

Klinik, Patientensicherheit und Notbetrieb

Leitfaden für Krankenhäuser mit vernetzter Medizintechnik und KI-gestützten Arbeitsabläufen

Fachlicher Leitfaden zur Cyber-Physical-AI-Security.

Fassung 1.1 · Stand 25. September 2026 · Adressaten: Ärztliche Direktion, Pflegedirektion, Geschäftsführung, klinisches Risikomanagement, Krankenhaus-IT, Informationssicherheit, Medizintechnik, Apotheke, Labor, Radiologie und Datenschutz.

Dokumenttyp: Ausgearbeitete Fachfassung; lokale klinische, medizintechnische und rechtliche Freigabe erforderlich

Die Fallstudien in diesem Leitfaden-Paket sind ausdrücklich konstruierte Prüfbeispiele; eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden.

Steckbrief

Merkmal	Wert
Dokumenttyp	Ausgearbeitete Fachfassung; lokale klinische, medizintechnische und rechtliche Freigabe erforderlich
Zielgruppe	Ärztliche Direktion, Pflegedirektion, Geschäftsführung, klinisches Risikomanagement, Krankenhaus-IT, Informationssicherheit, Medizintechnik, Apotheke, Labor, Radiologie und Datenschutz.
Recherche- und Rechtsstand	25. September 2026
Umfang	4.324 Wörter, 15 Seiten
Belege	0 Literatureinträge, 13 Quellenadressen
Gliederung	20 nummerierte Abschnitte, 0 Tabellen

Inhalt

1. Die zu schützende Leistung ist Versorgung, nicht IT-Verfügbarkeit	4
2. Verantwortung und rechtlicher Ausgangspunkt	4
3. Welche KI tatsächlich im Krankenhaus arbeitet	4
4. Patientendaten entlang des gesamten Lebenszyklus	5
5. Patientenidentität als durchgängige Sicherheitsfunktion	5
6. Integrität von Befunden und KI-Ausgaben	5
7. Labor und Bildung: Übertragung ist nicht gleich Versorgung	6
8. Medikation und klinische Entscheidung: klare Zuständigkeiten	6
9. Vernetzte Medizintechnik: lokal bedeutet nicht automatisch sicher	7
10. Interoperabilität und Sicherheitsarchitektur	7
11. Klinische Mindestversorgung statt globalem Ausschalten	7
12. Betriebsmodi mit nachgewiesenen Übergängen	8
13. Personal, Kommunikation und Schichtwechsel	8
14. Regionale Folgen und externe Abstimmung	8
15. Wiederherstellung, fachliche Validierung und Abgleich	9
16. Beschaffung und Herstellerzusammenarbeit	9
17. Übungen: drei nachweisbare Fähigkeiten	9
18. Kennzahlen und ihre Aussagegrenzen	10
19. Abnahmefragen für Klinikleitung und Prüfer	10
20. Unterlagen und Einführungsfolge	10
Literatur und Quellenstatus	10
12 Rechtliche Hinweise	13
12.1 Keine Beratung	13
12.2 Keine Zusicherung, keine Konformitätsaussage	13
12.3 Rechtsstand	13
12.4 Haftung	13
12.5 Verweise auf fremde Inhalte	13
12.6 Marken und Produktbezeichnungen	13
12.7 Urheberrecht und Nutzung	13
12.8 Keine personenbezogenen Daten	14
12.9 Unabhängigkeit	14
12.10 Anwendbares Recht	14

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Klinik, Patientensicherheit und Notbetrieb — Leitfaden für Krankenhäuser mit vernetzter Medizintechnik und KI-gestützten Arbeitsabläufen*. Fassung 1.1, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Setzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält eine schematische Abbildung: eine beispielhafte Leistungsabhängigkeitskette (Abschnitt 19). Die Abbildung ist ein Beispielschema, keine für jede Klinik gültige Referenzkette und keine erhobenen Betriebsdaten. Ergänzt in Fassung 1.1 am 27. September 2026.

1. Die zu schützende Leistung ist Versorgung, nicht IT-Verfügbarkeit

Eine IT-Abteilung kann eine Anwendung als verfügbar melden, während die Versorgung dennoch beeinträchtigt ist. Beispiele sind ein nicht erreichbarer Identitätsdienst, eine verzögerte Laborübertragung oder ein Befund, dessen Patientenbezug zweifelhaft ist. Umgekehrt kann ein Server ausfallen, ohne dass eine kritische Versorgung sofort ausfällt, weil eine vorbereitete lokale Funktion weiterarbeitet. Deshalb muss die Klinik die Zusammenhänge zwischen Technik und Leistung ausdrücklich erfassen.

Das Ziel lautet: **Eine klinisch verantwortete Mindestversorgung bleibt unter festgelegten Störungsbedingungen möglich; unsichere Informationen werden nicht unbemerkt weiterverarbeitet; die Rückkehr zum Normalbetrieb ist nachvollziehbar und kontrolliert.** Dieses Ziel besteht aus drei getrennten Nachweisen. Erstens muss die Versorgung im Ersatzmodus fachlich vertretbar sein. Zweitens muss die Datenlage ausreichend geklärt oder als unsicher sichtbar sein. Drittens muss die Rückkehr aus dem Ersatzmodus beherrscht werden. Eine bestandene Wiederherstellungsprobe der Datenbank erfüllt nicht automatisch alle drei Nachweise.

Die Verbindung von Cyberrisiken und Safety ist in der medizinproduktspezifischen MDCG-Leitlinie ausdrücklich angelegt. IEC 80001-1 adressiert dem öffentlichen Normabstract zufolge das Risikomanagement beim Anschluss an Gesundheits-IT. Beide Quellen stützen die Notwendigkeit der gemeinsamen Betrachtung; sie erteilen aber weder eine pauschale Freigabe für eine Architektur noch ersetzen sie die Bewertung der konkreten Klinik. [Q22, insbesondere Annex IV; Q23, Scope]

2. Verantwortung und rechtlicher Ausgangspunkt

Für Deutschland ist § 391 SGB V die zentrale krankenhausspezifische Suchstelle dieses Anhangs. Die Vorschrift adressiert geeignete organisatorische und technische Vorkehrungen, Sensibilisierung und eine verhältnismäßige Orientierung an den Folgen von Ausfällen. Absatz 5 regelt ihr Verhältnis zu Pflichten für Betreiber kritischer Anlagen. Es wäre deshalb falsch, aus einer nicht festgestellten KRITIS-Einstufung auf das Fehlen krankenhausspezifischer IT-Sicherheitsanforderungen zu schließen. [Q30, Abs. 1–5]

Daneben ist die konkrete Anwendbarkeit des BSIG zu prüfen. Der organisatorische Träger, die Art der Einrichtung, Größen- und Sondertatbestände sowie gegebenenfalls die Einstufung einer kritischen Anlage sind gesondert zu dokumentieren. Patientendaten unterliegen außerdem datenschutzrechtlichen Anforderungen. Für Medizinprodukte kommen produktspezifische Regeln und Betreiberpflichten hinzu. Diese Ebenen gelten nicht alternativ nach freier Wahl. Der Rechtsband enthält die Rollen- und Quellenmatrix sowie die ausdrücklich kenntlich gemachten Grenzen des aktuellen Volltextzugriffs. [Q29, insbesondere § 28; Q38, rechtlicher Nachschlagepfad; Q22]

Die klinische Verantwortung für Versorgung darf im Incident nicht stillschweigend an das SOC übergehen. Das SOC beurteilt technische Anzeichen und schlägt Eingrenzungsmaßnahmen vor. Die medizinisch verantwortliche Leitung beurteilt deren Folgen für die Versorgung. Medizintechnik bewertet gerätebezogene Betriebsbedingungen. Der Datenschutzbeauftragte berät zu Betroffenenrisiken und datenschutzrechtlichen Pflichten, übernimmt aber nicht allein die unternehmerische Risikoentscheidung. Diese Rollen werden vor dem Vorfall benannt und durch Vertretungen abgesichert.

3. Welche KI tatsächlich im Krankenhaus arbeitet

Für das Inventar reicht das Feld „KI vorhanden“ nicht. Zu unterscheiden sind Dokumentationsassistentz, Termin- und Bettenplanung, Bild- oder Befundunterstützung, klinische Entscheidungsunterstützung, Logistiksteuerung und direkt mit Geräten verbundene Funktionen. Ferner ist festzuhalten, ob eine Anwendung nur anzeigt, Vorschläge erzeugt, Datensätze schreibt, Bestellungen auslöst oder Geräte beeinflusst. Derselbe Modelltyp kann in verschiedenen Anwendungen völlig unterschiedliche Befugnisse erhalten.

Die Risikoanalyse folgt der beabsichtigten Verwendung und den tatsächlich erreichbaren Handlungen, nicht dem Markennamen des Modells. Ein Schreibassistent kann relativ begrenzte technische Rechte besitzen und dennoch in einem kritischen Prozess eingesetzt werden, wenn seine Texte unkontrolliert in die Akte übernommen werden. Ein Terminagent kann ohne Therapiekompetenz große Mengen personenbezogener Daten einsehen. Ein Logistikroboter kann Versorgung indirekt beeinträchtigen, obwohl er kein diagnostisches Medizinprodukt ist. Der bloße Einsatz in

einem Krankenhaus entscheidet die Produktklassifikation nicht.

Im Systemsteckbrief werden daher fünf Fragen verbindlich beantwortet: Welche Informationen erhält die Anwendung? Welchen Teil davon speichert sie oder ein externer Anbieter? Welche Ausgaben werden von wem verwendet? Welche Änderungen kann sie selbst ausführen? Welche Abhängigkeit entsteht, wenn sie nicht verfügbar oder nicht vertrauenswürdig ist? Erst danach lässt sich festlegen, welche Kontrollen erforderlich sind. Die hochrisikorechtliche Einordnung ist ein eigener Prüfschritt und darf nicht aus dem allgemeinen Wort „Klinik-KI“ abgeleitet werden. [Q33; Q39, Einzelfallprüfung]

4. Patientendaten entlang des gesamten Lebenszyklus

Die Sicherheitsbetrachtung beginnt nicht erst bei der elektronischen Patientenakte. Daten entstehen bei Aufnahme und Identifikation, an Geräten, im Labor, in der Bildgebung, in Gesprächen und in der Dokumentation. Anschließend werden sie übertragen, transformiert, zwischengespeichert, in Berichten zusammengeführt und gegebenenfalls von KI-Systemen aufbereitet. Kopien können in Protokollen, Suchindizes, Testsystemen oder Exportdateien entstehen. Welche dieser Orte tatsächlich existieren, muss erhoben werden; sie dürfen nicht pauschal jedem Produkt unterstellt werden.

Eine Datenflussaufnahme enthält deshalb den fachlichen Zweck, die Datenkategorien, Empfänger, Verarbeitungsschritte, Speicherorte, Löschlogik und Rückwege. Bei KI-Diensten werden Eingaben, Ausgaben, Konversationsspeicher, Abrufsysteme und diagnostische Telemetrie getrennt betrachtet. Ein Vertrag über die Hauptanwendung reicht als Nachweis nicht, wenn ein zusätzlicher Modell- oder Protokolldienst Daten erhält, der im Vertrag und Verarbeitungsverzeichnis nicht auftaucht.

Vier Schäden sind getrennt zu behandeln: unbefugtes Offenlegen, Nichtverfügbarkeit, Löschen und unbemerkte Veränderung. Hinzu kommt eine für den klinischen Betrieb besonders wichtige Zwischenlage: **Die Herkunft oder Zuordnung eines Datensatzes ist nicht mehr hinreichend gesichert.** In dieser Lage kann das System technisch weiterarbeiten. Der Gefährdung liegt gerade zugrunde, dass die Unsicherheit unsichtbar bleibt.

Die Datenschutzprüfung muss die Zweckbindung, Datenminimierung, Rechtsgrundlagen, Auftragsverarbeitung und etwaige Drittlandbezüge abdecken. Sie wird in diesem Band nicht durch die unzureichende Formel „Patienten haben eingewilligt“ ersetzt. Welche Rechtsgrundlage für die konkrete Versorgung und zusätzliche KI-Verarbeitung trägt, ist gesondert zu prüfen. Die einschlägigen Artikel und der erforderliche juristische Volltextcheck stehen in Q38 und Band 5.

5. Patientenidentität als durchgängige Sicherheitsfunktion

Ein technisch korrekter Messwert kann gefährlich fehlverwendet werden, wenn er der falschen Person zugeordnet ist. Das Sicherheitsmodell muss daher Patient, Aufenthalt, Auftrag, Probe, Gerätedaten und Befund miteinander verbinden. Der Schutz beschränkt sich nicht auf den Zugang zur Akte, sondern umfasst die Zuordnung zwischen Objekten und realem Versorgungsvorgang.

Im Notbetrieb braucht die Klinik ein freigegebenes Verfahren für vorläufige Identitäten, Wiedererkennung, Etiketten und die spätere Zusammenführung. Eine zentrale Identitätsprüfung darf nicht die einzige Möglichkeit sein, eine behandelte Person im gesamten Ersatzprozess nachvollziehbar zu führen. Gleichzeitig darf eine Ersatzidentität nicht unkontrolliert zur Dublette werden. Zuständigkeiten für Identitätskonflikte und spätere Zusammenführungen müssen außerhalb des ausgefallenen Systems verfügbar sein.

Der prüfbare Nachweis ist ein durchgehender Fallpfad. Ein synthetischer Patient wird aufgenommen, ein Auftrag erstellt, eine Probe bearbeitet und ein Ergebnis zurückgemeldet. Anschließend wird die digitale Welt wieder verfügbar gemacht. Die Prüfung untersucht, ob der Zusammenhang erhalten bleibt und ob Konflikte sichtbar werden. Der Test verwendet keine echten Patientendaten und keine klinisch wirksamen Aufträge. Ein positives Ergebnis in einem Demonstrationsbildschirm ist nicht ausreichend, wenn Etikettierung, Transport und Rückmeldung nicht einbezogen wurden.

6. Integrität von Befunden und KI-Ausgaben

Die technische Integrität eines Dokuments und seine fachliche Richtigkeit sind unterschiedliche Eigenschaften. Eine signierte Nachricht kann beweisen, dass sie unter bestimmten Bedingungen von einem bekannten System stammt und unterwegs nicht verändert wurde. Sie beweist nicht, dass das Quellsystem den richtigen Patienten oder die richtige Messgröße erfasst hat. Ebenso belegt die Speicherung einer KI-Antwort nicht deren medizinische Richtigkeit.

Die Klinik benötigt deshalb eine **sichtbare Vertrauenseinstufung** für kritische Informationen: Herkunft bestätigt, Version bestätigt, Patientenbezug bestätigt, fachlich geprüft oder ungeklärt. Diese Kategorien sind Vorschläge für die lokale Ausgestaltung, kein bereits normiertes einheitliches Kennzeichnungssystem. Sie sollen vermeiden, dass ein technischer Prüfstatus als klinische Freigabe missverstanden wird.

Eine KI-Anwendung darf ungeklärte Eingangsdaten nicht automatisch durch sprachliche Glättung in scheinbar sichere Aussagen verwandeln. Im vorgesehenen Workflow muss die Herkunft erreichbar bleiben, ein veralteter Stand erkennbar sein und eine fachliche Korrektur dokumentiert werden können. Für den Notbetrieb ist festzulegen, welche KI-Funktionen bei fraglicher Datengrundlage ausgesetzt werden. Das kann einen Schreibzugriff oder die automatische Übernahme betreffen, ohne zwangsläufig sämtliche lesenden Hilfsfunktionen abzuschalten. Die konkrete Entscheidung hängt vom Verwendungszweck ab.

7. Labor und Bildgebung: Übertragung ist nicht gleich Versorgung

Ein Laborworkflow besteht nicht nur aus einem funktionierenden Analysesystem. Er umfasst Auftrag, Probennahme, Identifikation, Transport, Verarbeitung, Freigabe, Befundübertragung und klinische Kenntnisnahme. In jedem Übergang kann ein IT-Ausfall den Prozess verändern. Ein Ergebnis, das technisch erzeugt, aber nicht sicher übermittelt wurde, ist für die Versorgung möglicherweise nicht nutzbar. Ein mehrfach übermitteltes Ergebnis kann zu Verwechslungen führen, wenn Korrekturstände nicht erkennbar sind.

Der Ersatzprozess muss daher festlegen, wie Aufträge und Proben zusammengeführt werden, welche lokale Dokumentation benutzt wird und wie eine empfangende Stelle den Eingang bestätigt. Klinisch dringliche Kommunikation wird nach den örtlich freigegebenen Verfahren behandelt. Dieser Leitfaden setzt dafür keine allgemeinen medizinischen Zeitgrenzen fest. Er verlangt, dass die medizinisch begründeten Grenzen erhoben, kommuniziert und in der Übung überprüft werden.

In der Bildgebung sind Identität, Untersuchungszeitpunkt, Serie, Vorbefund und Freigabestatus entsprechend auseinanderzuhalten. Die bloße Erreichbarkeit eines Bildarchivs beweist nicht die Vollständigkeit aller relevanten Voruntersuchungen. Eine KI-Auswertung kann ihren vorgesehenen Nutzen verlieren, wenn Metadaten, Modalität oder Datenbestand vom validierten Betrieb abweichen. Die passende Konsequenz ist eine fachlich verantwortete Einschränkung des Einsatzes, nicht eine improvisierte Änderung des Modells im laufenden Klinikbetrieb.

Ein veröffentlichter Bericht über 25 Tage Labor-Downtime zeigt, dass längere Ausfälle ein eigener Organisationsgegenstand sind. Da hier nur Abstract und Metadaten ausgewertet wurden, dient er als belegter Erfahrungs- und Literaturzugang, nicht als übernommene vollständige Musterlösung. [Q21]

8. Medikation und klinische Entscheidung: klare Zuständigkeiten

Bei medikationsbezogenen Prozessen müssen Vorschlag, Verordnung, Bereitstellung, Verabreichungsdokumentation und spätere Korrektur getrennt nachvollziehbar bleiben. Ein KI-System darf nicht dadurch weitergehende Wirkung erhalten, dass seine Ausgabe in einer anderen Anwendung als bereits freigegebener Auftrag interpretiert wird. Die Kontrolle muss an der Stelle greifen, an der sich aus Information eine verbindliche Handlung ergibt.

Der Leitfaden enthält ausdrücklich keine Dosierungs-, Substitutions- oder Therapieanweisungen. Er fordert ein von den zuständigen klinischen und pharmazeutischen Stellen genehmigtes Ersatzverfahren. Dieses muss erklären, welche Informationsquellen im Ausfall zur Verfügung stehen, wie Unklarheiten behandelt werden und wie bereits erfolgte Handlungen dokumentiert werden. Der anschließende Abgleich darf insbesondere nicht dazu führen, dass ein im Ersatzbetrieb bereits erledigter Vorgang digital erneut ausgelöst wird.

Eine besonders wichtige Negativprobe lautet: Ein manipuliertes Dokument behauptet, die Sicherheitsregeln seien aufgehoben oder eine zusätzliche Freigabe sei bereits erfolgt. Die KI darf daraus weder neue Systemrechte ableiten

noch einen nicht vorgesehenen Schreibpfad benutzen. Die Prüfung erfolgt mit synthetischen, eindeutig als Test markierten Inhalten in einer isolierten Umgebung. Sie untersucht technische Durchsetzung und menschliche Darstellung, nicht die Leistungsfähigkeit eines Modells bei echten Behandlungsentscheidungen. [Q11, Angriffseinordnung; Q16, Autorisierung]

9. Vernetzte Medizintechnik: lokal bedeutet nicht automatisch sicher

Die FDA berichtete 2025 über konkrete Schwachstellen bestimmter Patientenmonitore von Contec beziehungsweise Epsimed. Die Aktualisierung vom 2. Juli beschreibt eine Korrektur, die die Netzwerkfunktion entfernt und lokale Überwachung erhält. Die Mitteilung bezeichnet dies nicht als allgemeinen Schutzweg für alle Geräte und meldete zu ihrem damaligen Stand keine bekannten damit verbundenen Verletzungen oder Todesfälle. [Q19, July 2 Update und Recommendations]

Der für die Klinikplanung wichtige Punkt ist die **veränderte Arbeitsteilung**. Fällt eine zentrale Alarmweiterleitung weg, kann ein lokal anzeigendes Gerät zusätzliche Personalpräsenz und andere Eskalationswege erfordern. Dass ein Bildschirm Messwerte zeigt, belegt nicht, dass die bisherige Überwachungskette erhalten ist. Deshalb werden Datenverbindung, Alarmfunktion, lokale Anzeige, Dokumentation und Fernwartung getrennt bewertet.

Das Trennen eines Geräts vom Netz ist nur zulässig, wenn dessen vorgesehene Verwendung, Herstellerinformationen und klinische Folgen verstanden und freigegeben sind. Es gibt in diesem Paket keine Handlungsanweisung „alle Monitore abstecken“. Die Geräteliste muss vielmehr je Modell und Betriebsart ausweisen, welche Funktionen ohne Netz, Serverkontakt oder externe Dienste verbleiben. Fehlt diese Information, ist das eine Beschaffungs- beziehungsweise Nachweisaufgabe und kein Anlass für einen unkontrollierten Liveversuch.

10. Interoperabilität und Sicherheitsarchitektur

Ein standardisiertes Austauschformat erleichtert nicht automatisch die sichere Autorisierung. Die FHIR-R5-Dokumentation beschreibt ausdrücklich eine zusätzliche Sicherheitsarchitektur für Authentisierung, Zugriffsentscheidungen und Auditierung. Ein erreichbarer FHIR-Endpunkt darf daher nicht mit einem fertig abgesicherten Versorgungssystem gleichgesetzt werden. [Q16, General Considerations und Authorization/Access Control]

Für jede Schnittstelle werden erlaubte Ressourcen und Operationen festgelegt. Ein Terminagent benötigt möglicherweise ausgewählte Planungsdaten, nicht die vollständige Krankengeschichte. Ein Dokumentationsdienst kann Entwürfe erstellen, ohne Freigabestände zu verändern. Der tatsächliche API-Umfang muss an den klinischen Zweck angepasst werden; pauschale Rollen wie „KI-Service = Vollzugriff“ sind nicht durch technische Bequemlichkeit zu rechtfertigen.

Auch die semantische Seite gehört zum Schnittstellenvertrag. Einheiten, Zeitzonen, Identifikatoren, Korrekturstände, fehlende Werte und Versionen müssen zwischen den Systemen eindeutig interpretiert werden. Ein technisch gültiges Datenpaket kann fachlich ungeeignet sein. Eine Änderung des Integrationsmappings wird deshalb wie eine klinisch relevante Änderung behandelt, wenn sie die Bedeutung der Daten beeinflusst. Die Freigabe muss Testfälle mit Grenz-, Fehler- und Korrektursituationen enthalten.

11. Klinische Mindestversorgung statt globalem Ausschalten

Die Klinikleitung definiert zunächst, welche Leistungen im untersuchten Störungsszenario erhalten bleiben müssen, welche reduziert und welche geordnet ausgesetzt werden können. Die Auswahl ist lokal: Leistungsauftrag, Patientenkollektiv, Standortverbund und verfügbare Ersatzkapazität unterscheiden sich. Es gibt keine in diesem Anhang behauptete universelle Liste, die für jedes Krankenhaus gleichermaßen abschließend wäre.

Für jede priorisierte Leistung werden Mindestdaten, notwendige Geräte, Personalkompetenzen, Verbrauchsmaterialien und Kommunikationswege benannt. Danach wird geprüft, welche dieser Ressourcen von derselben digitalen Grundlage abhängen. Eine Papiermappe hilft nicht, wenn sie ausschließlich in einem gesperrten Serverraum liegt. Ein Ersatztelefon hilft nicht, wenn seine Anmeldung denselben Identitätsdienst benötigt. Ein lokales Archiv hilft nicht, wenn niemand die Zugriffsmittel unter Ausfallbedingungen erhalten kann.

Die Mindestversorgung ist außerdem zeitlich begrenzt. Personaleinsatz, Ermüdung, Materialverbrauch, Dokumentationsrückstand und Belegung verändern ihre Tragfähigkeit. Die Eintrittsentscheidung wird daher durch wiederkehrende Lagebewertungen ergänzt. Das Ende eines vertretbaren Ersatzbetriebs muss vorab erkennbar sein, damit Einschränkung, Verlegung oder andere Maßnahmen rechtzeitig fachlich und regional koordiniert werden können.

12. Betriebsmodi mit nachgewiesenen Übergängen

Eine geeignete Modusmatrix kann zwischen vernetztem Normalbetrieb, eingeschränkten externen Verbindungen, isoliertem Teilbereich, lokalem Gerätebetrieb und manuellem Ersatzprozess unterscheiden. Nicht jede Leistung durchläuft alle Stufen. Ein System kann sofort eine lokale Überwachung benötigen, während eine administrative Anwendung vorübergehend ganz entbehrlich ist.

Die Matrix enthält neben der technischen Maßnahme deren klinische Wirkung. Beispiel: „Externe KI-Verbindung gesperrt“ bedeutet möglicherweise, dass Dokumentationsentwürfe manuell erstellt werden; die Patientenakte bleibt verfügbar. „Zentrale Anmeldung ausgefallen“ hat andere Folgen und erfordert vorbereitete lokal zulässige Zugänge. „Datenintegrität ungeklärt“ betrifft die Nutzung von Informationen, selbst wenn keine Verbindung getrennt wurde.

Für jeden Übergang werden Entscheidungskompetenz, Informationsweg, Voraussetzungen und Rückkehrkriterien dokumentiert. Kritische Geräte dürfen nicht durch ein globales SOC-Playbook ohne vorherige lokale Wirkungsanalyse abgeschaltet werden. Umgekehrt darf die Berufung auf klinische Verfügbarkeit nicht jede technische Eingrenzung blockieren. Genau diesen Zielkonflikt muss die vorbereitete Zusammenarbeit lösen; im Ereignisfall darf sie nicht erstmals verhandelt werden.

13. Personal, Kommunikation und Schichtwechsel

Ein Ersatzverfahren ist nur tragfähig, wenn es mit den tatsächlich anwesenden Personen funktioniert. Die Übung muss Nacht- und Wochenendbesetzung, Vertretungen, externe Dienste und Sprach- beziehungsweise Verständnishürden berücksichtigen. Ein Plan, dessen Schlüsselfigur im Urlaub nicht ersetzt werden kann, beschreibt keine belastbare Organisation.

Die Kommunikation benötigt einen vom ausgefallenen Hauptpfad hinreichend unabhängigen Zugang. „Unabhängig“ wird konkret geprüft: Strom, Endgerät, Zugangsdaten, Netzbetreiber, Kontaktliste und Erreichbarkeit der Gegenstelle. Die Reservekommunikation muss nicht zwingend ein bestimmtes technisches Medium sein; sie muss unter den definierten Ausfallbedingungen nutzbar sein. Kontaktlisten und Rollenbezeichnungen sind so zu führen, dass nicht erst aus kompromittierten Nachrichten erkannt werden muss, wer tatsächlich zuständig ist.

Ein Schichtwechsel enthält den aktiven Betriebsmodus, bekannte Datenunsicherheit, offene Aufträge, zurückgestellte Leistungen und dokumentierte Entscheidungen. Der Wechsel ist ein eigener Testschritt. Ein nach Stunden wiederhergestelltes System kann trotzdem gefährlich sein, wenn die neue Schicht nicht weiß, welche Informationen nur im Ersatzverfahren vorliegen.

14. Regionale Folgen und externe Abstimmung

Die Versorgung lässt sich nicht allein innerhalb eines Kliniknetzes betrachten. Umleitungen, abgesagte Leistungen und Kommunikationsstörungen können benachbarte Einrichtungen betreffen. Eine retrospektive US-Studie dokumentiert solche Zusammenhänge bei angrenzenden Notaufnahmen. Daraus folgt kein allgemeiner deutscher Belastungswert, wohl aber eine begründete Planungsfrage: Welche regionalen Abhängigkeiten müssen vorab abgestimmt werden? [Q20, Methods, Results und Limitations]

Die Klinik klärt mit den zuständigen regionalen Strukturen, wie Lageinformationen übermittelt werden, wer Einschränkungen kommuniziert und welche Alternativen tatsächlich zugesagt sind. Eine angenommene freie Nachbarkapazität ist kein Nachweis. Die Planung muss auch einen gleichzeitigen Ausfall eines gemeinsam genutzten Dienstleisters berücksichtigen. Ein Verbund kann seine Ersatzkapazität verlieren, wenn alle Standorte von demselben Laborportal, Identitätsanbieter oder Kommunikationsdienst abhängen.

Externe Kommunikation an Patienten und Öffentlichkeit muss zwischen bestätigten Tatsachen, noch offenen Punkten und konkreten Handlungsinformationen unterscheiden. Eine Aussage über möglichen Datenabfluss ist nicht identisch mit einer Aussage über Versorgungsfähigkeit. Umgekehrt bedeutet fortgesetzte Versorgung nicht, dass kein Datenschutzvorfall vorliegt. Die Meldeentscheidungen werden getrennt dokumentiert.

15. Wiederherstellung, fachliche Validierung und Abgleich

Die technische Wiederherstellung erfolgt in einer kontrollierten Umgebung nach dem lokal festgelegten Abhängigkeitsplan. Die automatische Wiedereinbindung sämtlicher externer Schnittstellen ist kein zulässiger Standardabschluss. Zunächst muss geklärt sein, welche Konten, Konfigurationen und Datenbestände betroffen sein können. Agenten werden nur in dem Umfang wieder zugelassen, der gesondert geprüft ist; häufig kann eine zunächst eingeschränkte Nutzung sinnvoll sein.

Der **klinische Abgleich** umfasst Ereignisse aus dem Ersatzbetrieb. Dabei bleiben tatsächlicher Ereigniszeitpunkt, spätere Erfassung, Urheber und Freigabe unterscheidbar. Offene Aufträge werden nicht blind erneut versendet. Dubletten, Korrekturen und Patientenidentitätskonflikte werden in einer Arbeitsliste geführt und durch zuständige Fachpersonen entschieden. Ein technischer Importbericht allein belegt nicht, dass die Versorgungshistorie konsistent ist.

Für Daten mit Integritätsverdacht braucht es einen fachlich bestimmten Validierungsumfang. Nicht jede komplette Akte lässt sich unmittelbar erneut prüfen. Deshalb wird priorisiert, welche entscheidungsrelevanten Informationen vor weiterer Verwendung bestätigt werden müssen und welche Unsicherheiten sichtbar bleiben. Der Restbestand offener Abgleiche wird als Risiko geführt. Eine Freigabe unter Bedingungen kann zulässig sein, sofern die Bedingungen konkret, überwacht und fachlich verantwortet sind; ein allgemeines „später bereinigen“ genügt nicht.

16. Beschaffung und Herstellerzusammenarbeit

Bei der Beschaffung werden Betriebsarten und Abhängigkeiten ebenso verbindlich abgefragt wie Hauptfunktionen. Der Anbieter muss erläutern, welche Funktionen bei fehlender Cloud, fehlender zentraler Anmeldung oder unterbrochener Schnittstelle verbleiben, wie Warnungen angezeigt werden und wie Daten exportiert werden können. Für Geräte sind die zulässigen Betriebsbedingungen aus der maßgeblichen Dokumentation zu entnehmen.

Die Klinik verlangt geeignete Informationen zu Sicherheitsupdates, unterstützten Versionen, Meldewegen für Schwachstellen, Fernzugriffen, Protokollen und Wiederherstellung. Ein Versprechen „DSGVO-konform“ oder „KI-sicher“ beantwortet keine dieser Fragen. Ebenso reicht ein Softwarekomponentenverzeichnis allein nicht aus, wenn ein Integrationsfehler oder ein zentraler Dienst den klinischen Betrieb bestimmt.

Verträge sollen Verantwortlichkeiten für Änderungen und Störungen klären. Dazu gehören Benachrichtigung vor funktional relevanten Änderungen, Möglichkeiten eines kontrollierten Rollbacks und Unterstützung im Notbetrieb. Ob konkrete Vertragsklauseln wirksam und angemessen sind, ist juristisch zu prüfen. Das Formular zur Beschaffung ist deshalb ein fachliches Anforderungs- und Nachweiseraster, kein ungeprüfter Mustervertrag. [Q17, Vendor / Supplier Goals; Q23, Scope]

17. Übungen: drei nachweisbare Fähigkeiten

Die erste Übung prüft einen geplanten Ausfall der zentralen Dokumentation in einer Test- oder ausdrücklich freigegebenen Übungsumgebung. Der Maßstab ist nicht allein, ob Papierformulare gefunden werden. Geprüft wird ein vollständiger synthetischer Fall vom Beginn bis zum späteren Abgleich, einschließlich Übergabe und offener Aufgaben.

Die zweite Übung prüft Datenunsicherheit bei weiterlaufender IT. Ein synthetischer Befund weist einen widersprüchlichen Zuordnungs- oder Versionshinweis auf. Die Beteiligten müssen die Unsicherheit erkennen, die automatische Weiterverarbeitung begrenzen und einen dokumentierten fachlichen Klärungsweg verwenden. Dieser Fall verhindert die falsche Gleichsetzung von technischer Verfügbarkeit und Vertrauenswürdigkeit.

Die dritte Übung prüft eine mögliche Fehlreaktion der Cyberabwehr. Das SOC erhält einen simulierten verdächtigen Zugriff und soll eine Einschränkung vorschlagen. Vor der Ausführung wird untersucht, ob die vorgesehene Maßnahme kritische Kommunikation oder Alarmierung beeinträchtigen würde. Der Test muss vorab festlegen, welche Aktionen nur simuliert werden. Keine Übung rechtfertigt eine unkontrollierte Unterbrechung realer Patientenversorgung.

18. Kennzahlen und ihre Aussagegrenzen

Aussagekräftig sind der Anteil kritischer Leistungen mit geprüftem Ersatzverfahren, die Zeit bis zur verantworteten Modusentscheidung, die Anzahl ungeklärter Identitätskonflikte, der offene fachliche Abgleich und die Wiederholbarkeit eines Ersatzprozesses unter Schichtwechsel. Diese Kennzahlen müssen Definition, Messpunkt, Verantwortlichen und Beobachtungszeitraum besitzen.

Eine mittlere Wiederherstellungszeit verdeckt Ausreißer und unvollständig abgeschlossene Prozesse. Deshalb werden wichtige Leistungen einzeln ausgewiesen. Eine geringe Zahl gemeldeter Fehler beweist ebenfalls keine gute Sicherheit, wenn Meldungen nicht erfasst oder Unsicherheiten nicht erkannt werden. Das Qualitätsziel lautet nicht „möglichst wenige Befunde“, sondern „relevante Unsicherheit rechtzeitig erkennen und beherrscht bearbeiten“.

Die in den Vorlagen vorgeschlagenen Messgrößen sind Arbeitsinstrumente, keine allgemeinen klinischen Grenzwerte. Klinisch notwendige Zeiten und Sicherheitsbedingungen werden durch zuständige Fachverantwortliche festgelegt. Weder dieses Paket noch ein Herstellerdashboard darf diese Entscheidung ersetzen.

19. Abnahmefragen für Klinikleitung und Prüfer

Vor einer Freigabe müssen die wichtigsten Leistungsabhängigkeiten nachvollziehbar sein. Es muss gezeigt werden können, welche KI-Dienste welche Daten sehen und welche Handlungen sie auslösen. Mindestens ein negativer Berechtigungstest und ein durchgängiger Ausfall-/Abgleichfall müssen für den freizugebenden Prozess vorliegen. Die Nutzung von Informationen mit ungeklärter Herkunft muss sichtbar begrenzt sein.

Ein Ausschuss sollte gezielt nach den schwächsten Stellen fragen: Welche notwendige Funktion wurde noch nie ohne zentrale Anmeldung getestet? Welche Datenkopie könnte trotz intaktem Hash fachlich falsch sein? Welche Personalannahme ist nachts nicht erfüllt? Wer entscheidet einen Konflikt zwischen technischer Eingrenzung und Versorgung? Welche Herstellerinformation fehlt? Diese Fragen sind konkreter als die Bitte um ein allgemeines Cybersecurity-Zertifikat.

Eine nicht geklärte letzte Schutzfunktion, eine nicht auflösbare Patientenidentität oder ein unbekannter Effekt der geplanten Isolation sind Sperrgründe für die jeweils betroffene Betriebsfreigabe. Das bedeutet nicht zwangsläufig einen vollständigen Stillstand der Klinik. Es bedeutet, dass der Nutzungsumfang auf den nachweisbar beherrschten Teil begrenzt und die Versorgung über die dafür verantworteten Wege organisiert werden muss.

20. Unterlagen und Einführungsfolge

Für diesen Band sind die Kontrollen **K09–K18** sowie die bereichsübergreifenden Kontrollen zu Identitäten, Recovery und Governance maßgeblich. Die Formulare **F01–F06**, **F08 Modusmatrix**, **F10 Wiederanlauf**, **F11 Ereignisabgleich** und **F15 Übungsprotokoll** werden gemeinsam mit den klinischen Bereichen ausgefüllt. Fallstudie **S-KLINIK** zeigt einen synthetischen Integritätsvorfall bei weiterlaufendem System.

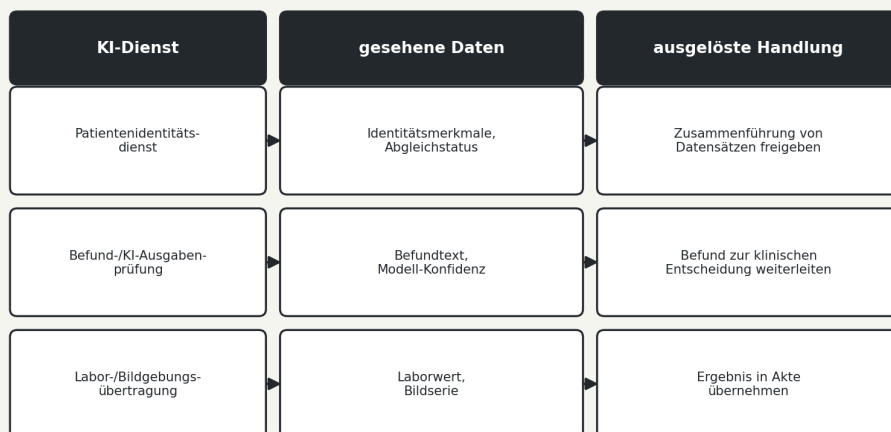
Die Einführung beginnt mit einem klar abgegrenzten klinischen Prozess, nicht mit einem großflächigen Sicherheitsumbau ohne Fachbezug. Nach der Erhebung werden fehlende Verantwortlichkeiten und unmittelbare unzulässige Zugriffspfade geklärt. Danach folgen Ersatzprozess, Übung und Wiederanlaufprobe. Erst ein dokumentierter Nachweis rechtfertigt die Ausweitung autonomer Funktionen. Die entscheidende Freigabe lautet nicht „Die KI läuft“, sondern: **Die Klinik versteht ihre Wirkung, ihre Grenzen und ihren beherrschten Ausfall.**

<!-- GENERATED_LOCAL_BIBLIOGRAPHY -->

Literatur und Quellenstatus

Beispielhafte Leistungsabhängigkeitskette

KI-Dienst → gesehene Daten → ausgelöste Handlung — für die konkrete Freigabe je Prozess einzeln erheben



Ausfall-/ Abgleichfall

- ✗ nicht geklärte letzte Schutzfunktion
- ✗ nicht auflösbare Patientenidentität
- ✗ unbekannter Effekt der geplanten Isolation

→ Sperrgründe für die Betriebsfreigabe

Prüffragen des Ausschusses (Auszug):

- Welche notwendige Funktion wurde noch nie ohne zentrale Anmeldung getestet?
- Welche Datenkopie könnte trotz intaktem Hash fachlich falsch sein?
- Welche Personalannahme ist nachts nicht erfüllt?

Abbildung · Beispielhafte Leistungsabhängigkeitskette (zu Abschnitt 19)

Die folgenden Angaben gehören zu diesem Band. Das vollständige Quellenregister erläutert Verwendungszweck und Zugriff. Quellenstatus und Grenzen sind bei jeder Weiterverwendung zu erhalten. Die Q-Nummern im Text beziehen sich auf diese Einträge; Fundstellen bezeichnen die externe Quelle, nicht eine erfundene PDF-Seite dieses Bandes.

Q11 – Apostol Vassilev et al. / NIST. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, AI 100-2e2025. 2025-03. DOI: 10.6028/NIST.AI.100-2e2025. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Attack goals, capabilities and knowledge; Errata. Zugriff: Publikationsseite / Abstract einschließlich Erratahinweis gelesen. Grenze: Taxonomie belegt keine Häufigkeit; keine Aussage, dass jede beschriebene Angriffsklasse im betrachteten System praktisch funktioniert.

Q16 – HL7 International. FHIR R5, Security, Version 5.0.0. R5 (2023); abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: General Considerations; Authentication; Authorization/Access Control; Audit Log. Zugriff: Webtext / Abschnitte 6.1.0.1–6.1.0.5 gelesen. Grenze: Release R5 ausdrücklich gewählt; keine Behauptung, alle Kliniken nutzten R5 oder die Seite sei in jedem Verweis aktuell. OAuth-Draftverweis dort wird hier durch RFC 9700 ergänzt.

Q17 – US HHS. Healthcare and Public Health Cybersecurity Performance Goals. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Essential / Enhanced Goals; Incident Planning; Network Segmentation; Centralized Log Collection. Zugriff: Webtext und konkrete Zielabschnitte gelesen. Grenze: Freiwillige US-Empfehlungen, keine unmittelbar geltenden deutschen Klinikpflichten.

Q19 – US FDA. Cybersecurity Vulnerabilities in Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication. 2025-01-30; maßgebliches Update 2025-07-02. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: July 2, 2025 Update; Recommendations for Health Care Providers and Facilities. Zugriff: Webvolltext einschließlich zeitlich jüngster Ergänzung gelesen. Grenze: Historische Mitteilung; kein Beleg für erfolgten Patientenschaden. Kein allgemeiner Auftrag, Medizintechnik vom Netz zu trennen. Juli-Update geht älterem Text zur fehlenden Korrektur vor.

Q20 – Christian Dameff et al.. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. 2023-05-08. DOI: 10.1001/jamanetworkopen.2023.12270. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: JAMA Network Open 6(5):e2312270; Methods; Results; Limitations. Zugriff: Web-Volltext, Methoden, Ergebnisse und Limitationen gelesen. Grenze: Assoziation, keine randomisierte Kausalidentifikation; begrenzte regionale Übertragbarkeit; keine Studie über KI-Angriffe.

Q21 – Goodwin et al.. Anatomy of a Cyberattack: Part 2: Managing a Clinical Pathology Laboratory During 25 Days of Downtime. 2022. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: American Journal of Clinical Pathology 157(5):653–663; Abstract. Zugriff: PubMed-Abstract / Metadaten gelesen; Volltext nicht ausgewertet. Grenze: Nur Abstractzugriff; keine Detailbehauptungen über Interventionseffekt, Kennzahlen oder Volltextmethodik.

Q22 – Medical Device Coordination Group / Europäische Kommission. MDCG 2019-16 rev. 1: Guidance on Cybersecurity for medical devices. 2020-07 (Rev. 1). [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abschnitte zu Design / Post-market; Annex IV, gedruckte S. 46. Zugriff: Relevante PDF-Abschnitte gelesen; Inhaltsverzeichnis und Annex IV visuell geprüft. Grenze: Leitlinie ist ausdrücklich nicht rechtsverbindlich; kein Ersatz für MDR/IVDR oder den Normvolltext.

Q23 – IEC. IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices — Part 1. 2021-09-21. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract / Scope; edition 2.0. Zugriff: Offizielle Metadaten und öffentliches Abstract; Normvolltext nicht zugänglich. Grenze: Keine Klausel- oder Konformitätsprüfung. Normbeschaffung und Anwendungsprüfung erforderlich.

Q29 – Bundesrepublik Deutschland / Gesetze im Internet. BSI-Gesetz (BSIG 2025), aktuelle bereitgestellte Fassung. Gesetz 2025; Änderungsstand im Abruf 2026. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: § 28 und Anlagen: Scope; § 30: Risikomanagement; § 31: kritische Anlagen; § 32: Meldung; § 38: Geschäftsleitung. Zugriff: Bereitgestellter Volltext; §§ 28, 30–32, 38–39 und Änderungsvermerk gelesen. Grenze: Keine automatische Einstufung eines konkreten Unternehmens. Gesetze-im-Internet-Fassung enthält Bearbeitungshinweise; Einzelfall und Spezialregeln separat prüfen.

Q30 – Bundesrepublik Deutschland / Gesetze im Internet. SGB V § 391 – IT-Sicherheit in Krankenhäusern. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Absätze 1–5; besonders Abs. 5. Zugriff: Vollständiger Paragraph gelesen. Grenze: Keine Gleichsetzung aller Krankenhäuser mit Betreibern kritischer Anlagen; Abgrenzung nach Abs. 5 beachten.

Q33 – Europäische Kommission, DG CONNECT. AI Act — Application timeline and implementation. Webupdate 2026-08-03. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Application timeline; How has the Commission simplified the implementation of the AI Act?. Zugriff: Aktuelle Webseite einschließlich Omnibus- und Fristenabschnitt gelesen. Grenze: Amtliche Erläuterung ersetzt nicht konsolidierten Normtext. Dessen Abruf war technisch blockiert; rechtsverbindliche Subsumtion bleibt Freigabeaufgabe.

Q38 – Europäische Union. Verordnung (EU) 2016/679 — Datenschutz-Grundverordnung. 2016; aktuelle Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff.. Zugriff: Direkter Web-Volltextabruf technisch blockiert; nicht als neu volltextverifiziert ausgewiesen. Grenze: Artikelzuordnung dient der rechtlichen Prüfung. Redaktionell bekannte Regelungsinhalte werden nicht als vollständig neu geprüfte konsolidierte Rechtsberatung ausgegeben.

Q39 – Europäische Union. AI Act, Verordnung (EU) 2024/1689 — konsolidierte Fassung vom 27.07.2026. 2026-07-27. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 6, 9–15, 26, 113; Anhänge I/III; Änderungsverordnung EU 2026/1744. Zugriff: Abruf technisch blockiert; aktuelle Zeitachse über Q33/Q34 geprüft. Grenze: Keine Behauptung, der konsolidierte Volltext sei in dieser Recherche geprüft worden. Geänderte Detailvorschriften vor konkreter Nutzung juristisch lesen.

Arbeitsmittel: Kontrollkatalog, Formularbuch, Fallstudien und Claim–Evidence-Matrix.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.