GUTcert
AFNOR Group

Checkliste
& praktische Hinweise zur Implementierung

ISO/IEC 27001
ISO 27799

... weil Ihr Knowhow am wichtigsten ist!

Einleitung

Eine Zertifizierung leichter machen

Ob Sie eine Zertifizierung nach EN ISO 13485 und ISO/IEC 27001 brauchen, ist keine Frage. Die Medizinbranche steht vor der großen Herausforderung, Entwicklung und Forschung mit den gesetzlichen Anforderungen im Bereich Qualitätsmanagement und Informationssicherheit zu vereinbaren.

Uns ist bewusst, dass Ihnen ein Zertifizierungsverfahren sehr wichtig, aber nicht der Kernbereich Ihres Geschäfts ist. Andererseits wissen wir als akkreditierte Zertifizierungsstelle, dass es unerlässlich ist, sich gründlich auf eine Zertifizierung vorzubereiten. Dabei wollen wir Ihnen mit dieser Checkliste helfen.

Unsere Checkliste hilft Ihnen:

- die richtigen Fragen zu stellen, um das Managementsystem Ihrer Organisation selbst zu prüfen
- Ihre Schwachstellen aufzudecken
- sich ohne tiefergehende Kenntnisse des Gesetzes auf das Audit vorzubereiten
- einen ersten Überblick darüber zu gewinnen, was der Auditor prüfen wird

Wie nutzen Sie die Checkliste erfolgreich?

Diese Checkliste ist als Hilfsmittel konzipiert, um die Komponenten der Informationssicherheit eines integrierten Managementsystems aus DIN EN ISO 13485:2016 und ISO/IEC 27001 für die Anwendung im Bereich medizinischer Software auf Vollständigkeit zu prüfen. Basis für eine entsprechende Zertifizierung ist dabei die ISO/IEC 27001, zu berücksichtigen sind aber auch weitere Anforderungen durch die ISO 27799 sowie andere Normen und gesetzliche Regelungen.

Die Gliederung orientiert sich an den verbindlichen Maßnahmen, die nach ISO/IEC 27001 implementiert werden müssen. Für die Umsetzung der einzelnen Maßnahmen empfehlen wir, die ausführlichen Erläuterungen in der ISO/IEC 27002 mit heranzuziehen. Für viele Maßnahmen gibt es weiterhin Ergänzungen in der ISO 27799, die speziell auf die Umsetzung im Gesundheitswesen abzielen.

Während alle Maßnahmen der ISO/IEC 27001 verbindlich einzuführen sind (ggf. mit Ausnahme nicht zutreffender Anforderungen), unterscheidet die für den Umgang mit medizinischen Werten (i. S. d. Norm) im Gesundheitswesen wichtige ISO 27799 zwischen verbindlichen und fakultativen Forderungen. Diese sind im englischen Original mit „shall“ und „should“ bezeichnet und in unserer Checkliste entsprechend formuliert.

Wird in der Checkliste das Wort „dokumentiert“ verwendet, so ist hiermit eine dokumentierte Information im Sinne der DIN EN ISO 9001 gemeint. Die Formatierung [Hinweis] kennzeichnet einen solchen.

In der Checkliste wird der Begriff „subject of care“ der DIN EN ISO 27799 immer synonym mit dem Wort „Patient“ verwendet. Die Daten des Patienten sind dann entsprechend der DSGVO die „Gesundheitsdaten“.

Nr.	Fragen	Bemerkungen
1	**Grunddaten**	
0.01	Geltungsbereich des gewünschten Zertifikates (Standorte und Tätigkeiten)	
0.02	Anzahl der Mitarbeiter	
4.01	Werden die für das ISMS relevanten internen und externen Aspekte bestimmt und bewertet? (Z.B. ortsbezogen, gesetzlich, technisch, ökonomisch, kulturell, sozial?)	
4.02	Werden die für das ISMS relevanten Stakeholder und deren Erwartungen ermittelt?	
4.03	Werden diese Informationen regelmäßig aktualisiert und bewertet?	
4.04	Ist der Anwendungsbereich des ISMS (auch in Bezug auf ausgelagerte Dienstleistungen) dokumentiert? [Passt der Anwendungsbereich zu dem der DIN EN ISO 13485?]	
4.05	Berücksichtigt er den Kontext der Organisation und die Anforderungen der Stakeholder?	
4.06	Werden die Schnittstellen interner & externer Tätigkeiten bestimmt und dokumentiert?	
4.07	Wird das eingeführte ISMS aufrecht-erhalten und fortlaufend verbessert?	
5.01	Nimmt das Top Management (ToM) seine Führungsverantwortung für das ISMS wahr?	
5.02	Übernimmt es Verantwortung für seine Effektivität?	
5.03	Sind Informationssicherheits-Politik und Informationssicherheits-Ziele mit Kontext und Strategie vereinbar?	
5.04	Werden ausreichende Ressourcen geplant (Budget)?	
5.05	Kommuniziert das ToM das ISMS und ist Vorbild?	
5.06	Stellt es sicher, dass geplante Ergebnisse erreicht werden?	
5.07	Unterstützt das ToM Führungskräfte und andere für das ISMS relevante Personen?	

5.08	Fördert es Verbesserungen des ISMS?	
5.09	Hat das ToM eine Informationssicherheits-Politik aufgestellt, die der Strategie, dem Zweck und dem Kontext der Organisation angemessen ist und hält es diese aktuell?	
5.10	Enthält die Informationssicherheits-Politik eine Verpflichtung zur Erfüllung von (zutreffenden) Forderungen und zur kontinuierlichen Verbesserung des ISMS?	
5.11	Wird die Informationssicherheits-Politik dokumentiert, intern kommuniziert und allen Interessierten zur Verfügung gestellt?	
5.3	**Verantwortung und Befugnisse**	
5.12	Stellt das ToM sicher, dass Verantwortlichkeiten und Befugnisse für relevante Aufgaben im ISMS zugewiesen und kommuniziert werden?	
5.13	Wird das ToM regelmäßig über die Leistung des ISMS informiert?	
A.5	**Informationssicherheitsrichtlinien**	
A.5.1.1	Ist ein Satz Informationssicherheitsrichtlinien festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht? Diese Richtlinien sollten Folgendes enthalten: a) die Notwendigkeit des Schutzes der Gesundheitsdaten? b) Ziele des Schutzes der Gesundheitsdaten? c) Anwendungsbereich bzgl. externer Anforderungen (wie in A.18)? d) gesetzliche, regulatorische und vertragliche Anforderungen, auch in Bezug auf den Schutz der persönlichen Gesundheitsdaten sowie gesetzliche und ethische Anforderungen an Gesundheitspersonal? e) Vorkehrungen für die Meldung von Vorfällen im Bereich der Informationssicherheit, einschließlich einem Kanal, über den Bedenken hinsichtlich der Vertraulichkeit geäußert werden können, ohne Angst vor Tadel oder Schuldzuweisungen? f) die Identifikation von Prozessen und Systemen, die Patienten Schaden zufügen können? § DIN EN ISO 27799	

A.5.1.2	Werden die Informationssicherheitsrichtlinien in geplanten Abständenüberprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind? Werden die Informationssicherheitsrichtlinien mindestens jährlich und nach Sicherheitsvorfällen oder jeweils nach erheblichen Änderungen überprüft? [Die DIN EN ISO 27799 nennt weiterhin die Punkte a) bis h) explizit, diese treffen aber auf Hersteller nur eingeschränkt zu]. § DIN EN ISO 27799 5.1.2	
A.6	**Organisation der Informationssicherheit**	
A.6.1.1	Sind alle Informationssicherheitsverantwortlichkeiten klar festgelegt und zugeordnet? Gibt es ein ISMF (Informationssicherheitsmanagement-Forum) um sicherzustellen, dass es eine klare Ausrichtung und sichtbare Unterstützung des Managements für Sicherheitsinitiativen gibt, die die Sicherheit von Gesundheitsinformationen betreffen? Ist mindestens eine Person benannt für die Sicherheit von Gesundheitsinformationen benannt? Tritt das Forum für die Sicherheit von Gesundheitsinformationen regelmäßig (annähernd) einmal im Monat zusammen? Gibt es eine formelle Erklärung zum Geltungsbereich, die die Grenzen der Compliance-Aktivitäten in Bezug auf Personen, Prozesse, Orte, Plattformen und Anwendungen festlegt? § DIN EN ISO 27799 6.1.1 und B1 B4	
A.6.1.2	Sind miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren? Sind Gesundheitsdaten als Werte identifiziert, die mit besonderer Sorgfalt zu verarbeiten sind? § DIN EN ISO 27799 6.1.2	
A.6.1.3	Werden angemessene Kontakte mit relevanten Behörden gepflegt?	
A.6.1.4	Werden angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheits-orientierten Expertenforen und Fachverbänden gepflegt?	

A.6.1.5	Wird die Informationssicherheit im Projektmanagement berücksichtigt, ungeachtet der Art des Projekts? Werden die Risiken für die Patientensicherheit in jedem Projekt, das die Verarbeitung personenbezogener Gesundheitsdaten enthält, sorgfältig analysiert und explizit angegangen? § DIN EN ISO 27799 6.1.5	
A.6.2.1	Sind eine Richtlinie und unterstützende Sicherheitsmaßnahmen umgesetzt, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben? a) Wird speziell auf die Risiken bei der Verwendung mobiler Geräte im Gesundheitswesen eingegangen? b) Ist eine Richtlinie über die Vorkehrungen, die bei der Nutzung mobiler Computergeräte innerhalb der Organisation zu treffen sind, gemeinsam mit den Maßnahmen zur Einhaltung der gesetzlichen Datenschutzbestimmungen eingeführt? c) Wird von den Anwendern verlangt, dass sie sich an diese Richtlinie halten? Ist erkennbar, dass die Richtlinie die besonderen Gefahren der drahtlosen Kommunikation adressiert (Benutzung veralteter Standards)? Wird auf die Gefahr fehlender Backups für Daten von Mobilgeräten eingegangen? § DIN EN ISO 27799 6.2.1	
A.6.2.2	Sind eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, umgesetzt?[1] a) Sind in der Richtlinie die bei der Telearbeit zu treffenden Vorsichtsmaßnahmen enthalten? b) Ist sichergestellt, dass die Nutzer von Gesundheitsinformationssystemen bei der Telearbeit diese Richtlinie einhalten? § DIN EN ISO 27799 6.2.2 § 9 Abs. 1 MBO-Ä, § 203 Abs. 1 StGB	

[1] In Deutschland besteht die Regelung nach § 9 Abs. 1 MBO-Ä (ärztliche Schweigepflicht) die nach § 203 Abs. 1 StGB strafbewehrt ist. Allerdings wurde §203 neu gefasst und enthält nun die „sonstigen mitwirkenden Personen", es ist also vor diesem Hintergrund notwendig diesen speziellen Personenkreis zu berücksichtigen. Diese Änderung war zum Zeitpunkt, als die DIN EN ISO 27799 gültig wurde, noch nicht Bestandteil des § 203.

6	Planung	
6.1.1	**Risiken und Chancen**	
6.01	Werden in der Planung des ISMS der Kontext und die Stakeholder berücksichtigt, daraus Chancen und Risiken bestimmt und Maßnahmen zum Umgang damit systematisch geplant und umgesetzt?	
6.02	Wird die Wirksamkeit der Maßnahmen bewertet?	
6.1.2	**IS- Risikobeurteilung**	
6.03	Wird ein Prozess zur Informationssicherheitsrisikobeurteilung (ISRB) angewendet und dessen Ergebnisse dokumentiert?	
6.04	Wird im Prozess festgelegt, welche Kriterien zur Risikoakzeptanz einer IRSB angewendet werden?	
6.05	Sichert der Prozess, dass wiederholende IRSB zu konsistenten, gültigen und vergleichbaren Ergebnissen führt?	
6.06	Werden im Prozess Risiken und deren Eigentümer identifiziert?	
6.07	Werden durch die IRSB, die Informationssicherheitsrisiken analysiert, indem die Risikofolgen abgeschätzt, die Eintrittswahrscheinlichkeit der Risiken abgeschätzt, die Risikoniveaus bestimmt werden?	
6.08	Werden durch die IRSB die Risiken bewertet, indem die Ergebnisse der IRSB mit den festgelegten Kriterien zur Risikoakzeptanz verglichen, die Ergebnisse der Analyse für die Risikobehandlung priorisiert werden?	
6.1.3	**IS-Risikobehandlung / SoA**	
6.09	Wird ein Prozess zur Informationssicherheitsrisikobehandlung (ISRBH) angewendet und dessen Ergebnisse dokumentiert?	
6.10	Werden aus den Ergebnissen der Risikobeurteilung Optionen für die ISRBH abgeleitet?	

6.11	Sind alle erforderlichen Maßnahmen bezüglich der gewählten Optionen der ISRBH sowie unter Berücksichtigung der ISO 27001 Anhang A und ISO 27799 festgelegt?	
6.12	Wurde ein Dokument „Erklärung zur Anwendbarkeit“ (SoA) erstellt und wird es fortlaufend aktualisiert?	
6.13	Sind im SoA alle Maßnahmen nach ISO 27001 Anhang A, ISO 27799[2] sowie ggf. zusätzliche Maßnahmen enthalten?	
6.14	Werden in der SoA aufgeführt: Gründe für die Einbeziehung aller Maßnahmen, der Stand der Umsetzung der Maßnahmen und Gründe für die Nicht-Einbeziehung von Maßnahmen aus dem Anhang A der ISO 27001, und der ISO 27799?	
6.15	Wurde ein Plan für die ISRBH erstellt und wurde dieser durch die Risikoeigentümer akzeptiert und genehmigt?	
6.2	**IS-Ziele**	
6.16	Sind – abgeleitet aus der Informationssicherheits-Politik – S.M.A.R.T.e Informationssicherheitsziele und Ressourcen für alle relevanten Funktionseinheiten festgelegt und dokumentiert?	
6.17	Ist festgelegt, wie die Ergebnisse kontrolliert und bewertet werden?	
6.18	Werden dabei anwendbare (gesetzliche, Kunden-) Forderungen sowie die Ergebnisse der ISRB und ISRBH berücksichtigt?	
6.19	Werden die Ziele kommuniziert, regelmäßig überwacht und bei Bedarf angepasst?	

[2] Die weiteren Maßnahmen aus der DIN EN ISO 27799 sind als Unterpunkte in Maßnahmen der ISO/IEC 27001 verborgen und tragen vierstellige Nummern: A 14.1.1.1, A 14.1.1.2 und 14.1.3.1.

7	Unterstützung	
7.1	**Ressourcen**	
7.01	Werden alle Ressourcen (finanziell, personell, Infrastruktur) zum Betrieb und zur kontinuierlichen Verbesserung des ISMS definiert und bereit gestellt?	
A.8	**Verwaltung der Werte**	
A.8.1.1	Sind Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, erfasst und wurde ein Inventar dieser Werte erstellt und wird dieses gepflegt? a) Sind Gesundheitsdaten berücksichtigt? b) Verfügt die Organisation über einen Verantwortlichen für die Gesundheitsdaten (siehe auch A.8.1.2)? c) Sind Regeln für die Nutzung dieser Daten festgelegt, dokumentiert und umgesetzt? § DIN EN ISO 27799 8.1.1.	
A.8.1.2	Gibt es für alle Werte, die im Inventar geführt werden, Zuständige? Wird der besondere Wert von Patientendaten angemessen berücksichtigt (einschließlich juristischer und ethischer Fragen, z.B. zu Datenschutz, Dateneigentum, Beauftragten)? § DIN EN ISO 27799 8.1.2	
A.8.1.3	Sind Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, aufgestellt sowie dokumentiert und werden diese angewendet?	
A.8.1.4	Geben alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurück? Sind dabei Gesundheitsdaten ausreichend berücksichtigt? Werden personenbezogene Gesundheitsinformationen in elektronischer Form auf allen einschlägigen Systemen aktualisiert und anschließend sicher von allen Geräten gelöscht, auf denen sie sich befunden haben? § DIN EN ISO 27799 8.1.4	

A.8.2.1	Ist Information anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert? Wird dabei berücksichtigt, dass die Anforderungen an die Vertraulichkeit individuell sehr unterschiedlich ausgeprägt sein können und daher alle personenbezogenen Patientendaten zu jeder Zeit angemessen zu schützen sind? Wird dabei berücksichtigt, dass für bestimmte Patienten ggf. erhöhte Maßnahmen notwendig sind? (Prominente, Politiker, etc.)? Beachtet die Organisation das Gebot der Datensparsamkeit nach DSGVO? § DIN EN ISO 27799 8.2.1 § Verordnung (EU) 2016/679 (DSGVO)	
A.8.2.2	Ist ein angemessener Satz von Verfahren zur Kennzeichnung von Information entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt? Informieren alle Patienteninformationssysteme, die personenbezogene Gesundheitsdaten verarbeiten, die Benutzer über die Vertraulichkeit personenbezogener Gesundheitsinformationen, die über das System zugänglich sind (z. B. beim Start oder bei der Anmeldung), und werden Ausdrucke als vertraulich gekennzeichnet, wenn sie personenbezogene Gesundheitsdaten enthalten? § DIN EN ISO 27799 8.2.2	
A.8.2.3	Sind Verfahren für die Handhabung von Werten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt?	
A.8.3.1	Sind Verfahren für die Handhabung von Wechseldatenträgern entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt? Werden Wechseldatenträger mit personenbezogenen Gesundheitsinformationen entweder physisch geschützt oder sind ihre Daten verschlüsselt? Wird der Status und der Standort von Datenträgern, die unverschlüsselte personenbezogene Gesundheitsdaten enthalten, überwacht? § DIN EN ISO 27799 8.3.1	

A.8.3.2	Werden nicht mehr benötigte Datenträger sicher und unter Anwendung formaler Verfahren entsorgt? Werden alle Patientendaten sicher gelöscht oder die Datenträger zerstört, wenn die Daten nicht länger benötigt werden? Hat die Organisation erkannt, das dies auch für Daten gilt, die in Medizinprodukten gespeichert sind? § DIN EN ISO 27799 8.3.2	
A.8.3.3	Sind Datenträger, die Information enthalten, während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt?	
7.2	**Kompetenz**	
7.3	**Bewusstsein**	
7.02	Werden für interne und externe Personen, die Informationssicherheitsrelevante Tätigkeiten ausführen, die notwendigen Kompetenzen bestimmt?	
7.03	Wird erforderlicher Schulungsbedarf ermittelt?	
7.04	Wird die Wirksamkeit von Schulungsmaßnahmen bewertet?	
7.05	Können die verantwortlichen Personen ihre Kompetenzen und deren Aufrechterhaltung **dokumentiert** nachweisen?	
7.06	Kennen alle Personen (interne & externe), die im Auftrag tätig werden, die Informationssicherheits-Politik, Informationssicherheits-Ziele und die Bedeutung ihrer Tätigkeit an der Wirksamkeit des ISMS?	
7.07	Haben diese Personen ein ausreichendes Bewusstsein über die Einhaltung der Regelungen zur Informationssicherheit erlangt?	
A.7	**Personalsicherheit**	
A.7.1.1	Werden alle Personen, die sich um eine Beschäftigung bewerben, einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist?	

	Hat die Organisationen sichergestellt, dass von Mitarbeitern, Auftragnehmern oder Freiwilligen, die personenbezogene Gesundheitsdaten verarbeiten (oder von denen erwartet wird, dass sie sie verarbeiten), zumindest die Identität, die aktuelle Adresse und die vorherige Beschäftigung dieser Mitarbeiter, Auftragnehmer und Freiwilligen zum Zeitpunkt der Bewerbung überprüft wird? Ist festgelegt, dass die Überprüfung des Hintergrunds aller Bewerber für eine Beschäftigung die einschlägige berufliche Qualifikationen im Gesundheitswesen umfassen sollte, sofern diese beruflich anerkannt ist (z. B. Ärzte, Krankenschwestern usw.)? Ist bei der Einstellung einer Person für eine bestimmte Aufgabe im Bereich der Informationssicherheit sichergestellt, dass der Kandidat: a) über die erforderliche Kompetenz für die Ausübung der Sicherheitsfunktion verfügt; b) dass man ihm die Rolle zutraut, vor allem, wenn sie für die Organisation von entscheidender Bedeutung ist? § DIN EN ISO 27799 7.1.1	
A.7.1.2	Sind in den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern deren Verantwortlichkeiten und diejenigen der Organisation festgelegt?3 Hat die Organisation, deren Mitarbeiter mit der mit der Verarbeitung personenbezogener Gesundheitsdaten befasst sind, dies in den entsprechenden Stellenbeschreibungen dokumentiert? Sind die in der Informationssicherheitsrichtlinie der Organisation festgelegten Sicherheitsrollen und Verantwortlichkeiten ebenfalls in den entsprechenden Stellenbeschreibungen dokumentiert werden? Ist zu erkennen, dass ein besonderes Augenmerk auf die Aufgaben und Zuständigkeiten von Zeit- oder Kurzzeitmitarbeitern (wie Vertretungskräften, Studenten, Praktikanten usw.) zu richten ist? Ist sichergestellt, dass Mitarbeiter oder Auftragnehmer verpflichtet sind, Verstöße gegen die der Sicherheit von Gesundheitsinformationen oder der Privatsphäre von Patienten zu melden? § DIN EN ISO 27799 7.1.2	

[3] DIN EN ISO 27799 enthält im Abschnitt 7.1.2 weitere Hinweise zur Sicherheitsüberprüfung von Personal.

A.7.2.1	Verlangt die Leitung von allen Beschäftigten und Auftragnehmern, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen? Hat die Organisation berücksichtigt, dass ein besonderes Gewicht auf die Belange von Patienten zu legen ist, die nicht möchten, dass ihre persönlichen Gesundheitsdaten von Angehörigen des Gesundheitswesens, die Nachbarn, Kollegen oder Verwandte sind, eingesehen werden? Werden andererseits auch Mitarbeiter nicht unnötig in die Lage versetzt, Informationen über Freunde, Verwandte oder Nachbarn zu überprüfen? § DIN EN ISO 27799 7.2.1	
A.7.2.2	Bekommen alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind? Hat die Organisation sichergestellt, dass Aus- und Weiterbildung zur Informationssicherheit nach der Einstellung und im Rahmen regelmäßiger Aktualisierungen der organisatorischen Sicherheitsrichtlinien und -verfahren für alle Mitarbeiter und gegebenenfalls externe Auftragnehmer, Forscher, Studenten und Freiwillige, die personenbezogene Gesundheitsdaten verarbeiten, durchgeführt wird? Werden die Mitarbeiter der Organisation und gegebenenfalls die externen Auftragnehmer über Disziplinarverfahren und Konsequenzen bei Verstößen gegen die Informationssicherheit aufgeklärt? § DIN EN ISO 27799 7.2.2	
A.7.2.3	Ist ein formal festgelegter und bekanntgegebener Maßregelungsprozess eingerichtet, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben? Gehen die Disziplinarverfahren der Organisation bei Verstößen gegen die Informationssicherheit nach Verfahren vor, die sich in den Richtlinien widerspiegeln und somit den Betroffenen des Disziplinarverfahrens bekannt sind? Entsprechen sie geltendem Recht und den Vereinbarungen, die zwischen der Organisation und den Berufsverbänden getroffen wurden? § DIN EN ISO 27799 7.2.3	

A.7.3.1	Sind Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt?	
7.4	**Kommunikation**	
7.08	Ist festgelegt, wer, worüber, wann, wie und mit wem intern & extern zum ISMS kommuniziert?	
7.09	Ist insbesondere die Kommunikation im Fall von Informationssicherheitsvorfällen geregelt?	
A.11	**Physische und umgebungsbezogene Sicherheit**	
A.11.1.1	Sind Sicherheitsperimeter zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, festgelegt und werden diese verwendet? Hat die Organisation erkannt, dass Einrichtungen, die Patientendaten verarbeiten, in Sicherheitsbereichen betrieben werden sollen? § DIN EN ISO 27799 11.1.1	
A.11.1.2	Sind Sicherheitsbereiche durch eine angemessene Zutrittssteuerung geschützt, um sicherzustellen, dass nur berechtigtes Personal Zugang hat? § DIN EN ISO 27799 11.1.2	
A.11.1.3	Ist die physische Sicherheit für Büros, Räume und Einrichtungen konzipiert und wird diese angewendet?	
A.11.1.4	Ist ein physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen konzipiert und wird dieser angewendet?	
A.11.1.5	Sind Verfahren für das Arbeiten in Sicherheitsbereichen konzipiert und werden diese angewendet?	
A.11.1.6	Werden Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, überwacht und sind diese, falls möglich, von informationsverarbeitenden Einrichtungen getrennt, um unbefugten Zutritt zu verhindern?	

A.11.2.1	Sind Geräte und Betriebsmittel so platziert und geschützt, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind? Sind alle Arbeitsplätze, die Zugang zu personenbezogenen Gesundheitsinformationen ermöglichen, so aufgestellt, dass eine unbeabsichtigte Einsichtnahme oder ein unbeabsichtigter Zugriff durch Betroffene und die Öffentlichkeit verhindert wird? Sind elektromagnetische Felder oder Strahlung von Medizinprodukten als Umweltbedingung identifiziert? § DIN EN ISO 27799 11.2.1	
A.11.2.2	Sind Geräte und Betriebsmittel vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt?	
A.11.2.3	Sind Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung vor Unterbrechung, Störung oder Beschädigung geschützt?	
A.11.2.4	Werden Geräte und Betriebsmittel instand gehalten, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen? Wurde die Abschirmung von Geräten in Bereichen mit hohen Emissionen von Medizinprodukten eingehend erwogen? § DIN EN ISO 27799 11.2.4	
A.11.2.5	Werden Geräte, Betriebsmittel, Information oder Software nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt? Wurde der besondere Bezug zu Patientendaten berücksichtigt? § DIN EN ISO 27799 11.2.5	
A.11.2.6	Werden Werte außerhalb des Standorts gesichert, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen? Ist sichergestellt, dass jede Verwendung von Medizinprodukten, die Daten aufzeichnen oder wiedergeben, außerhalb ihrer Räumlichkeiten genehmigt wurde? Gilt dies auch für Geräte, die von externen Mitarbeitern verwendet werden, selbst wenn die Nutzung ein wesentliches Merkmal der Rolle des Mitarbeiters ist, wie z. B. bei Sanitätern, Therapeuten usw.)? § DIN EN ISO 27799 11.2.6	

A.11.2.7	Werden alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind? Werden alle Datenträger (einschließlich in Geräten eingebaute), die Anwendungssoftware für Patientendaten oder Patientendaten enthalten, sicher gelöscht oder vernichtet, wenn sie nicht mehr benötigt werden? § DIN EN ISO 27799 11.2.7	
A.11.2.8	Stellen Benutzer sicher, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind?	
A.11.2.9	Werden Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen angewendet?	
8	**Betrieb**	
8.1	**Betriebliche Planung und Steuerung**	
8.01	Werden die im SoA und in den Zielen definierten Maßnahmen umgesetzt und dokumentiert?	
8.02	Werden auch die Ressourcen dafür geplant?	
8.03	Werden die Auswirkungen unbeabsichtigter Änderungen bewertet und ggf. gemindert?	
8.04	Werden ausgelagerte Prozesse in das ISMS einbezogen? (Festlegung, Überwachung, Bewertung)?	
8.05	Werden in regelmäßigen Abständen, oder bei erheblichen Veränderungen Informationssicherheitsbeurteilungen durchgeführt und dokumentiert?	

A.9	Zugangssteuerung	
A.9.1.1	Ist eine Zugangssteuerungsrichtlinie auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft? Enthält diese Richtlinie auch die Anforderung zur Dokumentation von Zugangsberechtigungen? Wird der Zugang zu Gesundheitsdaten auf die Personen beschränkt, die diesen Zugang benötigen und dabei ggf. auch nur auf Daten von spezifischen Patienten? Sind dabei auch Regelungen für Zugänge in Notfallsituationen aufgestellt?	
A.9.1.2	Haben Benutzer ausschließlich Zugang zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind?	
A.9.2.1	Ist ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen? Unterliegt der Zugang zu Gesundheitsinformationssystemen, die personenbezogene Gesundheitsdaten verarbeiten, einem förmlichen Benutzerregistrierungsverfahren? Stellen die Verfahren für die Benutzerregistrierung sicher, dass ein ausreichender Grad der Authentifizierung der behaupteten Benutzeridentität abhängig von Ausmaß der Zugangsberechtigung, gewährleistet wird? Werden die Angaben zur Benutzerregistrierung regelmäßig überprüft, um sicherzustellen, dass sie vollständig und korrekt sind und dass der Zugang weiterhin erforderlich ist? § DIN EN ISO 27799 9.2.1	
A.9.2.2	Ist ein formaler Prozess zur Zuteilung von Benutzerzugängen umgesetzt, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen? Ist in den Verfahren zur Bereitstellung des Benutzerzugangs eindeutig festgelegt, ob die Benutzer Zugang zu personenbezogenen Gesundheitsinformationen haben? § DIN EN ISO 27799 9.2.2	
A.9.2.3	Ist die Zuteilung und Gebrauch von privilegierten Zugangsrechten eingeschränkt und wird dieser gesteuert?	

	Werden bei der Zuteilung privilegierter Zugangsrechte Strategien nach dem Stand der Technik berücksichtigt?[4] Ermöglichen es die Gesundheitsinformationssysteme, den Benutzer (einschließlich Angehörige der Gesundheitsberufe, Hilfspersonal und andere) mit den Datensätzen von Patienten zu verknüpfen und den künftigen Zugang auf der Grundlage dieser Verknüpfung herzustellen? § DIN EN ISO 27799 9.2.3 [Weitere Hinweise zur Verwaltung von Zugriffsrechten im Gesundheitswesen finden sich in ISO 22600-1 und ISO 22600-2.]	
A.9.2.4	Wird die Zuordnung von geheimer Authentisierungsinformation über einen formalen Verwaltungsprozess gesteuert? Wird bei diesem Verfahren berücksichtigt, dass in Situationen mit Zeitdruck ein ausreichender Zugang gewährleistet wird? § DIN EN ISO 27799 9.2.4	
A.9.2.5	Überprüfen die für Werte Zuständigen in regelmäßigen Abständen die Benutzerzugangsrechte? Wie wird mit Benutzergruppen umgegangen, die Notfallbehandlungen durchführen, da sie Zugang zu Informationen benötigen, in denen die zu betreuende Person möglicherweise nicht in der Lage ist, ihre Zustimmung zu erteilen? § DIN EN ISO 27799 9.2.5	
A.9.2.6	Werden die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst? Wird sichergestellt, dass die Zugriffsrechte der Benutzer in Bezug auf die Patientendaten so bald wie möglich für alle ausscheidenden Mitarbeiter, externe Auftragnehmer oder Freiwillige bei Beendigung des Arbeitsverhältnisses, des Vertragsverhältnisses oder der Freiwilligentätigkeit entzogen werden? § DIN EN ISO 27799 9.2.6	

[4] Die DIN EN ISO 27799 versteht unter privilegierten Rechten auch solche, die Benutzern Zugriff auf Gesundheitsdaten gewähren. Diese sind im Sinne der DSGVO besonders sensibel, fallen aber nach Ansicht der Autoren dieser Checkliste nicht in den Abschnitt 9.2.3, sondern wären auch unter 9.2.2 zu betrachten. Ferner liefert die DIN EN ISO 27799 im Abschnitt 9.2.3 umfangreiche Beispiele zur Gestaltung von Sicherheitsrichtlinien.

A.9.3.1	Sind Benutzer verpflichtet, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen? § DIN EN ISO 27799 9.3.1	
A.9.4.1	Wird der Zugang zu Information und Anwendungssystemfunktionen entsprechend der Zugangssteuerungsrichtlinie eingeschränkt? Ist eine Zweifaktorauthentifizierung eingesetzt? Ist der Zugang zu Patientendaten vom Zugang zu anderer IT-Infrastruktur getrennt? Ist dabei der Zugriff von Patienten auf ihre eigenen Daten berücksichtigt und werden dabei auch behinderte Personen oder deren Stellvertretern einbezogen? § DIN EN ISO 27799 9.3.2	
A.9.4.2	Wird der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert, soweit es die Zugangssteuerungsrichtlinie erfordert?	
A.9.4.3	Sind Systeme zur Verwaltung von Kennwörtern interaktiv und stellen starke Kennwörter sicher?	
A.9.4.4	Ist der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, eingeschränkt und streng überwacht?	
A.9.4.5	Ist der Zugang zu Quellcode von Programmen eingeschränkt?	
A.10	**Kryptographie**	
A.10.1.1	Ist eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information entwickelt und umgesetzt? Werden die Richtlinien für die Ausstellung und Verwendung von digitalen Zertifikaten im Gesundheitswesen und für die Verwaltung von Schlüsseln beachtet? § DIN EN ISO 27799 10.1.1 § ISO 17090-3	
A.10.1.2	Ist eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln entwickelt und wird über deren gesamten Lebenszyklus umgesetzt?	

	Werden die Richtlinien für die Ausstellung und Verwendung von digitalen Zertifikaten im Gesundheitswesen und für die Verwaltung von Schlüsseln beachtet? § DIN EN ISO 27799 10.1.2 § ISO 17090-3	
A.12	**Betriebssicherheit**	
A.12.1.1	Sind Bedienabläufe dokumentiert und allen Benutzern, die sie benötigen, zugänglich?	
A.12.1.2	Werden Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen gesteuert? Beachtet der Änderungsprozess die Risiken der Änderung ausdrücklich, wird dies aufgezeichnet und bewertet? Wird dabei das Risiko einbezogen, dass unangemessene, unzureichend getestete oder fehlerhafte Änderungen bei der Verarbeitung von personenbezogenen Gesundheitsinformationen katastrophale Folgen für die Patientenversorgung und -sicherheit haben können? § DIN EN ISO 27799 12.1.2 § ISO/TS 14441	
A.12.1.3	Wird die Ressourcennutzung/Benutzung von Ressourcen überwacht und abgestimmt, und werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen?	
A.12.1.4	Sind Entwicklungs-, Test- und Betriebsumgebungen voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern? Sind Regeln für die Migration von Software vom Entwicklungs- zum Betriebsstatus von der Organisation, die die betroffene(n) Anwendung(en) betreibt, festgelegt und dokumentiert? § DIN EN ISO 27799 12.1.4	
A.12.2.1	Sind Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer umgesetzt?	

A.12.3.1	Werden Sicherheitskopien von Information, Software und Systemabbildern entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet? Wird eine Sicherungskopie aller personenbezogenen Gesundheitsdaten erstellt und in einer physisch sicheren Umgebung, aufbewahrt, um ihre künftige Verfügbarkeit zu gewährleisten? Werden die personenbezogene Gesundheitsdaten zum Schutz ihrer Vertraulichkeit in einem verschlüsselten Format gesichert? [Die DIN EN ISO 27799 geht als Stand der Technik hier über die Forderungen der DiGAV hinaus.] § DIN EN ISO 27799 12.3.1 § DiGAV[5]	
A.12.4.1	Werden Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, erzeugt, aufbewahrt und regelmäßig überprüft?[6] Wird jedes Mal ein sicherer Prüfdatensatz erstellt, wenn ein Benutzer über das System auf personenbezogene Gesundheitsinformationen zugreift, diese erstellt, aktualisiert oder archiviert? Identifiziert das Ereignisprotokoll eindeutig den Benutzer, das Datensubjekt (d. h. die betroffene Person), die vom Benutzer ausgeführte Funktion (Erstellung eines Datensatzes, Zugriff, Aktualisierung usw.) sowie Uhrzeit und Datum, an dem die Funktion durchgeführt wurde? Wird ein Datensatz mit dem früheren Inhalt der Daten und dem Ereignisprotokoll (d. h. wer die Daten zu welchem Zeitpunkt eingegeben hat) aufbewahrt, wenn personenbezogene Gesundheitsinformationen aktualisiert werden? Führen Nachrichtensysteme, die für die Übermittlung von Nachrichten mit personenbezogenen Gesundheitsdaten verwendet werden, ein Protokoll der Nachrichtenübertragungen (mit Zeit, Datum, Herkunft und Ziel der der Nachricht, nicht aber deren Inhalt)? Hat die Organisation die Aufbewahrungsfrist für diese Ereignisprotokolle unter besonderer Berücksichtigung der klinischen Berufsnormen und der rechtlichen Verpflichtungen	

[5] Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf: Werden auf nicht in der persönlichen Verfügung der nutzenden Person stehenden IT-Systemen verarbeitete personenbezogene Daten auf diesen Systemen nur verschlüsselt gespeichert?
[6] Die Anforderungen an die Ereignisprotokollierung werden in der ISO 27789 ausführlich behandelt.

	sorgfältig bewertet und festgelegt, damit bei Bedarf Untersuchungen durchgeführt werden können und gegebenenfalls der Nachweis von Missbrauch erbracht werden kann? Sind die Ereignisprotokollierungssysteme des Gesundheitsinformationssystems zu jeder Zeit in Betrieb, in der das überwachte Gesundheitsinformationssystem zur Verfügung steht? Sind die Gesundheitsinformationssysteme, die personenbezogene Gesundheitsinformationen enthalten, mit Einrichtungen zur Analyse von Protokollen und Prüfpfaden, die: a) die Identifizierung aller Systembenutzer ermöglichen, die in einem bestimmten Zeitraum auf die Akte(n) eines bestimmten Patientenzugegriffen oder diese geändert haben; b) die Identifizierung aller Patienten ermöglichen, auf deren Datensätze ein bestimmter Systembenutzer über einen bestimmten Zeitraum zugegriffen hat, ausgestattet? § DIN EN ISO 27799 12.4.1 § ISO 27789	
A.12.4.2	Sind Protokollierungseinrichtungen und Protokollinformation vor Manipulation und unbefugtem Zugriff geschützt? Sind die Prüf-Aufzeichnungen sicher und fälschungssicher? Ist der Zugang zu Systemprüfungsinstrumenten und Prüfpfaden gesichert, um Missbrauch oder Kompromittierung zu verhindern? Wird die Verwaltung der Prüfungsaufzeichnungen nach der internationalen Norm für die Verwaltung von Aufzeichnungen ISO 15489 durchgeführt? Sind die Sicherheitsanforderungen für die Archivierung von Prüfungsunterlagen entsprechen denen für die Archivierung von elektronischen Gesundheitsakten, die in ISO/TS 21547 festgelegt sind? Ist ein besonderes Augenmerk auf die Sicherheit von verteilten Prüfpfaden gelegt worden? Elektronische Krankenakten können über mehrere Informationssysteme verteilt sein und sich über verschiedene Domänen für Sicherheitsrichtlinien verteilen. Dies gilt auch für Prüfpfade. Wird die Sicherheit der logischen Prüfpfade beibehalten? Sieht das Prüfsystem ausreichende Maßnahmen vor, um zu gewährleisten, dass Einträge in den Prüfpfaden vorgenommen werden, wenn das Gesundheitsinformationssystem in Betrieb ist? Dokumentiert das Prüfsystem alle Fälle, in denen der Prüfpfad durch einen Systemausfall außer Betrieb, abgeschaltet oder durch einen Systemausfall nicht funktionsfähig war?	

	Meldet das Prüfsystem, welche Prüfungen zu einem bestimmten Zeitpunkt ein- oder ausgeschaltet sind? Hat die Organisation, die für die Führung eines Auditprotokolls verantwortlich ist, eine Aufbewahrungsrichtlinie festgelegt? Entspricht die Aufbewahrung der Prüfungsunterlagen den gesetzlichen Anforderungen und den einschlägigen Richtlinien? Ist die Aufbewahrung der Ereignisprotokolle an der Lebensdauer der Gesundheitsakten, Daten und Dokumente orientiert? Sieht das Prüfsystem ausreichende Sicherheitsmaßnahmen vor, um die Ereignisprotokolle vor Manipulationen zu schützen? a) Es muss den Zugang zu den Ereignisprotokollen sichern, b) es muss den Zugang zu den Audit-Tools des Systems sichern, um Missbrauch oder Kompromittierung zu verhindern, c) es protokolliert alle Eingriffe in den Prüfpfad in einem sicheren Protokoll mit Angabe von Zeitpunkt, Eingriff und Akteur, d) es muss alle Fälle dokumentieren, in denen der Prüfpfad außer Betrieb ist (z.B. durch Abschaltung oder einen Systemausfall) e) es meldet, welche Audits zu einem bestimmten Zeitpunkt aktiviert/deaktiviert sind. Ist der Zugang zu Prüfungsdaten streng kontrolliert und selbst Gegenstand einer Prüfung? Erfolgt der Zugang über ein geeignetes Informationssystem, das diese Kontrollen durchsetzen kann, und nicht direkt auf den Audit-Prüfpfad selbst? Ermöglichen die Prüfeinrichtungen eine Analyse des Prüfpfads nach beliebigen Datenfeldern im Protokoll, gegebenenfalls nach Datum/Zeitraum, entweder einzeln oder in Kombination (z. B. alle Zugriffe von Benutzer X, alle "Lösch"-Ereignisse von Benutzern der Rolle "Y", alle Ereignisse, die im letzten Monat das pflegebedürftige "Z" betrafen, usw.)? [In manchen Fällen kann es erforderlich sein, dass ein Prüf-Benutzer zusätzlich zum Prüfpfad auf weitere Informationsquellen zugreifen muss, um beispielsweise Muster zu erkennen (z. B. alle Suchvorgänge zu Kindern, die von einem Nutzer durchgeführt wurden, der kein Kinderarzt ist oder mit der Pädiatrie in Verbindung steht).][7] § DIN EN ISO 27799 12.4.2 § ISO 15489 § ISO/TS 21547	

[7] Anleitungen zur Langzeitarchivierung bei gleichzeitiger Sicherstellung der Datenintegrität finden sich auch in den Dokumenten IETF RFC 4810 Long-Term Archive Service Requirements und IETF RFC 4998 Evidence Record Syntax (ERS).

A.12.4.3	Werden Tätigkeiten von Systemadministratoren und Systembedienern aufgezeichnet und sind die Protokolle geschützt und werden diese regelmäßig überprüft?	
A.12.4.4	Werden die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder einem Sicherheitsbereich mit einer einzigen Referenzzeitquelle synchronisiert? Wird berücksichtigt, dass eine Verfolgung und Wiederherstellung von zeitlichen Abläufen in Gesundheitsinformationssystemen notwendig sein kann, falls zeitkritische gemeinsame Behandlungstätigkeiten durchgeführt werden? § DIN EN ISO 27799 12.4.4	
A.12.5.1	Sind Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb umgesetzt?	
A.12.6.1	Werden Informationen über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt, wird die Gefährdung der Organisation durch derartige Schwachstellen bewertet und werden angemessene Maßnahmen ergriffen, um das dazugehörige Risiko zu behandeln?	
A.12.6.2	Sind Regeln für die Softwareinstallation durch Benutzer festgelegt und umgesetzt?	
A.12.7.1	Werden Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhalten, sorgfältig geplant und vereinbart, um Störungen der Geschäftsprozesse zu minimieren?	
A.13	**Kommunikationssicherheit**	
A.13.1.1	Werden Netzwerke verwaltet und gesteuert, um Information in Systemen und Anwendungen zu schützen?	
A.13.1.2	Sind Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste bestimmt und werden diese sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufgenommen? Wird sorgfältig abgewogen, welche Auswirkungen der Verlust der Verfügbarkeit von Netzdiensten auf die klinische Praxis haben könnte?[8] § DIN EN ISO 27799 13.1.2	

[8] Siehe auch Abschnitt 17.

A.13.1.3	Werden Informationsdienste, Benutzer und Informationssysteme in Netzwerken gruppenweise voneinander getrennt gehalten?	
A.13.2.1	Sind formale Übertragungsrichtlinien, -verfahren und -maßnahmen vorhanden, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen? Hat die Organisationen sichergestellt, dass die Sicherheit eines solchen Informationsaustauschs Gegenstand der Erstellung von Richtlinien sowie der Prüfung der Einhaltung der Compliance ist (siehe Abschnitt 18).? Ist die Sicherheit des Informationsaustauschs durch die Verwendung von Vereinbarungen über den Informationsaustausch, in denen ein Mindestmaß an Kontrollen festgelegt ist, gewährleistet? Wurde ein besonderes Augenmerk auf die Benutzerfreundlichkeit von kryptographischen Werkzeugen gelegt, um deren Nutzung im Gesundheitswesen zu fördern und die Ablehnung von zu komplexen Werkzeugen zu vermeiden?[9] § DIN EN ISO 27799 13.2.1	
A.13.2.2	Behandeln Vereinbarungen die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien?[10]	
A.13.2.3	Ist Information in der elektronischen Nachrichtenübermittlung angemessen geschützt? Hat die Organisation Maßnahmen ergriffen, um die Vertraulichkeit und Integrität in der elektronischen Nachrichtenübermittlung zu gewährleisten? Sind Nachrichten, die Patientendaten enthalten, verschlüsselt?[11] § DIN EN ISO 27799 13.2.3	

[9] Siehe auch die gesundheitsspezifischen Implementierungsleitlinien unter 8.2.1.
[10] Wie in Abschnitt 13.2.1 erwähnt, finden sich in der ISO-Norm 22857 spezifische Leitlinien für den Austausch von Gesundheitsinformationen. Obwohl diese internationale Norm sich ausdrücklich auf den grenzüberschreitenden Fluss personenbezogener Gesundheitsinformationen bezieht (wobei die Grenzen in diesem Zusammenhang die Zuständigkeitsbereiche im Gesundheitswesen und nicht notwendigerweise die nationalen Grenzen sind), können viele ihrer Ratschläge bei Bedarf angepasst werden, um den Austausch von Daten zwischen zwei Organisationen zu regeln.
[11] Im Abschnitt Bibliography der DIN EN ISO 27799 findet sich eine Liste von Internationalen Normen zur Verwendung von digitalen Zertifikaten im Gesundheitswesen.

A.13.2.4	Werden Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, identifiziert, regelmäßig überprüft und sind diese dokumentiert? Verfügt die Organisation über eine Vertraulichkeitsvereinbarung, in der der vertrauliche Charakter der Gesundheitsinformationen festlegt ist? Gilt die Vereinbarung für alle Mitarbeiter, die Zugang zu Gesundheitsinformationen haben? § DIN EN ISO 27799 13.2.4	
A.14	**Anschaffung, Entwicklung und Instandhalten von Systemen**	
A.14.1.1	Sind die Anforderungen, die sich auf Informationssicherheit beziehen, in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen?[12] § ISO/TS 14441	
A.14.1.1.1	Kann die Organisation sicherstellen, dass jeder Patient innerhalb des Systems eindeutig identifiziert werden kann? Ist die Organisation in der Lage, doppelte oder mehrfache Datensätze zusammenzuführen, wenn festgestellt wird, dass mehrere Datensätze für ein und dieselbe Person unbeabsichtigt oder in einem medizinischen Notfall angelegt worden sind? Werden Gesundheitsinformationen nur im notwendigen Ausmaß gespeichert und wird dabei Datensparsamkeit (z.B. durch Löschen, Anonymisieren oder Pseudonymisieren) berücksichtigt? § DIN EN ISO 27799 14.1.1.1	
A.14.1.1.2	Kann die Organisation personenbezogene Identifizierungsinformationen zur Verfügung stellen, um den Angehörigen der Gesundheitsberufe dabei zu helfen, zu bestätigen, dass die abgerufenen elektronischen Gesundheitsdaten mit dem behandelten Patienten übereinstimmt? Kann gedruckter Information entnommen werden, dass sie vollständig ist (z. B. durch durchgehende Seitennummerierung)? § DIN EN ISO 27799 14.1.1.2	

[12] Die ISO/TS 14441 enthält einen detaillierten Satz von funktionalen Datenschutz- und Sicherheitsanforderungen für Electronic-Health-Record-Systeme

A.14.1.2	Sind Informationen, die durch Anwendungen oder Dienste über öffentliche Netzwerke übertragen werden, vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter Offenlegung sowie Veränderung geschützt? Kann die Organsiation sicherstellen, dass im elektronischen Geschäftsverkehr und bei Online-Transaktionen eventuell enthaltene Gesundheitsdaten angemessen geschützt werden?[13] § DIN EN ISO 27799 14.1.2	
A.14.1.3	Sind Informationen, die an Transaktionen bei Anwendungsdiensten beteiligt sind, so geschützt, dass unvollständige Übertragung, Fehlleitung, unbefugte Offenlegung, unbefugte Vervielfältigung oder unbefugte Wiederholung von Nachrichten verhindert wird?	
A.14.1.3.1	Werden öffentlich zugängliche Gesundheitsinformationen (im Unterschied zu persönlichen Gesundheitsinformationen) archiviert? Wird die Integrität der öffentlich zugänglichen Gesundheitsinformationen geschützt, um eine unbefugte Änderung zu verhindern? Wird die Quelle (Urheberschaft) von öffentlich zugänglichen Gesundheitsinformationen angegeben und ihre Integrität geschützt? § DIN EN ISO 27799 14.1.3	
A.14.2.1	Sind Regeln für die Entwicklung von Software und Systemen festgelegt und werden diese bei Entwicklungen innerhalb der Organisation angewendet?	
A.14.2.2	Werden Änderungen an Systemen innerhalb des Entwicklungszyklus durch formale Verfahren zur Verwaltung von Änderungen gesteuert?	
A.14.2.3	Werden bei Änderungen an Betriebsplattformen, geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder Organisationssicherheit gibt?	
A.14.2.4	Werden Änderungen an Softwarepaketen nicht gefördert, sind diese auf das Erforderliche beschränkt und unterliegen alle Änderungen einer strikten Steuerung?	

[13] Dies gilt inbesondere für Daten im Zusammenhang mit der Rechnungsstellung, medizinischen Forderungen, Rechnungszeilen, Bestellanforderungen und anderen Daten des elektronischen Geschäftsverkehrs, aus denen personenbezogene Gesundheitsinformationen abgeleitet werden können. Siehe auch 18.1.4 für eine Diskussion über die Zustimmung vor der Kommunikation außerhalb der Organisation.

A.14.2.5	Sind Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme festgelegt, dokumentiert, werden diese aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet?	
A.14.2.6	Sind sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus geschaffen und schützen diese angemessen?	
A.14.2.7	Wird die Tätigkeit ausgegliederter Systementwicklung beaufsichtigt und überwacht?	
A.14.2.8	Wird die Sicherheitsfunktionalität während der Entwicklung getestet?	
A.14.2.9	Sind für neue Informationssysteme, Aktualisierungen und neue Versionen Abnahmetestprogramme und dazugehörige Kriterien festgelegt? Sind Akzeptanzkriterien für geplante neue Informationssysteme, Upgrades und neue Versionen festgelegt? Werden vor der Abnahme geeignete Tests des Systems durchgeführt? Werden klinische Anwender in die Tests klinisch relevanter Systemfunktionen einbezogen? § DIN EN ISO 27799 14.2.9	
A.14.3.1	Werden Testdaten sorgfältig ausgewählt, geschützt und gesteuert? Ist sichergestellt, dass keine aktuellen persönlichen Gesundheitsdaten als Testdaten verwendet werden?[14] § DIN EN ISO 27799 14.3.1 § ISO/TS 14441	
A.15	**Lieferantenbeziehungen**	
A.15.1.1	Werden Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation mit dem Zulieferer vereinbart und sind diese dokumentiert? Werden die Risiken bewertet, die infolge des Zugriffs externer Parteien auf Gesundheitsdaten oder auf Systeme, die diese verarbeiten, entstehen? Werden Sicherheitsmaßnahmen eingeführt, die dem ermittelten Risiko und den eingesetzten Technologien angemessen sind?	

[14] ISO/TS 14441 enthält eine detaillierte Anleitung zur Konformitätsprüfung von Electronic-Health-Record-Systemen, einschließlich der Verwendung von Testdaten.

	Werden die Rechte der Betroffenen geschützt, auch wenn eine externe Partei mit potenziellem Zugang zu personenbezogenen Gesundheitsinformationen in einer anderen Rechtsordnung als derjenigen, die für die betroffene Person oder die Gesundheitsorganisation gilt, ansässig ist? § DIN EN ISO 27799 15.1.1	
A.15.1.2	Werden alle relevanten Informationssicherheitsanforderungen mit jedem Lieferanten festgelegt, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt und sind diese vereinbart?[15]	
A.15.1.3	Werden Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, in Vereinbarungen mit Lieferanten aufgenommen?	
A.15.2.1	Wird die Dienstleistungserbringung durch Lieferanten regelmäßig überwacht, überprüft und auditiert?	
A.15.2.2	Werden Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten gesteuert? Umfassen solche Änderungen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -verfahren und -maßnahmen und wird dabei die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet?	
A.17	**Informationssicherheitsaspekte beim Business Continuity Management**	
A.17.1.1	Sind Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen, z. B. Krise oder Katastrophe, bestimmt? Wird dabei berücksichtigt, dass in bestimmten Krisensituationen (z.B. Pandemien) die Verfügbarkeit der Gesundheitsversorgung eine besondere Rolle spielt und dabei auch Personalengpässe auftreten können?	
A.17.1.2	Sind Prozesse, Verfahren und Maßnahmen festgelegt, dokumentiert, umgesetzt und aufrechterhalten, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können?	

[15] Die Verwaltung von Drittanbieterdiensten wird erheblich vereinfacht, wenn eine formelle Vereinbarung getroffen wird, die ein Mindestsatz an Maßnahmen festlegt?

	Wurden Prozesse, Systeme und andere relevante Geräte identifiziert, die für die Gesundheitsversorgung wichtig sind? Wurden Ausweichverfahren für den Notfall in Betracht gezogen, um Ausfällen von Prozessen, Systemen und relevanten Ausrüstungen, die für die Gesundheitsversorgung von entscheidender Bedeutung sind, entgegenzuwirken? § DIN EN ISO 27799 17.1.2	
A.17.1.3	Werden die festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit in regelmäßigen Abständen überprüft, um sicherzustellen, dass diese gültig und in widrigen Situationen wirksam sind?	
A.17.2.1	Werden informationsverarbeitende Einrichtungen mit ausreichender Redundanz zur Einhaltung der Verfügbarkeitsanforderungen realisiert?	
9	**Leistungsbewertung**	
9.1	**Datenanalyse, -bewertung**	
9.01	Gibt es Vorgaben was, wie, wann überwacht oder gemessen werden muss, um Informationen und Daten zu bewerten und die Ergebnisse zu **dokumentieren**?	
9.02	Sind Methoden für die Analyse und Bewertung definiert?	
9.03	Werden Planungen effektiv umgesetzt?	
9.04	Wird die Leistung des ISMS insgesamt analysiert und bewertet und erfasst, ob es verbessert werden kann oder muss?	
9.2	**Internes Audit**	
9.05	Werden planmäßig interne Audits durchgeführt, um nachzuweisen, dass die Vorgaben der ISO/IEC 27001 und des ISMS eingehalten werden und wirksam umgesetzt sind?	
9.06	Wird in einem Auditprogramm festgelegt, wie häufig, wer, wie die Audits durchführt, auswertet und Berichte für das Management verfasst?	
9.07	Berücksichtigt das Auditprogramm die Bedeutung der Prozesse, Organisationsänderungen und Ergebnisse früherer Audits?	

9.08	Sichert der Auditprozess die Objektivität und Qualifikation der Auditoren und die zügige Bearbeitung festgestellter Korrekturmaßnahmen?	
9.09	Werden Auditprogramm und Auditergebnisse **dokumentiert**?	
9.3	**Managementreview**	
9.10	Findet eine regelmäßige Bewertung des ISMS durch das ToM zur Eignung, Effizienz und Wirksamkeit sowie dessen Anpassung an die Gesamtstrategie der Organisation statt?	

9.11	Werden für die Bewertung folgende Eingangsinformationen berücksichtigt:
	▸ Status von Maßnahmen früherer Reviews,
	▸ Interne und externe Themen mit Relevanz für das ISMS,
	▸ Informationen:
	  ▸ zur Leistung und Wirksamkeit des ISMS,
	  ▸ von Stakeholdern,
	  ▸ zum Stand von Zielen,
	  ▸ zu Abweichungen und Korrekturen,
	  ▸ zu Überwachungen und Messungen,
	  ▸ zu Auditergebnissen,
	▸ Möglichkeiten für Verbesserungen,
	▸ Ergebnisse der Risikobeurteilung und Status des Plans zur Risikobehandlung?	

9.12	Enthält das **dokumentierte** Ergebnis des Review eine Bewertung der fortdauernden Eignung, Angemessenheit und Wirksamkeit des ISMS?	
9.13	Werden Entscheidungen und Aktionen zu Möglichkeiten für Verbesserungen (neue Ziele) getroffen und benötigte Ressourcen festgelegt?	

A.18	Compliance	
A.18.1.1	Sind alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen für jedes Informationssystem und die Organisation ausdrücklich bestimmt und dokumentiert und werden diese auf dem neuesten Stand gehalten? Wird die Einhaltung der externen rechtlichen und vertraglichen Anforderungen in angemessenem Umfang und Abstand geprüft?[16]	
A.18.1.2	Werden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist?	
A.18.1.3	Sind Aufzeichnungen gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt?	
A.18.1.4	Sind die Privatsphäre und der Schutz von personenbezogener Information soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt? Ist dokumentiert, dass, wenn möglich, die Zustimmung der Betroffenen eingeholt werden sollte, bevor persönliche Gesundheitsinformationen per E-Mail, Fax, Telefon oder auf andere Weise an Parteien außerhalb der Gesundheitseinriclsthtung weitergegeben werden?[17] § DIN EN ISO 27799 18.1.4	
A.18.1.5	Werden kryptographische Maßnahmen unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt?	

[16] Die Auditprogramme der Gesundheitsorganisationen sollten formal so strukturiert sein, dass sie alle Elemente dieser Internationalen Norm, alle Risikobereiche und alle implementierten Maßnahmen in einem 12 bis 8-monatigen Zyklus erfassen. In dem stark regulierten und auditierten Umfeld vieler Gesundheitsorganisationen sollte sich der ISMF das Ziel setzen einen abgestuften Rahmen für die Prüfung der Einhaltung der Vorschriften zu schaffen, dessen unterste Ebene ist die Selbstauditierung durch die Prozessbetreiber und -manager. Danach folgt die Auditierung des ISMS im Auftrag des ISMF. Interne Audits, Bewertungen der Kontrollsicherheit und externe Audits werden in einer Weise definiert, die es jeder Ebene ermöglicht, Vertrauen aus allen darunter liegenden Ebenen zu ziehen.
[17] Die DIN EN ISO 27799 nennt im Abschnitt 18.1.4 Beispiele.

A.18.2.1	Wird die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Richtlinien, Prozesse und Verfahren zur Informationssicherheit) auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft?	
A.18.2.2	Überprüfen leitende Angestellte regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstiger Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich?	
A.18.2.3	Werden Informationssysteme regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft? Richtet die Organisation ein besonderes Augenmerk auf die Einhaltung der Vorschriften zum Zwecke der technischen Interoperabilität, da groß angelegte Gesundheitsinformationssysteme in der Regel aus vielen interoperablen Systemen bestehen? § DIN EN ISO 27799 18.2.3	
10	**Verbesserung**	
10.2	**Korrekturmaßnahmen**	
10.3	**Fortlaufende Verbesserung**	
10.01	Werden Möglichkeiten für Verbesserungen der Leistung und Wirksamkeit des ISMS verfolgt?	
10.02	Wird auf Abweichungen (einschließlich Beschwerden) reagiert, Maßnahmen zur Kontrolle und Korrektur eingeleitet und die Auswirkungen beseitigt?	
10.03	Werden Ursachen analysiert, um Maßnahmen zu ergreifen, diese Fehler zukünftig zu verhindern?	
10.04	Erfolgt eine Wirksamkeitsprüfung umgesetzter Korrekturmaßnahmen?	
10.05	Werden – falls nötig – Risiken neu bewertet und das ISMS angepasst?	
10.06	Werden dazu **dokumentierte Informationen** aufbewahrt (bspw. ein Korrektur- und Maßnahmenplan)?	

A.16	Handhabung von Informationssicherheitsvorfällen	
A.16.1.1	Sind Handhabungsverantwortlichkeiten und -verfahren festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen?	
A.16.1.2	Werden Informationssicherheitsereignisse so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet? Hat die Organisation Verantwortlichkeiten und Verfahren für das Management von Sicherheitsvorfällen festgelegt, um a) eine wirksame und rechtzeitige Reaktion auf Sicherheitsvorfälle zu gewährleisten; b) sicherzustellen, dass es einen wirksamen und nach Prioritäten geordneten Eskalationspfad für Vorfälle gibt, so dass Krisenmanagement- und Business-Continuity-Management-Pläne unter den richtigen Umständen und zum richtigen Zeitpunkt aufgerufen werden können; c) Audit-Protokolle und andere relevante Beweise zu sammeln und aufzubewahren? Hat die Organisation erkannt, dass Informationssicherheitsvorfälle die Schädigung oder unbeabsichtigte Offenlegung von persönlichen Gesundheitsinformationen oder den Verlust der Verfügbarkeit von Gesundheitsinformationssystemen umfassen können und ein solcher Verlust die Patientenversorgung beeinträchtigen oder zu unerwünschten klinischen Ereignissen beitragen kann? Werden die betroffenen Personen informiert, wenn personenbezogene Gesundheitsinformationen unbeabsichtigt offengelegt wurden? § DIN EN ISO 27799 16.1.2	
A.16.1.3	Werden Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden?	
A.16.1.4	Werden Informationssicherheitsereignisse beurteilt und wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind? Ist sichergestellt, dass die Organisation prüft, ob das Informationssicherheitsereignis personenbezogene Gesundheitsdaten betraf? § DIN EN ISO 27799 16.1.4	

A.16.1.5	Wird auf Informationssicherheitsvorfälle entsprechend den dokumentierten Verfahren reagiert?	
A.16.1.6	Werden aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern?	
A.16.1.7	Sind Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festgelegt und werden diese angewendet? Hat die Organisation berücksichtigt, dass diese Sammlung auch Beweise für Kunstfehler umfassen kann? Werden dabei auch die Anforderungen der verschiedenen Rechtsordnungen berücksichtigt, wenn Informationssysteme über deren Grenzen hinweg zugänglich sind? § DIN EN ISO 27799 16.1.7	

Quellen:	
Verwendete Normen:	DIN EN ISO/IEC 27001:2017, DIN ISO/IEC 27002:2016, DIN EN ISO 27799:2016, DIN EN ISO 13485:2016, ISO/TS 14441:2013, ISO 15489-1:2016; ISO/TS 21547:2010, ISO 22857:2013, ISO 27789:2013
Gesetzestexte:	Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) vom 8. April 2020 ; Bundesgesetzblatt Jahrgang 2020 Teil I Nr. 18, ausgegeben zu Bonn am 20. April 2020; Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (30.10.2017); Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 71, ausgegeben zu Bonn am 8. November 2017 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997); in der Fassung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt, geändert durch Beschluss des Vorstandes der Bundesärztekammer am 14.12.2018

Kontaktieren Sie uns

Haben Sie Fragen und Interesse an einem Zertifizierungsverfahren nach DIN EN ISO 13485 und ISO/IEC 27001?

Unser Team beantwortet gerne Ihre Fragen:

Martin Tettke – Leiter Zertifizierstelle, Berlin Cert GmbH

Dr. Nina Eschweiler – Leitung Koordination Zertifizierung

Pierre Boileau – Koordination Zertifizierung

cert@berlincert.de +49 30 58 58 216-10

Andreas Lemke – Leiter der Zertifizierungsstelle GUTcert GmbH
andreas.lemke@gut-cert.de +49 30 2332021-41

Bozena Jakubowska – Produktmanagerin ISMS
bozena.jakubowska@gut-cert.de +49 30 2332021-65

Immer besser werden

Eichenstraße 3b, 12435 Berlin
www.gut-cert.de