehlungen zu Entwicklung und Einsatz von in Kritischen Infrastrukturen eingesetzten Produkten". Zu diesem Zweck stellt der AG auf Anfrage dieses Whitepaper sowie eine Übersicht der relevanten Standards und Anforderungen zur Leistungserbringung zur Verfügung.

Der Nachweis der Anforderungserfüllung kann durch vorhandene Zertifizierungen erbracht werden (z.B. Produktzertifizierung nach IEC 62443).
In Abstimmung mit dem AG erfolgt die Dokumentation der Informationssicherheitsanforderungen in Form eines Pflichtenheftes durch den DLO.

28.3.5 Datenschutz

Der Schutz personenbezogener Daten ist bei der Erbringung von Dienstleistungen für die Praxis / Klinik ein wichtiges Anliegen. Die Verarbeitung personenbezogener Daten (z.B. Mitarbeiter, Kunden sowie Geschäftspartner) sind in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit durchzuführen.

Sollte eine Weitergabe dieser Informationen an Dritte (bspw. an Behörden o.ä.) erforderlich und rechtlich – insbesondere datenschutzrechtlich – notwendig sein, so können diese nur nach vorheriger Zustimmung der Praxis / Klinik unter Einbeziehung des Datenschutzbeauftragten sowie der IT-Sicherheitsbeauftragten der Praxis/Klinik erfolgen.

Umfasst die Dienstleistung eine Verarbeitung personenbezogener Daten, so ist eine Vereinbarung zur Datenverarbeitung im Auftrag gemäß den Anforderungen des Art. 28 DSGVO mit dem Dienstleister abzuschließen. Die genannten Vertragsmuster werden gemäß Dienstleistungsumfang zur Verfügung gestellt.
Gesetzliche Löschtermine und Aufbewahrungsfristen sind datentypengenau zu beachten und zu dokumentieren. Der Dienstleister hat die Einhaltung der Lösch- und Sperrfristen von personenbezogenen Daten im Dienstleistungsumfang sicherzustellen und eine dem Dienstleistungsumfang entsprechende Dokumentation zur Verfügung zu stellen. Die Aufbewahrungsfristen für medizinische Patientendaten sind zu berücksichtigen.

28.4 Technische und organisatorische Bestimmungen

28.4.1 Softwareentwicklung (sofern in der Zusammenarbeit relevant)

Softwareentwicklung für die Praxis / Klinik ist nach aktuellen Qualitäts- und Informationssicherheitsstandards zu betreiben. Aufgrund der Zertifizierungen der Praxis/Klinik, werden hierzu die notwendigen Anforderungen aus aktuellen Standards und relevanter Normen in den Entwicklungszyklus einer Anwendung eingebunden, um durch geeignete Vorgaben die Qualität und Sicherheit der Software zu gewährleisten. Hierbei ist entscheidend, dass an den verschiedenen Stellen, an denen Gefährdungen auftreten können, diesen durch entsprechende Maßnahmen entgegengewirkt wird.

Die Softwareentwicklung adressiert an vielen Stellen Themen der Qualität und Informationssicherheit. So sind verschiedene Aspekte zu bewerten und zu beschreiben. Dazu gehören die Auswahl der Sprache, die Architektur und die Datenhaltung. Die Entwicklung ist mittels Standards durchzuführen, die die Einhaltung von Qualitäts- und Sicherheitskriterien sicherstellen und die Abnahme des Ergebnisses durch geeignete Tests nachvollziehbar macht.
Ergänzend zu den Anforderungen des ISMS der Praxis / Klinik sind die Vorgaben an die Softwareentwicklung zu beachten, die in Form Technischer Richtlinien die Anforderungen an Softwareentwicklung innerhalb der Praxis / Klinik beschreiben. Diese werden bei Bedarf dem AN zur Verfügung gestellt.

28.4.2 Zugriffs- und Zutrittsschutz

Räume oder Bereiche beim Dienstleister, in denen Informationen elektronisch verarbeitet oder gespeichert werden, müssen durch geeignete Maßnahmen vor unberechtigtem Zutritt geschützt werden.
Alle informationsverarbeitenden Systeme des DLO, von denen ein Zugriff auf die Systemumgebung des AG oder dem AG zugeordnete sensible Informationen mittelbar oder unmittelbar möglich ist, müssen mit einem sicheren logischen Zugangsschutz versehen sein. Dabei ist eine Multi-Faktor-Authentifizierung

anzustreben (z. B. Kombination aus Benutzername/Passwort und einer ergänzenden Identifizierung mit Hilfe eines Hardwaretokens, einer Smartcard o. Ä. oder eines biometrischen Merkmals).

28.4.3 Kennwortanforderungen

An die Kennwörter für informationsverarbeitende Systeme und Komponenten werden besondere Anforderungen gestellt, der DLO muss deshalb eine verpflichtende Kennwortrichtlinie definiert haben.
Diese Richtlinie muss mindestens den Anforderungen an Kennwörter des AG entsprechen. Diese Anforderungen wird der AG dem DLO zur Verfügung stellen.

28.4.4 Netzwerksicherheit

Das interne Datennetzwerk des DLO wird von öffentlichen oder externen Netzen durch geeignete Maßnahmen nach dem Stand der Technik getrennt (z. B. Firewall). Drahtlose Netzwerke müssen nach Stand der Technik gesichert werden, insbesondere muss ein unbefugter Zugriff auf die System- und Wartungsumgebung des AG oder dem AG zugeordnete sensible Informationen sicher verhindert werden.

28.4.5 Schadsoftwareschutz

Der DLO muss sicherstellen, dass alle informationsverarbeitenden Systeme mit einem aktiven und aktuellen Schutz vor Schadsoftware versehen sind, soweit sich dies technisch realisieren lässt.

Insbesondere für diejenigen Systeme, von denen mittel- oder unmittelbar Zugriffe auf die System- und Wartungsumgebung des AG möglich sind (z. B. Parametrierlaptops, Terminalserver, Web-, Mail- und Dateiserver usw.) ist ein stringenter Schadsoftwareschutz sicherzustellen.

Der DLO muss sicherstellen, dass der Schadsoftwareschutz nicht durch Mitarbeiter deaktiviert wird.

Bei Pattern-basierten Lösungen ist dafür Sorge zu tragen, dass die Schadsoftware-Pattern unverzüglich aktualisiert werden.

Neben den Arbeitsplatzsystemen muss der Schutz vor Schadsoftware auch Kommunikationsverbindungen, wie Web-, E-Mail- und Datentransfer, umfassen.

28.4.6 Systemhärtung, Schwachstellen und Patch-Management

Systeme sind nach anerkannten und dokumentierten Verfahren (z. B. CIS-Standards) zu konfigurieren bzw. zu parametrieren, dazu gehört z. B. die dokumentierte Systemhärtung.

Betriebssysteme, Firmware oder Applikationen von IT-Komponenten des DLO sind unverzüglich durch Softwareupdates des jeweiligen Herstellers zu aktualisieren, wenn durch diese Updates Sicherheitslücken geschlossen oder Schwachstellen beseitigt werden.

Zu diesem Zweck ist ein Patchmanagement zu etablieren, welches sicherstellt, dass Patches vom Hersteller bezogen sowie nach Dringlichkeit kategorisiert und durch einen geregelten Prozess installiert werden können.

28.4.7 Administration von Systemen und Anwendungen

Die technischen und organisatorischen Anforderungen an die Administration von Anwendungen und Systemen der Praxis/Klinikdurch Dienstleister und beauftragte Dritte sind zu beachten und umzusetzen. Sie können sich aufgrund der privilegierten Rechte, Zugriff zu Informationen verschaffen, deren Schutzbedürfnis ggf. erhöht ist. Gerade deswegen gelten für Administratoren besondere Sorgfalts- und Verschwiegenheitspflichten. Sie haben durch ihre Berechtigungen erweiterten oder gar unbeschränkten Zugriff auf die Infrastruktursysteme, sowie die darüber vorgehaltenen Informationen.

Die für die Beauftragung benötigten Informationen werden dem Auftragnehmer dem Dienstleistungsumfang entsprechend zur Verfügung gestellt.

28.5 Umgang mit klassifizierten Informationen

Wenn der AG Klassifizierungen von Informationen vorgibt, muss der DLO diese Vorgaben zur Klassifizierung von Informationen des AG einhalten und seine Mitarbeiter dahingehend nachweislich unterweisen.
Alle Informationen des AG sind ihrer Vertraulichkeitsklasse entsprechend eindeutig eingeordnet und gekennzeichnet. Die Informationsklassifizierung richtet sich dabei nach dem möglichen Einfluss auf die Rechtskonformität des AG, der sich aus einer vorsätzlichen oder nicht beabsichtigten Bekanntgabe der Informationen ergeben kann.

Der AG kann Vertraulichkeitsklassen festlegen, aus denen sich jeweils unterschiedliche Konsequenzen für die Handhabung der relevanten Informationen ergeben.

28.5.1 Verarbeitung sensibler Informationen

Zu den besonders schützenswerten Daten des AG werden insbesondere die folgenden Informationen gezählt:

- Alle personenbezogenen Daten, insbesondere nach Art. 9 DSGVO
- Informationen zur Konfiguration und Implementierung von Sicherheitsmaßnahmen
- Passwörter und Authentisierungsinformationen
- Netzwerkpläne, -konfigurationen und IP-Adress-Informationen
- Aufbau und Konfiguration von Systemen und Komponenten der IT- und Prozessleittechnik des AG.

Diese Daten werden im Sinne der hier dargestellten Sicherheitsanforderungen auch als "sensibel" bezeichnet und können zusätzlich speziellen Vertraulichkeitsstufen unterliegen.

28.5.2 Zugriffsschutz, Speicherung und Entsorgung

Werden Daten des AG durch den DLO verarbeitet, so hat dieser sicherzustellen, dass der Zugriff auf diese Daten auf einen minimalen Kreis berechtigter Mitarbeiter eingeschränkt wird.
Werden sensible Daten auf mobilen Komponenten gespeichert (z. B. Notebooks, mobile Datenträger etc.), sind diese durch eine Verschlüsselung nach Stand der Technik zu sichern.

Werden IT-Systeme oder Komponenten des DLO, auf denen sensible Daten des AG gespeichert sind, zur Reparatur gegeben oder einer Entsorgung zugeführt, muss gewährleistet sein, dass diese Daten nicht für Dritte, auch nicht unter Verwendung von Daten-Wiederherstellungstechnologien, lesbar oder anderweitig auswertbar sind. Der Stand der Technik zur sicheren Vernichtung von Informationen ist nachweislich anzuwenden.

28.5.3 Übermittlung in Netzwerken

Datenverkehr, über den sensible Informationen zwischen AG und DLO über ein unsicheres Netz (z. B. Internet) ausgetauscht werden, muss mit Hilfe anerkannter technischer Verfahren gegen Manipulation oder Einsichtnahme geschützt werden. Dafür sind in der Regel VPN-Lösungen einzusetzen, deren kryptographische Algorithmen dem aktuellen Stand der Technik entsprechen.

Der VPN-Tunnel muss nach Beendigung der Kommunikation abgebaut werden; eine dauerhafte Einrichtung eines solchen Tunnels zwischen AG und DLO ist untersagt.

Werden per E-Mail sensible Informationen zwischen AG und DLO ausgetauscht, so muss der Mailverkehr kryptographisch gesichert werden. Der DLO trägt Sorge für die entsprechenden technischen Voraussetzungen auf seiner Seite

28.6 Anforderungen an die Wartungsprozesse

Unter "Wartung" werden alle vom DLO erbrachten Servicemaßnahmen verstanden, die sich auf die Komponenten oder Systeme der technischen IT-Umgebung des AG auswirken.

Servicemaßnahmen können beispielsweise sein:

- Instandhaltungs- und Reparaturarbeiten
- Fehleranalyse- und Fehlerbehebungsarbeiten
- Installation von Softwareupdates oder neuen Firmware- oder Betriebssystemen bzw. Applikationen
- System-, Geräte oder Software-Anpassungen, Neuparametrierungen u. Ä.

Wartungsarbeiten können innerhalb eines Remote-Zugriffs über eine Fernwartungsinfrastruktur bei DLO und AG, als auch in Form von Vor-Ort-Arbeiten (z. B. Anschluss mobiler Geräte an das Netzwerk oder die IT- und Prozesstechnikkomponenten des AG) durchgeführt werden.

28.6.1 Allgemeines

Wartungsarbeiten durch den DLO erfolgen ausschließlich durch qualifiziertes und geschultes Personal. Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen des AG nachweislich zu schulen, ggf. sind entsprechende Sicherheitsüberprüfungen nachzuweisen.

Alle zur Wartung genutzten Systeme müssen mit einem sicheren logischen Zugangsschutz versehen sein sowie vor einem unberechtigten physischen Zugriff geschützt werden.

Die anderweitige Nutzung von für Wartungsarbeiten genutzten Systemen / Komponenten ist durch den DLO zu untersagen. Dies gilt auch für den Fall, dass auf den Systemen eigens für die Wartung installierte virtuelle Maschinen (Betriebssystem und Applikationen) verwendet werden.

28.6.2 Sichere Systemkonfiguration von Wartungskomponenten

Für Wartungsarbeiten sind ausschließlich Systeme zu verwenden, die anhand anerkannter Best-Practice-Vorgaben und Die Systeme müssen beim Wartungszugriff

über einen aktiven Schadsoftwareschutz, basierend auf aktuellen AV-Pattern, verfügen.

28.6.3 Fernwartung

Fernwartungszugriffe dürfen nur über die vom AG zur Verfügung gestellten Fernwartungszugänge realisiert werden.
Die zur Fernwartung berechtigten Mitarbeiter sind dem AG namentlich mitzuteilen.
Fernwartungszugriffe dürfen auf Seiten des DLO nur aus einem nach Stand der Technik gesicherten und gegen unberechtigte Zugriffe geschützten Wartungsnetzwerk erfolgen. Sollen Fernwartungszugriffe direkt von Arbeitsplatzsystemen oder anderen Systemen (z. B. mobile Systeme, Heimarbeitsplatz) erfolgen, muss dies dem AG mitgeteilt und von diesem explizit genehmigt werden.

Fernzugriffe werden auf einem Terminalserver in einer separaten Sicherheitszone des AG terminiert. Der AG legt die technisch / organisatorischen Parameter für die Einwahl fest und übermittelt diese an den DLO. Der DLO benennt die für die Wartungsarbeiten benötigten Programme und Tools, welche auf den Systemen bereitgestellt werden müssen, stellt diese zur Installation zur Verfügung und stellt notwendige Aktualisierungen sicher.
Ein direkter Zugriff auf die zu wartenden Systeme des AG unter Umgehung des Terminalservers ist nicht zulässig

28.7 Spezielle Anforderungen der Telematikinfrastruktur (TI)

Die Praxis / Klinik nutzt die Telematikinfrastruktur (TI) der Kassenärztlichen Bundes-Vereinigung (KBV). Die Anforderungen sind dem DLO in der jeweils aktuellen Version bekannt (www.kbv.de). Der DLO verpflichtet sich, alle Mitarbeiter ausdrücklich und ausführlich über alle Vorschriften der Installation und Wartung der Konnektoren und anderer TI Komponenten zu informieren und dies in einem Schulungsprotokoll zu dokumentieren.

28.8 Meldung von Informationssicherheitsvorfällen

Wenn beim DLO ein Informationssicherheitsvorfall vorliegt, der Auswirkungen auf die vom DLO an den AG gelieferten Produkte oder Dienstleistungen hat oder auf andere Weise die Informationssicherheit des AG gefährdet, ist der DLO verpflichtet, den AG unverzüglich darüber zu informieren.

Wenn Zweifel darüber bestehen, ob es sich tatsächlich auch um einen Informationssicherheitsvorfall handelt, muss dies trotzdem gemeldet werden.

29 Qualitätsmanagement

Das Qualitätsmanagement orientiert sich an den gesetzlichen Rahmenbedingungen nach § 135ff SGB V. Auf das bereits bestehende QMS kann referenziert werden.

29.1 Übersicht der Praxis/Klinik

Beispiel:

Name der Praxis:
Anschrift 1:
Anschrift 2:
Ausrichtung:

IT Infrastruktur

Software:

EPA Software:	Name System mit Speicherung von Personendaten
Abrechnungs-SW:	Name System mit Speicherung von Personendaten
Terminkalender:	Name System (Web / oder nicht Web) mit Speicherung von Personendaten

Hardware:

- Server
- Anzahl Arbeitsplätze

Komplette Auflistung Siehe Anhang

29.2 Mission, Vision und Politik

29.2.1 Mission

Die Mission einer Klinik/Praxis wird individuell im Team erarbeitet und dokumentiert.
Beispiel:

„Unsere Praxis versorgt Kassen- und Privatpatienten in unserem Facharztbereich aus der näheren und weiteren Umgebung.

Die Sicherheit der Patientenversorgung und eine optimale medizinische und organisatorische Qualität sind zentrale Ziele der Leitung und des gesamten Praxisteams. Wirtschaftlichkeit und Rechtskonformität definieren dabei übergeordnete Rahmenbedingungen. Dazu setzen wir speziell für Arztpraxen entwickelte Managementsysteme für den Datenschutz und das damit verbundene Qualitätsmanagement ein.
In der fachspezifischen Patientenversorgung folgen wir strukturierten Behandlungspfaden, die transparente und immer dem individuellen Fall angemessene Untersuchungs-, Diagnose- und Therapie-Prozesse gewährleisten.

Die Patienten werden umfassend sowohl unter medizinischen wie auch rechtlichen (forensischen) Gesichtspunkten informiert und aufgeklärt. Dabei wird eine einfache und allgemein verständliche Sprache gewählt. Diese Sprache vermeidet negative Formulierungen und schafft dagegen mit positiven Formulierungen Vertrauen und ein sicheres Gefühl bei den Patienten.“

29.2.2 Vision

Eine Vision in der medizinischen Versorgung definiert Ziele, die in einem Team reflektiert und festgeschrieben wird.

„Die ärztliche Leitung und das Praxisteam versuchen gemeinsam die Qualität der Patientenversorgung ständig zu verbessern. Dabei unterstützen Weiter- und Fortbildungsmaßnahmen die Aktualität des medizinischen Wissens im Team. Aktuelles Fachwissen, das auf wissenschaftlichen Verifizierungen beruht, wird in die Standardbehandlungen einbezogen, wenn es die individuellen Fälle erforderlich machen. Evidenzbasierte Medizin, die als Leitlinien der Fachgesellschaften herausgegeben werden, sind bekannt und digital verfügbar.

Alle relevanten Gesetze, Verordnungen, Richtlinien, Vorschriften und Empfehlungen der Bundesärztekammer und der Bundes KV sind bekannt und digital verfügbar, soweit sie relevant für die Praxis sind. Dies gilt insbesondere für BGB (Ärztliche Schweigepflicht), SGB V (Qualitätsmanagement), DSGVO (Datenschutz Grundverordnung), BDSG (Bundesdatenschutzgesetz), Empfehlungen der Bundesärztekammer und der KBV zum Datenschutz IfSG (Infektionsschutzgesetz), Medizinproduktegesetz (MPG), Medizinprodukte Betreiber Verordnung (MPBetreibV) und alle aushangpflichtige Gesetze.

Praxisleitung und -team kommunizieren regelmäßig und bei aktuellem Bedarf, um mögliche kritische organisatorische oder technische Anforderungen zu adressieren und um einen aktuellen Wissensstand aller Beteiligten zu gewährleisten. Bei wichtigen Fragen zur Patientenversorgung wird der eingerichtete Ablauf im Sinne des Patienten umgesetzt und dokumentiert. Bei Identifikation von Verbesserungspotential wird der PDCA Prozess (Plan-Do-Check-Act) nach den Prinzipien des Qualitätsmanagements umgesetzt.“

29.3 Ressourcen und Prozesse

Die Ressourcen einer Praxis / Klinik haben einen wesentlichen Einfluss auf Wirtschaftlichkeit und Qualität der medizinischen Versorgung. In diesem Kontext ist jeweils zu prüfen, ob eine Investition in neue Medizintechnik oder / und Schulungsmaßnahmen eine Optimierung der Ergebnisse auslösen kann.

29.3.1 Technische Ressourcen

Bei den technischen Ressourcen sind die wesentlichen Komponenten die Ausstattung mit IT-Systemen und der spezifischen Medizintechnik.

29.3.2 IT-Infrastruktur

Die Informationstechnologie ist in den vergangenen 30 Jahren zu einem wesentlichen Kriterium für Qualität aber auch insbesondere die Produktivität geworden.

Die digitale Verarbeitung von medizinischen und abrechnungstechnischen Daten kennzeichnet die Produktivität einer medizinischen Einrichtung. Gemessen werden können Produktivität und Effektivität beispielsweise an „pro Kopf-Umsätzen“ pro Jahr.

Innerhalb der Planung ist beispielsweise festzulegen, ob eine Praxis / Klinik komplett papierlos oder mit einer Kombination aus Papier und elektronischer Dokumentation oder Patientenakte arbeitet. Die IT-Infrastruktur ist in einem ersten Schritt in einem Netzwerkplan zu erfassen und mit Einzelangaben zu dokumentieren. Anschließend wird die Systemarchitektur bewertet (Strukturqualität). Aus der Dokumentation können zukünftige Planungen abgeleitet werden (technischen Maßnahmen innerhalb von TOM).

29.3.3 Medizintechnik

Die vorhandene Medizintechnik ist unter verschiedenen Gesichtspunkten zu analysieren:

- Für welchen Anteil der Patienten kann ein bestimmtes Gerät eingesetzt werden?
- Welche Abrechnungsmöglichkeiten bestehen für die entsprechende Diagnose- oder Therapie-Leistung?
- Welche Alternativen existieren technisch oder organisatorisch?

29.3.4 Qualifikation und Kompetenz

Die wichtigsten Produktivfaktoren einer medizinischen Einrichtung sind Ärzte und ihre Mitarbeiter. Die Optimierung der Qualifikation und Kompetenz fallen in die organisatorischen Maßnahmen (TOM 2).

29.3.5 Patientenversorgung (Fortbildung)

Die professionelle Grundausbildung und die ständige Fortbildung der Mitarbeiter bestimmen Qualität aber auch Produktivität in einer Praxis. Deshalb ist es wichtig, dass am Anfang einer Periode (6 oder 12 Monate) ein Schulungsplan für alle Mitarbeiter besteht. Bei der Schulung ist zu unterscheiden nach externer Fortbildung durch Anbieter von Trainingsprogrammen und der internen Schulung durch die Ärzte selbst oder die Beauftragten oder Koordinatoren.

Zunehmend werden Online-Schulungen, sogenannte Webinare angeboten. Sie bieten sich an, da sie mit keinerlei Fahrtkosten verbunden sind und flexibel in einen Tagesablauf einbezogen werden können.

29.3.6 Qualitätsmanagement und Rechtskonformität

Unabhängig von der Patientenversorgung sind die Qualifikationen im Qualitätsmanagement ein Schlüssel für Rechtskonformität und auch die Produktivität.

In jeder Praxis sollte ein Qualitätsmanagementbeauftragter, eine Qualitätsmanagementbeauftragte (QMB) und eine Vertretung benannt sein. Das gleiche gilt für den Datenschutz. Eine Datenschutzkoordinatorin / ein Datenschutzkoordinator können die Leitung bei der Umsetzung der Rechtskonformität wesentlich unterstützen.

29.3.7 Kommunikation

Die Sprache und die Kommunikation generell sind wichtige Einflussfaktoren auf die Zufriedenheit von Patienten und Teammitgliedern.

29.3.8 Kommunikation mit Patienten

Die Kommunikation mit den Patienten ist an dem einzelnen Behandlungsfall auszurichten. Grundsätzlich sollte die Kommunikation verständlich (einfache Begriffe, kurze Sätze) und lösungsorientiert (positive Formulierung) sein. Es ist in diesem Kontext bekannt, dass die Sprache einen wesentlichen Beitrag zur positiven Entwicklung einer Therapie haben kann.

29.3.9 Kommunikation im Team

Auch die Produktivität im Team wird sehr stark über die Kommunikation untereinander gesteuert. Die Sprache kann Energie vermitteln aber auch entziehen. Mit dem Einsatz moderner Sprachkonzepte (beispielsweise Neurolinguistische Programmierung – NLP) können erhebliche Optimierungseffekte erzielt werden (Kaizen).

29.4 Messung, Analyse und Optimierung

29.4.1 Befragungen

Im Rahmen der QM Anwendung werden Analysen und Befragungen durchgeführt, um den Status und die Entwicklung der Qualität zu ermitteln und zu dokumentieren.

29.4.2 Patienten

Die Patienten stehen im Mittelpunkt der medizinischen Versorgung. Ihre Zufriedenheit mit Behandlung und Service wird durch Befragungen ermittelt.

29.4.3 Mitarbeiter/Kollegen

Die Mitarbeiter/Kollegen sind im Sinne der Qualität und Entwicklung die wesentlichen Aktivposten einer medizinischen Einrichtung. Die Zufriedenheit mit der Arbeitsumgebung (Strukturqualität) und der Transparenz der Abläufe (Prozessqualität) wird durch Mitarbeiter-Befragungen analysiert.

29.4.4 Partner und Lieferanten

Die Bewertung der externen Partner ist Bestandteil sowohl der QM wie auch der Datenschutz-Vorgaben:

- Lieferanten Audit nach QM ISO 9001
- AV Verträge nach DSGVO

Die Bewertungen werden regelmäßig wiederholt.

29.4.5 Statistiken und Auswertungen

Die Statistiken für QM und Datenschutz-Maßnahmen sind abhängig von der eingesetzten Software der Einrichtung und werden deshalb individuell definiert.

29.4.6 Audit

Nach der Datenschutz-Grundverordnung (DSGVO) sind Audits zur Prüfung der Einhaltung der Datenschutz-Anforderungen vorgesehen. Die Entwicklung dieser Anforderungen ist in Artikel 41 der DSGVO „Überwachung der genehmigten Verhaltensregeln“ beschrieben.

Langfristig sind Zertifizierungen für die DSGVO Rechtskonformität durch die EU-Behörden geplant. Diese werden dann auf Landesebene umgesetzt.

Von diesen Zertifizierungs-Audits sind die freiwilligen Konformitäts-Audits zu unterscheiden. Bei Letzteren handelt es sich um die Überwachung der Konformität mit den Verhaltensregeln der DSGVO.

Es werden 3 Audit Ebenen nach dem ISO Standard 19001 unterschieden:

- Ebene 1 (First Line Audit) wird durch interne Mitarbeiter oder externe Dienstleister auf freiwilliger Basis durchgeführt. Das Audit gibt der Leitung wesentliche Impulse für Optimierungs-Potentiale.
- Ebene 2 (Second Line Audit) wird außerhalb der eigenen Praxis durchgeführt und bezieht sich auf die AV Vertragspartner (sogenannte Lieferantenaudits)
- Ebene 3 (Third Line Audit) wird durch einen offiziellen Auditor in einem Zertifizierungs- (oder Akkreditierungs-) Prozess durchgeführt.

Solange noch keine offiziellen Audits mit definierten Strukturen bekannt sind, können die Prüfverfahren der Aufsichtsbehörden als vorläufige Audit-ähnliche Verfahren angesehen werden.

29.5 Anwendungsbereich (Patientenversorgung)

Die Praxis/Klinik erstellt eine Aufstellung über den Anwendungsbereich der medizinischen Patientenversorgung. Dabei wird unterschieden nach:

- Standardleistungen des Fachbereichs
- Sonderleistungen
    - GKV Patienten
    - PKV Patienten

Die Prozesse der Patientenversorgungen werden im Anhang dokumentiert:

- Diagnostik
- Behandlungsplanung
- Therapien
- Überweisungen
-

29.6 Rechtliche Anforderungen nach SGB V QM RL §4

29.6.1 Messen und Bewerten von Qualitätszielen

Wesentliche Zielvorgaben zur Verbesserung der Patientenversorgung oder der Einrichtungsorganisation werden definiert, deren Erreichungsgrad erfasst, regelmäßig ausgewertet und gegebenenfalls Konsequenzen abgeleitet.

29.6.2 Erhebung des Ist-Zustandes und Selbstbewertung

Regelmäßige Erhebungen des Ist-Zustandes und Selbstbewertungen dienen der Festlegung und Überprüfung von konkreten Zielen und Inhalten des einrichtungsinternen Qualitätsmanagements.

29.6.3 Regelung von Verantwortlichkeiten und Zuständigkeiten

Die Organisationsstruktur, Verantwortlichkeiten, Zuständigkeiten und Entscheidungskompetenzen werden schriftlich, beispielsweise durch eine Tabelle, Grafik oder ein Organigramm, festgelegt. Dabei werden wesentliche Verantwortlichkeiten besonders für alle sicherheitsrelevanten Prozesse berücksichtigt.

29.6.4 Prozess- bzw. Ablaufbeschreibungen

Die wesentlichen Prozesse der Patientenversorgung und der Einrichtungsorganisation werden einrichtungsspezifisch identifiziert, geregelt und beispielsweise in Form von Tabellen, Flussdiagrammen oder Verfahrensanweisungen dargestellt. Dabei werden die Verantwortlichkeiten, besonders für alle sicherheitsrelevanten Prozesse, in die Prozess- bzw. Ablaufbeschreibungen aufgenommen und fachliche Standards berücksichtigt.
Die Prozess- bzw. Ablaufbeschreibungen stehen den Mitarbeiterinnen und Mitarbeitern zur Verfügung und werden in festzulegenden Abständen überprüft und bei Bedarf angepasst. Alle beteiligten Mitarbeiterinnen und Mitarbeiter sollen diese nachvollziehen und ihre jeweilige Aufgabe ableiten können.

29.6.5 Schnittstellenmanagement

Ein systematisches Management an den Schnittstellen der Versorgung umfasst gezielte Kommunikation und abgestimmte Zusammenarbeit aller Beteiligten. Für eine sichere und patientenorientierte Versorgung sollen besonders die Übergänge entlang der gesamten Versorgungskette so gestaltet werden, dass alle erforderlichen Informationen zeitnah zur Verfügung stehen und eine koordinierte Versorgung gewährleistet ist.

29.6.6 Checklisten

In Checklisten werden Einzelaspekte eines Prozesses systematisiert, um deren verlässliche Umsetzung zu gewährleisten. Dies ist bei sicherheitsrelevanten Prozessen von besonderer Bedeutung. Das konsequente Anwenden von Checklisten, z.B. zur Vermeidung von Verwechslungen, unterstützt somit reibungslose Abläufe und ist ein bedeutsames Element einer Sicherheitskultur.
Bei operativen Eingriffen, die unter Beteiligung von zwei oder mehr Ärztinnen bzw. Ärzten oder die unter Sedierung erfolgen, werden OP-Checklisten eingesetzt. Diese OP- Checklisten sollen einrichtungsspezifisch entwickelt und genutzt werden sowie alle am Eingriff Beteiligten einbeziehen. Insbesondere sind sie auf die Erkennung und Vermeidung unerwünschter Ereignisse und Risiken auszurichten, wie z. B. Patienten-, Eingriffs- und Seitenverwechslungen und schwerwiegende Komplikationen. Gleichzeitig beinhalten sie Fragen zum Vorhandensein und zur Funktion des erforderlichen Equipments.

29.6.7 Teambesprechungen

Es werden regelmäßig strukturierte Besprechungen mit den Mitarbeiterinnen und Mitarbeitern bzw. Teams durchgeführt, die allen Mitarbeiterinnen und Mitarbeitern ermöglichen, aktuelle Themen und Probleme anzusprechen.

29.6.8 Fortbildungs- und Schulungsmaßnahmen

Alle Mitarbeiterinnen und Mitarbeiter sollen regelmäßig an Fortbildungen mit unmittelbarem Bezug zur eigenen Tätigkeit teilnehmen. Art und Umfang der Fortbildungs- bzw. Schulungsmaßnahmen werden mit der Leitung einer Einrichtung abgestimmt und in ein auf die Mitarbeiterin und den Mitarbeiter abgestimmtes Konzept eingebunden.

29.6.9 Patientenbefragungen

Die Einrichtung führt regelmäßig Patientenbefragungen durch und wertet diese aus. Deren Ergebnisse geben der Leitung und den Mitarbeiterinnen und Mitarbeitern eine Rückmeldung über die Patientenzufriedenheit und die Qualität der Versorgung aus Patientenperspektive sowie gegebenenfalls Anhaltspunkte für Verbesserungsmaßnahmen. Möglichst sollten dafür validierte Patientenbefragungsinstrumente genutzt werden.

29.6.10 Mitarbeiterbefragungen

Es werden regelmäßig möglichst anonyme Mitarbeiterbefragungen durchgeführt. Zweck der Befragung ist es, Informationen aus der Mitarbeiterperspektive zu ermitteln, um hieraus Veränderungsmaßnahmen – mit dem Ziel der Weiterentwicklung – abzuleiten.

29.6.11 Beschwerdemanagement

Die Einrichtung betreibt ein patientenorientiertes Beschwerdemanagement mit geregelter Bearbeitung der Beschwerden. Dazu gehört die Information der Patientinnen und Patienten über die persönliche oder anonyme Beschwerdemöglichkeit vor Ort. Die Rückmeldungen werden analysiert, bewertet und gegebenenfalls Veränderungsmaßnahmen daraus abgeleitet. Sofern möglich, erhalten die Beschwerdeführenden eine Rückmeldung über die gegebenenfalls eingeleiteten Maßnahmen.

29.6.12 Patienteninformation und -aufklärung

Zur Patienteninformation gehören Informations- und Aufklärungsmaßnahmen, die dazu beitragen, dass Patientinnen und Patienten besser im Behandlungsverlauf mitwirken und gezielt zur Erhöhung ihrer eigenen Sicherheit beitragen können. Für den gezielten Einsatz im individuellen Arzt-Patient-Kontakt wird eine Zusammenstellung zuverlässiger, verständlicher Patienteninformationen sowie von Angeboten von Selbsthilfeorganisationen und Beratungsstellen gepflegt.

29.6.13 Risikomanagement

Risikomanagement dient dem Umgang mit potenziellen Risiken, der Vermeidung und Verhütung von Fehlern und unerwünschten Ereignissen und somit der Entwicklung einer Sicherheitskultur. Dabei werden unter Berücksichtigung der Patienten- und Mitarbeiterperspektive alle Risiken in der Versorgung identifiziert und analysiert sowie Informationen aus anderen Qualitätsmanagement-Instrumenten, insbesondere die Meldungen aus Fehlermeldesystemen genutzt. Eine individuelle Risikostrategie umfasst das systematische Erkennen, Bewerten, Bewältigen und Überwachen von Risiken sowie die Analyse von kritischen und unerwünschten Ereignissen, aufgetretenen Schäden und die Ableitung und Umsetzung von Präventionsmaßnahmen. Ein relevanter Teil der Risikostrategie ist eine strukturierte Risikokommunikation.

29.6.14 Fehlermanagement und Fehlermeldesysteme

Der systematische Umgang mit Fehlern („Fehlermanagement“) ist Teil des Risikomanagements. Zum Fehlermanagement gehört das Erkennen und Nutzen von Fehlern und unerwünschten Ereignissen zur Einleitung von Verbesserungsprozessen in der Praxis.
Fehlermeldesysteme sind ein Instrument des Fehlermanagements. Ein Fehlerberichtsund Lernsystem ist für alle fach- und berufsgruppenübergreifend niederschwellig zugänglich und einfach zu bewerkstelligen. Ziel ist die Prävention von Fehlern und Schäden durch Lernen aus kritischen Ereignissen, damit diese künftig und auch für andere vermieden werden können. Die Meldungen sollen

freiwillig, anonym und sanktionsfrei durch die Mitarbeiterinnen und Mitarbeiter erfolgen. Sie werden systematisch aufgearbeitet und Handlungsempfehlungen zur Prävention werden abgeleitet, umgesetzt und deren Wirksamkeit im Rahmen des Risikomanagements evaluiert.

29.6.15 Notfallmanagement

Es wird eine dem Patienten- und Leistungsspektrum entsprechende Notfallausstattung und Notfallkompetenz, die durch regelmäßiges Notfalltraining aktualisiert wird, vorgehalten. Die Mitarbeiterinnen und Mitarbeiter sind im Erkennen von und Handeln bei Notfallsituationen geschult.

29.6.16 Hygienemanagement

Hygienemanagement umfasst den sachgerechten Umgang mit allen Hygieneassoziierten Strukturen und Prozessen einer Einrichtung und dient der Verhütung und Vorbeugung von Infektionen und Krankheiten. Dazu gehören z.B. auch der sachgerechte Einsatz antimikrobieller Substanzen sowie Maßnahmen gegen die Verbreitung multiresistenter Erreger.

29.6.17 Arzneimitteltherapiesicherheit

Arzneimitteltherapiesicherheit ist die Gesamtheit der Maßnahmen zur Gewährleistung eines optimalen Medikationsprozesses mit dem Ziel, Medikationsfehler und damit vermeidbare Risiken für die Patientin und den Patienten bei der Arzneimitteltherapie zu verringern. Die Einrichtung soll bei der Verordnung und Verabreichung von Arzneimitteln vermeidbare Risiken, die im Rahmen der Arzneimitteltherapie entstehen, durch geeignete Maßnahmen identifizieren, - durch geeignete Maßnahmen sicherstellen, dass einschlägige Empfehlungen im Umgang mit Arzneimitteln bekannt sind und - sicherstellen, dass angemessene Maßnahmen ergriffen werden, um Risiken im Medikationsprozess zu minimieren.

29.6.18 Schmerzmanagement

Bei Patientinnen und Patienten mit bestehenden sowie zu erwartenden Schmerzen erfolgt ein Schmerzmanagement von der Erfassung bis hin zur Therapie, das dem Entstehen von Schmerzen vorbeugt, sie reduziert oder beseitigt.

29.6.19 Maßnahmen zur Vermeidung von Stürzen bzw. Sturzfolgen

Sturzprophylaxe hat zum Ziel, Stürzen vorzubeugen und Sturzfolgen zu minimieren, in dem Risiken und Gefahren erkannt und nach Möglichkeit beseitigt oder reduziert werden. Dazu gehören Maßnahmen zur Risikoeinschätzung und vor allem adäquate Maßnahmen zur Sturzprävention.

29.6.20 Dokumentation

Die Praxis / Klinik überprüft die Umsetzung und Weiterentwicklung ihres Qualitätsmanagements im Sinne einer Selbstbewertung regelmäßig. Die Ergebnisse der Überprüfung werden für interne Zwecke dokumentiert

30 Anhang Rechtsvorschriften für Ärzte

Rechtsvorschriften für Ärzte	Gesetz
Arbeitsschutzgesetz	ArbSchG
Arbeitsstättenverordnung	ArbStätV
Arbeitszeitgesetz	ArbZG
Arzneimittelgesetz	AMG
Arzneimittel-Richtlinien	AMPL
Berufsgenossenschaftliche Vorschriften	BGV
Berufskrankheitenverordnung	BKV
Berufsordnung für Ärztinnen/Ärzte	MBO-Ä
Betäubungsmittelgesetz	BtMG
Betäubungsmittel-Verschreibungsverordnung	BtMVV
Biostoffverordnung	BioStoffV
Bundesärzteordnung	BÄO
Bundesdatenschutzgesetz	BDSG
Bürgerliches Gesetzbuch	BGB
Datenschutz Grundverordnung	DSGVO
Digitale Versorgung Gesetz	DVG
Gefahrstoff-Verordnung	GStV
Infektionsschutzgesetz	IfSG
Jugendarbeitsschutzgesetz	JArbSchG
Medizinprodukte-Betreiberverordnung	MPBetreibV
Medizinproduktegesetz	MPG
Medizinprodukte-Sicherheitsplanverordnung	MPSV
Patientendatenschutz Gesetz	PDSG
Patientenrechtegesetz	PatRechtG
Qualitätssicherungs-Vereinbarungen, Übersicht	SGB V
Richtlinien des Gemeinsamen Bundesausschusses, Übersicht	GBA
Röntgenverordnung	RöV
Schweigepflicht / Datenschutz Arztpraxen	MBO-Ä
Sozialgesetzbuch V	SGB V
Strafgesetzbuch	StGB
Strahlenschutz-Verordnung	StralSchV
Strukturverträge	StV
Terminvergabe / Service Gesetz	TSVG
Transfusionsgesetz	TFG
Unfallverhütungsvorschriften	UVV

31 Anhang Aufbewahrungsfristen

Liste der Aufbewahrungsfristen patientenbezogener Daten und medizinischer Unterlagen

Dokumente/Daten	Jahre	Rel. J / N	Ort	Datum	Verantw.
Ambulantes Operieren (Aufzeichnungen)	10 Jahre				
Arbeitsunfähigkeitsbescheinigungen (Durchschrift des gelben Dreifachsatzes, Teil C)	1 Jahr				
Arztakten	10 Jahre				
Arztbriefe (eigene und fremde)	10 Jahre				
Ärztliche Aufzeichnungen einschließlich Untersuchungsbefunde	10 Jahre				
Ärztliche Behandlungsunterlagen	10 Jahre				
Abrechnungsscheine (bei Diskettenabrechnung)	1 Jahr				
Aufzeichnungen (des Arztes in seiner Kartei)	10 Jahre				
Befunde	10 Jahre				
Berichte (Überweiser und Hausarzt)	10 Jahre				
Berufsunfähigkeitsgutachten	10 Jahre				
Betäubungsmittel BTM (BTM-Rezeptdurchschrift, -Karteikarten, BTM-Bücher)	3 Jahre				
Befundmitteilungen	10 Jahre				
Behandlung mit radioaktiven Stoffen und ionisierenden Strahlen	30 Jahre				
Blutprodukte (Anwendung von Blutprodukten sowie gentechnisch hergestellte Plasmaproteinen zur Behandlung von Hämastasestörungen)	30 Jahre				
Disease Management Programme (Unterlagen)	10 Jahre				
Durchgangsarzt / D-Arzt-Verfahren (ärztliche Unterlagen einschließlich Krankenblätter und Röntgenbilder)	15 Jahre				
EEG-Streifen	10 Jahre				

Dokumente/Daten	Jahre	Rel. J / N	Ort	Datum	Verantw.
EKG-Streifen nach Abschluss der Behandlung	10 Jahre				
Ersatzverfahren, Abrechnungsscheine	1 Jahr				
Gesundheitsuntersuchung (Teil B des Berichtsvordrucks nach der Untersuchung)	5 Jahre				
Gutachten über Patienten (für Krankenkasse, Versicherungen, Berufsgenossenschaften)	10 Jahre				
H-Ärzte (Behandlungsunterlagen einschließlich Röntgenbilder)	10 Jahre				
Häusliche Krankenpflege (Verordnung von) *	10 Jahre				
Heilmittelverordnungen (Verordnung von) *	10 Jahre				
Jugendarbeitsschutzuntersuchung (Untersuchungsbogen)	10 Jahre				
Jugendgesundheitsuntersuchung (Berichtsvordrucke, Dokumentation	5 Jahre				
Karteikarten (einschließlich ärztlicher Aufzeichnungen und Untersuchungsbefunde)	10 Jahre				
Koloskopie (Teil B des Berichtsvordrucks)	5 Jahre				
Kontrollkarten über interne Qualitätssicherung und Zertifikate über erfolgreiche Teilnahme an Ringversuchen	5 Jahre				
Krankenhausberichte (stationäre Behandlung) nach Abschluss der Behandlung	10 Jahre				
Krankenkassenanfragen (Durchschriften)	10 Jahre				
Krankenhausbehandlung (Verordnung, Krankenhauseinweisung Teil C)	10 Jahre				
Krankenhausberichte	10 Jahre				

Dokumente/Daten	Jahre	Rel. J / N	Ort	Datum	Verantw.
Kinderfrüherkennungs-untersuchungen (ärztliche Aufzeichnungen)	10 Jahre				
Krebsfrüherkennung Frauen (Berichtsvordruck Teil B)	5 Jahre				
Krebsfrüherkennung Frauen (Berichtsvordruck Teil A)	4 Quartale				
Krebsfrüherkennung Männer (Berichtsvordruck Teil B)	5 Jahre				
Krebsfrüherkennung Männer (Berichtsvordruck Teil A)	4 Quartale				
Laborqualitätssicherung (Kontrollkarten)	5 Jahre				
Labor (Zertifikate von Ringversuchen)	5 Jahre				
Labor (interne Qualitätssicherung)	5 Jahre				
Laborbuch	10 Jahre				
Laborbefunde	10 Jahre				
Langzeit EKG (Computerauswertung, keine Tapes)	10 Jahre				
Lungenfunktionsdiagnostik (Diagramme)	10 Jahre				
Notfallschein, Teil A (EDV abrechnende Ärzte)	1 Jahr				
Notfallschein, Teile B und C *	10 Jahre				
Patientenkartei (nach der letzten Behandlung)	10 Jahre				
Psychotherapie (Mitteilung der Krankenkasse)	10 Jahre				
Röntgen (Konstanzprüfungen und Dokumentation)	2 Jahre				
Röntgendiagnostik (Röntgenaufnahmen von Patienten über 18 Jahre. Die 10jährige Aufbewahrungsfrist beginnt erst ab dem 18. Lebensjahr bei Patienten, sodass alle Röntgenbilder von Kindern und Jugendlichen mindestens bis zur Vollendung des 28. Lebensjahres aufbewahrt werden müssen.)	10 Jahre				

Dokumente/Daten	Jahre	Rel. J / N	Ort	Datum	Verantw.
Röntgentherapie (Aufzeichnungen)	30 Jahre				
Sicherungsdiskette (Abrechnung mit der KV)	4 Jahre				
Sonographie (Aufzeichnungen, Fotos, Prints, Disketten)	10 Jahre				
Strahlenbehandlung, Röntgenbehandlung / -therapie (Aufzeichnungen, Berechnungen nach der letzten Behandlung)	30 Jahre				
Strahlendiagnostik, Röntgendiagnostik (Aufzeichnungen, Filme nach der letzten Untersuchung, auch mittels radioaktiven und ionisierenden Strahlen). Die 10jährige Aufbewahrungsfrist beginnt erst ab dem 18. Lebensjahr der Patienten, sodass alle Röntgenbilder von Kindern und Jugendlichen mindestens bis zur Vollendung des 28. Lebensjahres aufbewahrt werden müssen.	10 Jahre				
Strahlenschutzprüfung (Unterlagen)	5 Jahre				
Strahlenschutz (Unterlagen über Mitarbeiter-belehrung)	5 Jahre				
Transfusionsgesetz (siehe Blutprodukte)	15 Jahre				
Überweisungsschein (EDV abrechnende Ärzte, auch im Ersatzverfahren, auch Muster 7 Überweisung vor Aufnahme einer Psychotherapie)	1 Jahr				
Untersuchungsbefunde	10 Jahr				
Vertreterschein, Teil A (EDV abrechnende Ärzte)	1 Jahr				
Vertreterschein, Teile B und C *	10 Jahre				
Zertifikate von Ringversuchen	5 Jahre				

Dokumente/Daten	Jahre	Rel. J / N	Ort	Datum	Verantw.
Zytologie (Präparate und Befunde)	10 Jahre				
Zytologie (statistische Zusammenfassungen)	10 Jahre				

32 Anhang individuell

Alle relevanten, mitgeltenden Dokumente (Verfahrensanweisungen, Arbeitsanweisungen, Checklisten und Vereinbarungen) des ISMS, DSMS und QMS nach den vorstehenden Beschreibungen werden in den bestehenden Strukturen der Praxis / Klinik verwaltet.
Verweise können in einer „Cross Walk“ Matrix die Verbindungen zwischen den Dokumenten herstellen.

Verweise auf Primärdokumente die Grundlagen des vorliegenden ISMS-DSMS-QMS Kompendiums sind:

VdS Richtlinie 10000
https://vds.de/kompetenzen/cyber-security/zertifizierung/informationssicherheit-fuer-kmu-vds-10000

VdS Richtlinie 10010
https://vds.de/kompetenzen/cyber-security/zertifizierung/datenschutz-fuer-kmu-vds-10010-gem-dsgvo

GBA QM Richtlinie
https://www.g-ba.de/downloads/39-261-2434/2015-12-17_2016-09-15_QM-RL_Erstfassung_konsolidiert_BAnz.pdf

Weiterführende Informationen über das Autorenteam der MCSS AG, Köln
www.mcss-ag.de

Stephan Engels, Vorstandsvorsitzender, Geprüfter Datenschutzbeauftragter
Christian Fagel, Vorstand, Geprüfter Datenschutzbeauftragter und BSI Grundschutz Praktiker

Rainer Waedlich, Aufsichtsratsvorsitzender, Redaktionsleitung IS und QM
Claudia Wente-Waedlich, Aufsichtsrat, Redaktionsleitung QM und DS
Arno Zurstrassen, Aufsichtsrat, Anwalt für Medizinrecht, Rechtsaudit

MCSS AG, Köln, www.mcss-ag.de, Tel. 0221 474477-44