Der „offizielle“ Leitfaden für Software-Audits

Sicher durch das Audit:
Eine Checkliste für Hersteller und Auditoren medizinischer Software

Autoren: Prof. Dr. Christian Johner und Sven Wittorf

Kontakt: Johner Institut GmbH
Web: www.johner-institut.de
Telefon: +49(0)7531 94500 -20
E-Mail: info@johner-institut.de

Vorwort zur zweiten Auflage

Neue regulatorische Anforderungen

Mit der ersten Auflage des Leitfadens haben viele Medizinprodukte-hersteller ihre Audits und Zulassungen erfolgreich gemeistert. Inzwischen ist diese erste Auflage vergriffen. Zudem hat sich regulatorisch viel geändert.

Die folgenden Beispiele illustrieren, welche neuen und geänderten regulatorischen Anforderungen die Hersteller berücksichtigen müssen:

- Die EU hat die bisherigen EU-Richtlinien durch EU-Verordnungen **(MDR und IVDR)** abgelöst und die Anforderungen deutlich erhöht.
- Alle relevanten **Normen** sind in neuen Versionen erschienen, welche nennenswerte Änderungen mit sich bringen. Das betrifft die IEC 62304 ebenso wie die IEC 62366-1. Manche Benannte Stelle fordert sogar Konformität mit der IEC 82304 ein, obwohl es dafür keine rechtliche Grundlage gibt.
- Auch die FDA hat viele **Guidance-Documents** neu erstellt und bestehende überarbeitet.
- Die Anforderungen der **Datenschutzgrundverordnung DSGVO** betreffen die Hersteller von Medizinprodukten zumindest indirekt, deren Kunden, die Betreiber, unmittelbar.

Technologische Trends

Aktuelle Technologien – besonders auch deren Anwendung und Auswirkungen auf das tägliche Leben – waren Mitte der 2000er Jahre noch kaum vorstellbar. Heute finden viele dieser Technologien in Medizinprodukten Anwendung:

- Das Thema **IT-Security** hat in den letzten Jahren substanziell an Bedeutung gewonnen. Viele Best Practice Guidelines sind entstanden, und die EU-Verordnungen fordern die IT-Sicherheit explizit mit ein.
- Seit 2018 werden Medizinprodukte, die auf Verfahren der **Künstlichen Intelligenz**, insbesondere des Machine Learnings beruhen, Stand der Technik. Ein Konsens bezüglich der spezifischen Anforderungen an diese Produkte ist erst noch im Entstehen.
- Selbst die MDR und die IVDR haben erkannt, welche spezifischen Herausforderungen und Risiken durch **mobile Plattformen** (Smartphones, Tablets, Wearables etc.) entstehen und gemeistert werden müssen. Das Gleiche gilt für die **Vernetzung** von Medizinprodukten untereinander sowie von Medizinprodukten mit anderen Produkten und Systemen einschließlich Cloud-Speichern.

Integration der Leitfäden zur IT-Sicherheit und zur Künstlichen Intelligenz

Das Johner Institut trägt aktiv dazu bei, Best Practices zu etablieren und zu standardisieren, um die Vorteile des technischen Fortschritts durch Medizinprodukte nutzbar zu machen, ohne Patienten unvertretbaren Risiken auszusetzen. Die aktive Mitarbeit in Normengremien und die Leitfäden zur IT-Sicherheit und zur Künstlichen Intelligenz zeugen davon.

Diese Leitfäden hat das Johner Institut gemeinsam bzw. im Auftrag Benannter Stellen wie dem TÜV SÜD entwickelt. Sie sind in diese Auditcheckliste bereits integriert.

Neu im Fokus: „Post-Market"-Aktivitäten

Diese zweite Version des Auditleitfadens berücksichtigt auch die spezifischen Anforderungen an die **Post-Market-Surveillance**, die **klinische Bewertung** und die klinische Nachbeobachtung (**Post-Market Clinical Follow-up**).

Digitale und kontinuierlich aktualisierte Version des Leitfadens

Um den raschen Änderungen Rechnung tragen zu können, stellt das Johner Institut eine **digitale Version dieses Leitfadens** zur Verfügung. Informieren Sie sich auf der Webseite www.johner-institut.de über die Details.

Wie Sie von diesem Buch profitieren

„Würden Sie gerne schnell und ohne Normenstudium prüfen, wie wahrscheinlich es ist, dass Sie das nächste Audit bestehen?“

Genau dabei unterstützt Sie dieses Buch. Sie erlangen Sicherheit beim Audit und können mögliche Abweichungen frühzeitig erkennen und beheben. Das spart Geld und Zeit, denn Sie vermeiden unangenehme Wiederholungsaudits oder Nachbesserungen – vom Imageschaden für Ihre Abteilung ganz zu schweigen.

Dieses Buch erspart Ihnen, die Gesetze und Normen im Detail lesen zu müssen. Es fasst für Sie die Forderungen zusammen – in der Reihenfolge, die für Sie wichtig ist. So finden Sie beispielsweise die Forderungen aller Normen an den Entwicklungsprozess zusammengefasst. Dabei konsolidiert dieses Buch diese Forderungen nicht nur; es gibt auch Tipps, wie Sie bei der Entwicklung medizinischer Software am besten nachweisen, dass Sie diese Forderungen erfüllt haben. Das spart Ihnen das mühsame Zusammentragen.

Forderungen, die keinen Bezug zur Software haben (z. B. die Sterilität von Produkten betreffend), nennt dieses Buch nicht. Dadurch ist diese Checkliste kompakt und spezifisch für medizinische Software.

Jeder Käufer dieses Buchs erhält einen Gutschein für ein kostenloses digitales Exemplar. Dieses personalisierte PDF-Dokument lässt sich beliebig oft ausdrucken. So können Sie die Checklisten in diesem Buch immer wieder ausfüllen.

Wussten Sie, dass auch Benannte Stellen diesen Auditleitfaden nutzen?

Ihre Vorteile auf einen Blick

- Sie erlangen Sicherheit beim Audit.
- Sie vermeiden unangenehme Beanstandungen und aufwendiges Nachbessern.
- Sie ersparen sich das mühsame Interpretieren von Normen und Gesetzen.
- Sie gewinnen dank einfach auszufüllender Checklisten einen schnellen Überblick.
- Sie identifizieren rasch Schwachstellen. Beheben Sie diese vor dem Audit.
- Sie verschaffen sich einen Wissensvorsprung, denn diese Leitfaden-Auflage nutzen auch Benannte Stellen.
- PDF-Version: Nutzen Sie die Checklisten, sooft Sie mögen.

Profitieren Sie von 50 % Rabatt bei allen weiteren Auflagen. Sie bleiben dadurch auf dem aktuellen Stand.

Auch für die Zukunft gerüstet

Die regulatorischen Anforderungen ändern sich ebenso wie Technologien und Verfahren. Dem wird dieser Leitfaden gerecht:

- Käufer enthalten einen 50%igen Rabatt auf alle künftigen Ausgaben.
- Auf unserer Webseite finden Sie Errata und eine Historie der Änderungen: www.johner-institut.de/auditleitfaden
- Abhängig von Ihrer Mitgliedschaft können Sie auf die digitale und kontinuierlich erweiterte Version des Leitfadens zugreifen, mit Hilfe von Filtern die für Sie relevanten Teile extrahieren und für Ihre Audits nutzen.

Bleiben Sie auch künftig immer auf dem aktuellen Stand der Technik und Regularien.

Ziel dieses Dokuments

Mit diesem Buch möchten wir Ihnen ein Werkzeug an die Hand geben, mit dem Sie sich als Verantwortlicher für die Entwicklung oder Qualitätssicherung medizinischer Software optimal auf Audits vorbereiten können. Ebenso unterstützt dieser Leitfaden Auditoren bei ihrer Arbeit, besonders bei der Vorbereitung und Durchführung von Audits.

Dieses Buch bietet Ihnen mehr als nur eine Konsolidierung und Gruppierung gesetzlicher Forderungen. Es transformiert softwareunspezifische Forderungen in softwarespezifische. Es berücksichtigt Best Practices und gibt Empfehlungen, die teilweise über die Normenforderungen hinausgehen bzw. konkreter sind als diese. Es gibt einige Forderungen der Normen, die in diesen Checklisten keine Berücksichtigung gefunden haben. Das liegt beispielsweise darin begründet, dass diese (wenigen) Forderungen keine Relevanz bei Audits haben oder hatten. Forderungen ohne Bezug zur Software fehlen. Dadurch gelingt es, die Checklisten in diesem Dokument vergleichsweise kompakt und spezifisch für ein Audit medizinischer Software zu gestalten.

Es ist das erklärte Ziel dieses Buchs, dass sowohl die Hersteller als auch die Auditoren medizinischer Software sehr schnell einen repräsentativen Überblick über die Güte der Software-Lebenszyklusprozesse wie die Entwicklung erhalten. Dabei wird weniger Wert darauf gelegt, dass jeder einzelne Satz jeder Norm geprüft wird, als dass Schwachstellen bei der Entwicklung medizinischer Software identifiziert werden, die mit hoher Wahrscheinlichkeit zu Qualitätseinbußen führen.

Berücksichtigte Vorschriften

Der Fokus dieses Dokuments liegt auf der Auditierung medizinischer Software. Dabei beschränkt sich dieser Leitfaden aber nicht auf die Forderungen der IEC 62304. Er betrachtet den kompletten Entwicklungsprozess und bezieht die technische Dokumentation sowie die relevanten Anforderungen an das Qualitätsmanagement mit ein.

Teilweise beziehen sich die Checklisten in diesem Dokument sogar auf Hardware und enthalten Aspekte der IEC 60601-1.

Dieses Buch berücksichtigt alle für die medizinische Software relevanten Richtlinien, Gesetze und Normen. Dazu zählen insbesondere:

- Medical Device Regulation MDR (Verordnung 2017/745 über Medizinprodukte)
- In Vitro Diagnostic Medical Device Regulation IVDR (Verordnung 2017/746 über In-vitro-Diagnostika)
- ISO 13485:2016 zu Qualitätsmanagementsystemen
- ISO 14971:2019 zum Risikomanagement
- IEC 62304:2015 zu den Lebenszyklusprozessen sowie zur Verifizierung
- IEC 62366-1:2015 zur Gebrauchstauglichkeit
- Entsprechende Anforderungen der FDA wie deren Guidance Documents, z. B. “General Principles of Software Validation”, „Human Factors Engineering“ und die Cybersecurity Guidances

Auch weil wir eine Konvergenz medizinischer Informationssysteme und Systeme im Pharmaumfeld beobachten, sind zudem einige GxP-relevanten Dokumente berücksichtigt. Dies sind der GAMP “Best practice guide: Testing of GxP systems” sowie PIC/S.

Die ISO 25010 nennt Qualitätseigenschaften von Software. Auch wenn diese Taxonomie nicht spezifisch für medizinische Software ist, so ist diese Norm dennoch relevant: Zum einen basiert das Kapitel 5.2 der IEC 62304 darauf. Zum anderen sind die in der ISO 25010 genannten Eigenschaften so allgemeingültig, dass sie zumindest teilweise Eingang in diese Checklisten finden sollte.

Haftungsausschluss

Dieses Dokument wurde nach bestem Wissen und Gewissen erstellt. Viele Jahre an Erfahrungen bei der Softwareentwicklung, bei der Erstellung und Überprüfung von Qualitätsmanagementsystemen und der Ausbildung von Software-Entwicklern sind eingeflossen. Dennoch können Fehler nicht ausgeschlossen werden.

Das Dokument hat nicht den Anspruch auf Vollständigkeit, wohl aber darauf, ein Hilfsmittel für effektive und effiziente Audits von Software-Entwicklungsabteilungen zu sein.

Die Interpretation und Übertragung von normativen und gesetzlichen Anforderungen auf die Entwicklung medizinischer Software hat auch einen subjektiven Charakter. Dennoch ist die Zuordnung beider transparent dargestellt.

Die Autoren lehnen jede Haftung ab, speziell Ansprüche, die aus den Folgen fehlerhafter medizinischer Software und deren Audits herrühren.

Danksagung

Die Autoren bedanken sich herzlich bei Christian Denger, Matthias Hölzer-Klüpfel und all den treuen Kunden, die zu diesem Auditleitfaden beigetragen haben.

Nr.	Prio	Überprüfungskriterium	Anmerkungen Auditor
AB:C01	1	☐	☐ OK ☐ Abweichung:
AB:C02	3	☐	☐ OK ☐ Abweichung:

Die Checklisten sind möglichst kompakt gehalten, um ein effizientes Auditieren zu ermöglichen. Daher sind die Checklisten tabellarisch gestaltet. Dabei bedeuten:

1 **Nr:** Eine eindeutige Nummer, auf die Bezug genommen werden kann.

2 **Prio:** Die Priorität stellt das Maß dafür dar, wie wichtig es ist, dass das Überprüfungskriterium eingehalten ist.

- **1:** Hohe Priorität. Verstöße gegen das zugehörige Kriterium sind als kritisch zu erachten. Sie stehen im Widerspruch zu grundlegenden Vorschriften oder Best Practices und stellen typische Ursachen für fehlerhafte Software dar. Bei Verstößen ist eine entsprechende „Würdigung" empfohlen, beispielsweise in Form einer Abweichung.
- **2:** Mittlere Priorität. Verstöße gegen das zugehörige Kriterium müssen begründet sein. Sie stellen einen Hinweis darauf dar, dass relevante Vorschriften oder Best Practices nicht eingehalten werden. Es ist empfohlen, die Auswirkungen auf das Endprodukt zu untersuchen.
- **3:** Niedrige Priorität. Verstöße gegen das zugehörige Kriterium sind nicht unmittelbar kritisch. Eine hohe Anzahl solcher Verstöße kann allerdings die Güte des Produkts wesentlich beeinflussen. Dies sollte im Audit mit dem Kunden diskutiert werden.

3 **Überprüfungskriterium:** Hier sind Punkte gelistet, die als Hinweis für eine Einhaltung des Kriteriums zu verstehen sind. Treffen nur wenige der genannten Punkte zu, so ist davon auszugehen, dass das Kriterium nicht eingehalten ist, also ein Verstoß vorliegt. Essenzielle Kriterien sind mit (!) gekennzeichnet. Ein Verstoß dagegen macht eine Einhaltung des Kriteriums unwahrscheinlich. Die meisten Überprüfungskriterien sind mit einem Verweis versehen. Hier finden sich weiterführende Informationen, speziell die entsprechenden Kapitel/Abschnitte/Paragraphen der relevanten Normen, Gesetze und sonstiger Best Practices und Vorschriften. **Hinweise für Prüfer sind rot hervorgehoben.**

4 **Anmerkungen Auditor:** Hier tragen die Prüfer (interne Prüfer oder externe Auditoren) ihre Beobachtungen ein und bewerten, ob das jeweilige Kriterium erfüllt ist.

ZWECKBESTIMMUNG

Nr.	Prio	Überprüfungskriterium	Anmerkungen Auditor
	1	**Medizinische Indikation**	
ZB:A01		☐ (!) Es gibt eine dokumentierte Zweckbestimmung.[1]	☐ OK ☐ Abweichung:
ZB:A02		☐ Die Zweckbestimmung verweist eindeutig auf ein Produkt bzw. eine Produktversion, z. B. über dessen UDI-DI.	☐ OK ☐ Abweichung:
ZB:A03		☐ Die Zweckbestimmung legt den Nutzen des Produkts fest, z. B. ob es der Diagnose, Therapie, Linderung oder/und Überwachung dient.[2]	☐ OK ☐ Abweichung:
ZB:A04		☐ Die Zweckbestimmung legt die Indikation fest, d. h., bei welchen Krankheiten oder Verletzungen es diesen Nutzen bringt.[3, 4, 5]	☐ OK ☐ Abweichung:
ZB:A05		☐ Die Zweckbestimmung beschreibt, wie das Produkt der Diagnose, Therapie oder Überwachung von Krankheiten oder Verletzungen (oder physiologischer oder anatomischer Parameter) dient (z. B. physikalisches Prinzip).[6]	☐ OK ☐ Abweichung:
ZB:A06		☐ Die Zweckbestimmung nennt die Umstände (z. B. Krankheiten), unter denen die Verwendung des Produkts kontraindiziert ist.[7]	☐ OK ☐ Abweichung:
ZB:A07		☐ (!) Die Zweckbestimmung beschreibt die vorgesehene Patientengruppe (einschließlich Alter, Gesundheitszustand, Gewicht).	☐ OK ☐ Abweichung:
ZB:A08		☐ Die Zweckbestimmung beschreibt, welche Körperregion bzw. welches Gewebe untersucht, diagnostiziert, therapiert oder überwacht werden soll.	☐ OK ☐ Abweichung:

Nr.	Prio	Überprüfungskriterium	Anmerkungen Auditor
	2	**Nutzer, Nutzungskontext**	
ZB:B01		☐ (!) Die Zweckbestimmung charakterisiert die primären und sekundären[8] Nutzergruppen.[9]	☐ OK ☐ Abweichung:
ZB:B02		☐ Die Charakterisierung beinhaltet demographische Merkmale (Alter, Geschlecht) der vorgesehenen Nutzer.	☐ OK ☐ Abweichung:
ZB:B03		☐ Die Charakterisierung nennt den Beruf bzw. die Funktion innerhalb der Organisation der vorgesehenen Nutzer.	☐ OK ☐ Abweichung:
ZB:B04		☐ Die Charakterisierung legt notwendige Fähigkeiten und Kenntnisse der vorgesehenen Nutzer fest inklusive Ausbildung, Sprachkenntnisse, spezielle relevante Fähigkeiten, Erfahrungen mit gleichen oder ähnlichen Produkten.	☐ OK ☐ Abweichung:
ZB:B05		☐ Die Charakterisierung beschreibt mögliche körperliche oder andere Einschränkungen und Besonderheiten der vorgesehenen Nutzer.	☐ OK ☐ Abweichung:
ZB:B06		☐ Die Zweckbestimmung beschreibt den Nutzungskontext[10] inklusive Kernaufgaben, Häufigkeit der Anwendung und zu erzielende Ergebnisse.[11]	☐ OK ☐ Abweichung:
ZB:B07		☐ Die Zweckbestimmung legt den vorgesehenen Ort der Anwendung[12] und – soweit relevant – die dort vorherrschenden physikalischen Parameter fest wie Helligkeit, Temperatur, Lautstärke, Feuchtigkeit, Verschmutzung, Luftdruck.[13, 14, 15, 16, 17]	☐ OK ☐ Abweichung:
ZB:B08		☐ Die Zweckbestimmung charakterisiert die Nutzungsumgebung, z. B. Stress-Niveau, Schichtbetrieb, Notfallsituationen, Tragen von Handschuhen.	☐ OK ☐ Abweichung:
ZB:B09		☐ Die Zweckbestimmung dokumentiert, ob das Produkt im Rettungswagen, Hubschrauber oder bestimmten medizinischen Räumen wie OPs genutzt werden soll.[18]	☐ OK ☐ Abweichung: