

---

# Inhaltsübersicht

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>2</b>	<b>Rechtliche Grundlagen</b>	<b>9</b>
<b>3</b>	<b>Qualitätsmanagement</b>	<b>71</b>
<b>4</b>	<b>Risikomanagement</b>	<b>83</b>
<b>5</b>	<b>Lebenszyklus medizinischer Software</b>	<b>119</b>
<b>6</b>	<b>Gebrauchstauglichkeit</b>	<b>171</b>
<b>7</b>	<b>Dokumentenmanagement</b>	<b>205</b>
<b>8</b>	<b>Medizinische Informatik</b>	<b>215</b>
<b>9</b>	<b>IT-Sicherheit bei Medizinprodukten</b>	<b>231</b>

## Anhang

---

<b>Abkürzungsverzeichnis</b>	<b>249</b>
<b>Quellenverzeichnis</b>	<b>253</b>
<b>Index</b>	<b>257</b>

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Aufbau dieses Buches .....	2
1.2	Initiative »Certified Professional for Medical Software« (CPMS) ...	3
1.3	Zuordnung der Kapitel dieses Buches zum Curriculum des CPMS ..	4
<b>2</b>	<b>Rechtliche Grundlagen</b>	<b>9</b>
2.1	Die Rechtslage in Europa .....	9
2.1.1	Das sogenannte neue Konzept für Produktregulierung innerhalb der Europäischen Union .....	9
2.1.2	Regulatorische Landkarte für Medizinprodukte .....	12
2.2	Regulatorische Vorgaben für Medizinprodukte .....	14
2.2.1	Die Medizinprodukterichtlinie und die Medizin- produkteverordnung .....	14
2.2.2	Besonderheiten für aktive implantierbare medizinische Geräte .....	33
2.2.3	Besonderheiten für In-vitro-Diagnostika .....	33
2.2.4	Die Gesetzgebung in der Bundesrepublik Deutschland ...	35
2.3	Harmonisierte Normen .....	39
2.3.1	Das neue Konzept der Europäischen Union .....	39
2.3.2	Entstehung von harmonisierten Normen .....	39
2.3.3	Veröffentlichung von harmonisierten Normen .....	40
2.4	Relevante harmonisierte Normen .....	40
2.4.1	Qualitätsmanagement (EN ISO 13485) .....	41
2.4.2	Risikomanagement (EN ISO 14971) .....	41
2.4.3	Software-Lebenszyklus-Prozesse (EN 62304) .....	41
2.4.4	Gebrauchstauglichkeit (EN 62366 und EN 60601-1-6) ...	42
2.4.5	Normenfamilie EN 60601 über medizinische elektrische Geräte .....	42

2.5	Anwendung und Kontrolle rechtlicher Vorgaben	45
2.5.1	Lebenszyklus eines Medizinproduktes	45
2.5.2	Überwachung von Herstellern	50
2.5.3	Überwachung von benannten Stellen	54
2.6	Weltweite Harmonisierungsbemühungen – die GHTF und das IMDRF	56
2.7	Die Situation in den USA	56
2.7.1	Aufbau der Gesetzgebung	57
2.7.2	Federal Food, Drug, and Cosmetic Act (FD&C Act)	58
2.7.3	Code of Federal Regulations Title 21 (21 CFR)	59
2.7.4	Food and Drug Administration (FDA)	60
2.7.5	Klassifizierung von Medizinprodukten	60
2.7.6	Inverkehrbringen von Medizinprodukten	61
2.7.7	Softwarespezifische Vorgaben	63
2.7.8	Vergleich mit Europa	67
2.8	Weitere internationale Behörden	68
<b>3</b>	<b>Qualitätsmanagement</b>	<b>71</b>
3.1	Aufbau der Norm ISO 13485	71
3.2	Prozessorientierter Ansatz	72
3.3	Dokumentationsanforderungen	72
3.3.1	Qualitätsmanagement-Handbuch	73
3.3.2	Zu dokumentierende Verfahren	73
3.3.3	Dokumente und Aufzeichnungen	74
3.4	Verantwortung der Leitung	75
3.5	Management von Ressourcen	75
3.6	Produktrealisierung	76
3.6.1	Planung	76
3.6.2	Einbindung des Kunden	76
3.6.3	Design und Entwicklung	77
3.6.4	Beschaffung	78
3.6.5	Produktion und Dienstleistungserbringung	78
3.6.6	Umgang mit Kundeneigentum	79
3.6.7	Überwachung von Messmitteln	80
3.7	Messung, Analyse und Verbesserung	80
3.7.1	Sammeln von Rückmeldungen	80
3.7.2	Internes Audit	81
3.7.3	Messung von Prozessen	81

3.7.4	Fehlerhafte Produkte .....	81
3.7.5	Verbesserung .....	81
<b>4</b>	<b>Risikomanagement</b>	<b>83</b>
4.1	Einführung .....	83
4.1.1	Regulatorischer Rahmen .....	83
4.1.2	Bedeutung des Risikomanagements .....	85
4.1.3	Begriffe .....	85
4.2	Die Risikobewertungsmatrix .....	89
4.2.1	Definition der Achsen .....	90
4.2.2	Risikoakzeptanz .....	92
4.3	Verfahren zur Risikoanalyse .....	92
4.3.1	Vorläufige Gefährdungsanalyse (PHA) .....	92
4.3.2	Fehlerbaumanalyse (FTA) .....	95
4.3.3	Fehlermöglichkeits- und -einflussanalyse (FMEA) .....	96
4.3.4	Abschätzen von Wahrscheinlichkeit und Schweregrad ...	98
4.4	Die ISO 14971 .....	99
4.4.1	Allgemeine Anforderungen an das Risikomanagement ...	99
4.4.2	Der Risikomanagementprozess .....	101
4.4.3	Dokumentation .....	107
4.5	Zusammenspiel mit anderen Normen .....	109
4.5.1	Zusammenspiel mit der ISO 13485 .....	109
4.5.2	Zusammenspiel mit der IEC 62304 .....	110
4.5.3	Zusammenspiel mit der IEC 62366-1 .....	111
4.6	Risikomanagement bei Software .....	112
4.6.1	Definition Softwaresicherheitsklassen .....	112
4.6.2	Wahrscheinlichkeit und Softwaresicherheitsklassen .....	114
4.6.3	Dekomposition des Softwaresystems .....	115
4.6.4	Einflüsse auf die Architektur .....	116
4.7	Zusammenfassung .....	117
<b>5</b>	<b>Lebenszyklus medizinischer Software</b>	<b>119</b>
5.1	Softwareentwicklungsprozesse .....	119
5.1.1	Regulatorische Anforderungen .....	119
5.1.2	Vorgehensmodelle .....	119
5.1.2.1	Einführung .....	119
5.1.2.2	Wasserfallmodell .....	121
5.1.2.3	V-Modell .....	122
5.1.2.4	Iterativ-inkrementelle Modelle .....	123

---

5.1.3	Prozessbeschreibung	124
5.1.3.1	Einführung	124
5.1.3.2	Prozessgebiete festlegen	125
5.1.4	Konformitätsnachweis	126
5.1.4.1	Einführung	126
5.1.4.2	Audits bestehen	126
5.2	Softwareentwicklung	127
5.2.1	Entwicklungsplanung	127
5.2.1.1	Einführung	127
5.2.1.2	Softwareentwicklung planen	127
5.2.1.3	Entwicklungsprozesse anpassen	128
5.2.1.4	Standards, Methoden und Werkzeuge auswählen	128
5.2.1.5	Projekte planen	129
5.2.2	Softwareanforderungsanalyse	129
5.2.2.1	Einführung	129
5.2.2.2	Softwareanforderungen ableiten	130
5.2.2.3	Softwareanforderungen formulieren	131
5.2.2.4	Softwareanforderungen verifizieren	133
5.2.3	Softwarearchitektur	134
5.2.3.1	Einführung	134
5.2.3.2	Softwarearchitektur beschreiben	135
5.2.3.3	Sicherheitsklasse reduzieren	138
5.2.3.4	Risikobehandlung sicherstellen	139
5.2.3.5	SOUP einsetzen	140
5.2.3.6	Softwarearchitektur verifizieren	140
5.2.4	Softwaredesign	141
5.2.4.1	Einführung	141
5.2.4.2	Softwaredesign beschreiben	142
5.2.4.3	Schnittstellen definieren	143
5.2.4.4	Design verifizieren	143
5.2.5	Implementierung	143
5.2.5.1	Einführung	143
5.2.5.2	Softwareeinheiten implementieren	144
5.2.5.3	Akzeptanzkriterien festlegen	144
5.2.5.4	Codierrichtlinien einsetzen	145
5.2.5.5	Softwareeinheiten verifizieren	145
5.2.6	Integration	146
5.2.6.1	Einführung	146
5.2.6.2	Software-Build beherrschen	147
5.2.6.3	Integrationsstrategie festlegen	148
5.2.6.4	Integration verifizieren	148

5.2.7	Softwaretest	149
5.2.7.1	Einführung	149
5.2.7.2	Testebenen auswählen	149
5.2.8	Tests planen	150
5.2.8.1	Tests durchführen	150
5.2.8.2	Tests verifizieren	151
5.2.8.3	Änderungen prüfen	152
5.2.9	Freigabe	152
5.2.9.1	Einführung	152
5.2.9.2	Entwicklung abschließen	153
5.2.9.3	Software archivieren	153
5.2.9.4	Validierung durchführen	154
5.3	Softwarekonfigurationsmanagement	156
5.3.1	Einführung	156
5.3.2	Konfigurationskontrolle	156
5.3.2.1	Konfigurationselemente identifizieren	156
5.3.2.2	Elemente und Versionen kennzeichnen	157
5.3.2.3	Versionskontrollsystem nutzen	157
5.3.2.4	Softwareversionen benennen	159
5.3.2.5	SOUP identifizieren	160
5.3.3	Änderungskontrolle	161
5.3.3.1	Änderungsanforderungen genehmigen	161
5.3.3.2	Änderungen implementieren	161
5.3.3.3	Rückverfolgbarkeit sicherstellen	162
5.4	Softwareproblemlösung und -wartung	162
5.4.1	Einführung	162
5.4.2	Softwareproblemlösung	163
5.4.2.1	Problembereiche erstellen	163
5.4.2.2	Probleme lösen	164
5.4.2.3	Problemlösung verifizieren	165
5.4.2.4	Trends analysieren	165
5.4.3	Softwarewartung	165
5.4.3.1	Wartung planen	165
5.4.3.2	Rückmeldungen behandeln	166
5.4.3.3	Änderung implementieren	167
5.4.3.4	Software freigeben	168
5.5	Umgang mit älterer Software	168
5.5.1	Einführung	168
5.5.2	Risikomanagement	169
5.5.2.1	Rückmeldungen auswerten	169
5.5.2.2	Risikomanagementaktivitäten durchführen	169

5.5.3	Umgang mit Lücken . . . . .	169
5.5.3.1	Lücken identifizieren . . . . .	169
5.5.3.2	Aktivitäten planen . . . . .	170
5.5.3.3	Lücken schließen . . . . .	170
5.5.4	Dokumentation . . . . .	170
5.5.4.1	Version dokumentieren . . . . .	170
5.5.4.2	Nutzung begründen . . . . .	170
<b>6</b>	<b>Gebrauchstauglichkeit</b>	<b>171</b>
6.1	Einführung . . . . .	171
6.1.1	Bedeutung der gebrauchstauglichkeitsorientierten Entwicklung . . . . .	171
6.1.2	Übersicht . . . . .	172
6.1.3	Definitionen . . . . .	173
6.2	Regulatorisches Umfeld . . . . .	175
6.2.1	EU-Verordnungen, Gesetze und Behörden . . . . .	175
6.2.2	Normen . . . . .	177
6.3	Weg zu validen Anforderungen . . . . .	180
6.3.1	Benutzer identifizieren und charakterisieren . . . . .	181
6.3.2	Kontext erheben und Zweckbestimmung festlegen . . . . .	182
6.3.3	Nutzungsanforderungen ableiten . . . . .	182
6.4	Benutzungsschnittstelle konzipieren . . . . .	185
6.4.1	Nutzungsszenarien für jede zu unterstützende Kernaufgabe konstruieren . . . . .	185
6.4.2	Benutzungsschnittstelle spezifizieren . . . . .	186
6.4.3	Prototyp entwerfen und prüfen . . . . .	189
6.5	Prüfung: Verifizierung und Validierung . . . . .	190
6.5.1	Inspektionsverfahren . . . . .	190
6.5.2	Teilnehmende Beobachtung (Usability-Test) . . . . .	194
6.5.3	Qualitative und quantitative Benutzerbefragungen . . . . .	195
6.5.4	Zusammenfassung der Prüfverfahren . . . . .	195
6.6	IEC-62366-1-konforme Dokumentation . . . . .	196
6.6.1	Gebrauchstauglichkeitsorientierter Entwicklungsprozess . . . . .	196
6.6.2	Gebrauchstauglichkeitsakte . . . . .	198
6.7	UOUP: Benutzer-Produkt-Schnittstellen unbekannter Herkunft . . .	202
6.8	Zusammenfassung . . . . .	203

<b>7</b>	<b>Dokumentenmanagement</b>	<b>205</b>
7.1	Einführung	205
7.2	Allgemeine Anforderungen an Dokumente	205
7.3	Geforderte Dokumentation	207
7.3.1	Qualitätsmanagement	207
7.3.2	Risikomanagementakte	208
7.3.3	Gebrauchstauglichkeitsakte	208
7.3.4	Dokumentation der Softwareentwicklung	209
7.3.5	Technische Dokumentation	210
7.3.6	Sonstige Dokumente	211
7.3.7	Übersicht über geforderte Dokumente	211
7.4	Umgang mit Dokumenten	212
7.5	Zusammenfassung	214
<b>8</b>	<b>Medizinische Informatik</b>	<b>215</b>
8.1	Einführung	215
8.1.1	Gesundheitswesen	215
8.1.2	Informationssysteme	217
8.2	Interoperabilität	218
8.2.1	Interoperabilitätsebenen	218
8.2.2	Kommunikationsstandards	220
8.2.3	Semantische Standards	229
8.3	Zusammenfassung	230
<b>9</b>	<b>IT-Sicherheit bei Medizinprodukten</b>	<b>231</b>
9.1	Einführung	231
9.1.1	Probleme mit der IT-Sicherheit	231
9.1.2	IT-Sicherheit: Begriffsdefinition und Ziele	231
9.1.3	Das STRIDE-Modell	233
9.2	Regulatorische Rahmen	233
9.2.1	MDR und IVDR	233
9.2.2	Normen	234
9.2.3	MDCG 2019-16	235
9.2.4	Nationale Vorgaben für Medizinprodukte	235
9.2.5	Vorgaben an die IT-Sicherheit, die nicht spezifisch für Medizinprodukte gelten	236



9.3	IT-Sicherheit im Produktlebenszyklus . . . . .	236
9.3.1	Allgemeines . . . . .	236
9.3.2	Zweckbestimmung und Stakeholder-Anforderungen . . . .	237
9.3.3	System- und Softwareanforderungen . . . . .	237
9.3.4	System- und Softwarearchitektur . . . . .	240
9.3.5	Testaktivitäten . . . . .	241
9.3.6	Softwarefreigabe . . . . .	241
9.3.7	Überwachung des Produktes im Markt nach dem Inverkehrbringen . . . . .	242
9.4	Produktanforderungen . . . . .	243
9.4.1	Authentifizierung und Autorisierung . . . . .	243
9.4.2	Daten und Kommunikation . . . . .	244
9.4.3	Audit-Log . . . . .	244
9.4.4	Begleitmaterialien . . . . .	245
9.5	Zusammenfassung . . . . .	245

## Anhang

---

<b>Abkürzungsverzeichnis</b>	<b>249</b>
<b>Quellenverzeichnis</b>	<b>253</b>
<b>Index</b>	<b>257</b>