

-

Die APV-Richtlinie
„Computergestützte Systeme“
basierend auf dem Annex 11 zum EU-GMP-Leitfaden

Ein Beitrag der APV-Fachgruppe Informationstechnologie

Die in diesem Beitrag aufgeführten Interpretationen des Annex 11 stellen die persönliche Sicht der Mitglieder der Fachgruppe dar

Vorwort

Mit der Betriebsverordnung für Pharmazeutische Unternehmer in der Fassung vom August 1994 wurde die Rechtsgrundlage zur umfassenden Durchsetzung des EU-GMP-Leitfadens mit seinem Annex 11 „Computergestützte Systeme“ geschaffen.

Dieser Annex beschreibt die Vorkehrungen für die Entwicklung und den Betrieb von Computersystemen im GMP-Bereich. Darüber hinaus ist dieser Annex auch für den GCP-Teilbereich der Dateneingabe durch einen Verweis in der EU-GCP-Richtlinie gültig.

Die Kürze der Abschnitte im Annex 11 läßt viel Raum für Interpretationen und erzeugt somit eine erhebliche Unsicherheit bei den Herstellern und Anwendern Computergestützter Systeme.

Aus diesem Grund haben die Mitglieder der Fachgruppe Informationstechnologie der APV den Annex 11 auf Basis der bisher erschienenen Richtlinien, Publikationen und eigenen Erfahrungen interpretiert. Diese Interpretation wird in diesem Beitrag in Form einer APV-Richtlinie veröffentlicht.

Die vorliegende APV-Richtlinie stellt ein mögliches Procedere für die Entwicklung und den Betrieb von Computergestützten Systemen dar. In jedem Einzelfall bleibt es deshalb in der Verantwortung des Pharmazeutischen Unternehmers, festzustellen, wo Schwerpunkte zu setzen sind oder wo definierte Kriterien einen reduzierten Aufwand zulassen bzw. einen erhöhten Aufwand erfordern.

Die folgenden Mitglieder der Fachgruppe Informationstechnologie haben die APV-Richtlinie erarbeitet:

Dr. Helmut Bender	Boehringer Ingelheim KG
Dr. Rango Dietrich	Byk Gulden GmbH
Dr. Heinrich Hambloch	GITP (Leiter der Fachgruppe)
Dipl.-Ing. Ottomar Henning	Schering AG
Ap. Karl-Heinz Menges	Regierungspräsidium Darmstadt
Dr. Dirk Spingat	Bayer AG

Anmerkungen

- Zur Unterscheidung zwischen Annex 11 und dieser APV-Richtlinie sind die Themenbereiche des Annex 11 durchgängig als "Punkte" und die Aufteilung innerhalb dieser APV-Richtlinie als "Abschnitte" bezeichnet. Die APV-Richtlinie behandelt alle Punkte des Annex 11, weicht jedoch aus Gründen einer günstigeren Strukturierung von der dort vorgegebenen Reihenfolge ab:

Abschnitte der APV-Richtlinie	Punkte des Annex 11
Allgemeiner Teil	Begriffsbestimmungen, Grundsätze, Punkte 1, 18
Lebenszyklusmodell	Punkte 2, 3, 4, 5, 7, 11
Zugriffsautorisierung	Punkte 8, 10
Dateneingabe	Punkte 6, 9, 19
Datenablage und Datensicherung	Punkte 12, 13, 14
Fehlerbehandlung und Systemausfall	Punkte 15, 16, 17

- Die Randzahlen verweisen auf die Punkte und Sätze des Annex 11 ([8.3] bedeutet Punkt 8, Satz 3: In einem Verfahren sollte). Ein entsprechend durchnummerierter Annex 11 befindet sich im Anhang 7.1).
- Durch *Kursivdruck* gekennzeichnete Begriffe sind im Glossar näher erläutert
- Die APV-Richtlinie setzt implizit voraus, daß alle im Text vorgeschlagenen Aktivitäten und Festlegungen auf beliebigen Medien lesbar und nachvollziehbar dokumentiert werden, auch wenn dies im jeweiligen Text nicht gesondert erwähnt ist.

Inhaltsverzeichnis

1 ALLGEMEINER TEIL	5
1.1 Begriffsbestimmungen	5
1.2 Grundsätze	7
1.3 Personal	8
1.4 Dienstleistungen externer Unternehmen	10
2 LEBENSZYKLUSMODELL	12
2.1 Phasenbezogene Aktivitäten	14
2.2 Phasenübergreifende Aktivitäten	19
2.3 Prospektive und Retrospektive <i>Validierung</i>	23
3 ZUGRIFFSAUTORISIERUNG	25
4 DATENEINGABE	26
5 DATENABLAGE UND DATENSICHERUNG	28
6 FEHLERBEHANDLUNG UND SYSTEMAUSFALL	31
7 ANHANG	33
7.1 Ergänzende Leitlinien für computergestützte Systeme	33
7.2 Glossar	37
7.3 Literatur	39

1 Allgemeiner Teil

1.1 Begriffsbestimmungen

System, Computergestütztes System

Wird der Begriff "System" auf computergestützte Systeme (CS) angewendet, so sollten diese ganzheitlich die Kombination aller Hard- und Software-Elemente umfassen. Die Aktivitäten und Techniken zur Erstellung und zum Betrieb eines CS werden im Lebenszyklusmodell definiert und umgesetzt (siehe Abschnitt 2). [0.1]
[0.2]
[2.2]

Entsprechend dieser ganzheitlichen Sicht sind periphere Komponenten zur Eingabe wie [4.1]

- Barcodeleser
- Scanner
- on-line Datenerfassung aus Prozessen
- manuelle Erfassung von Daten über Bildschirm und Tastatur

dem System zuzurechnen.

Die elektronische Verarbeitung umfaßt die Systemkomponenten [4.1]

- Rechnerhardware (CPU, Netzwerkkomponenten)
- systemnahe Softwarebestandteile wie
 - ◆ Betriebssysteme
 - ◆ Netzwerksoftware
 - ◆ Datenbankumgebungen
 - ◆ Peripherietreiber
 - ◆ Programmiersprachen (Interpreter, Compiler)
 - ◆ SPS Entwicklungsumgebungen
- Anwendungsprogramme wie
 - ◆ Textverarbeitung
 - ◆ Datenbanken
 - ◆ Spreadsheets
 - ◆ Grafikprogramme
 - ◆ Materialwirtschaftssysteme
 - ◆ PPS
 - ◆ SPS Programme und Prozeßleitsysteme

und alle denkbaren Kombinationen dieser Teile.

Die Ausgabe erfolgt durch die entsprechenden Systemteile der oben

genannten Komponenten zur Verarbeitung sowie durch periphere Hardware wie

[4.1]

- Bildschirme
- Drucker
- Medien (Papier)
- Datenträger
- Steuerungen

1.2 Grundsätze

Alle validierungspflichtigen CS sollten identifiziert werden. Dazu zählen alle CS, die die Produktqualität und Qualitätssicherung in den im Annex genannten Bereichen Herstellung, Lagerhaltung, Verteilung und Qualitätskontrolle beeinflussen können.

Zu diesem Zweck sollten Vorschriften zur Identifizierung solcher CS zusammen mit Entscheidungskriterien für die Zuordnung „validierungspflichtig“ vorhanden sein.

[0.3]

[0.4]

Der Annex verlangt auch für CS die Berücksichtigung allgemeiner GMP Grundsätze und geht sogar über das klassische Anwendungsgebiet von GMP hinaus, indem die Verteilung der Arzneimittel ebenfalls diesem Annex unterworfen wird.

[0.3]

1.3 Personal

Es sollte qualifiziertes Personal mit einschlägiger Erfahrung in ausreichender Zahl vorhanden sein, das alle in der Verantwortung des Pharmazeutischen Unternehmers liegenden Aufgaben im Zusammenhang mit Planung, Einführung, Anwendung (Betrieb), Anwendungsberatung und regelmäßiger Überprüfung von Computersystemen ausführt.

[1.1]
[1.2]
[1.3]

Die Qualifikation des Personals sollte gemäß beruflicher Ausbildung, Schulung und Erfahrung im Umgang mit und der Entwicklung von computergestützten Systemen beurteilt werden. Die Qualifikationsanforderungen sollten sich nach dem Einsatzbereich des Personals richten. Es darf nur entsprechend seiner Ausbildung und seinen Kenntnissen beschäftigt werden.

Die individuellen Verantwortungsbereiche sollten schriftlich festgelegt von jedem einzelnen klar verstanden sein. Die Übernahme von Entscheidungsfunktionen durch computergestützte Systeme ändert nichts an den gesetzlich festgelegten Verantwortlichkeiten der Personen in Schlüsselstellungen.

Die Gefahr, daß nach Einführung eines CS durch eine verringerte Beteiligung des Bedienungspersonals bestimmte Gesichtspunkte des früheren Verfahrens wie Qualität oder *Sicherheit* verlorengehen, sollte berücksichtigt werden.

[0.5]

Der Pharmazeutische Unternehmer sollte für die Schulung aller Personen sorgen, die Aufgaben im Zusammenhang mit computergestützten Systemen zu erfüllen haben, und ihnen die Inhalte der einschlägigen computergestützten Systeme betreffenden Richtlinien nahebringen. Das sollte auch für Systementwickler, Wartungs- und Reparaturpersonal und Personal gelten, dessen Tätigkeit die dokumentierte Funktionsfähigkeit der Systeme beeinflussen könnte.

Neben der Grundunterweisung im Zusammenhang mit computergestützten Systemen sollten neu eingestellte Personen den ihnen jeweils zugewiesenen Aufgaben entsprechend geschult werden. Darüber hinaus sollten gemäß festgelegten Schulungsprogrammen fortlaufende Unterweisungen durchgeführt und deren Umsetzung in die Praxis periodisch bewertet werden.

Im Rahmen der Schulung sollten das Konzept der GMP, des Lebenszyklus und alle Maßnahmen, die dessen Verständnis und Anwendung verbessern können, vermittelt werden. Schulungsmaßnahmen und Qualifikationsnachweise sollten dokumentiert und als Bestandteil der Lebenszyklusdokumentation archiviert werden.

1.4 Dienstleistungen externer Unternehmen

Sind externe Unternehmen an dem Betrieb oder der Entwicklung von computergestützten Systemen beteiligt, sollten die Verantwortlichkeiten in entsprechenden schriftlichen Verträgen, wie sie auch im GMP Bereich als Verträge über die Herstellung im Auftrag vorge-schrieben sind, festgelegt und abgegrenzt werden.

[18.1]
[5.2]

Technische und qualitätssichernde Aspekte des Vertrags sollten unter Beteiligung von kompetenten, in pharmazeutischer Technologie, Analytik und in der Entwicklung, Wartung, dem Betrieb und der Anwendung von computergestützten Systemen qualifizierten Personen abgefaßt werden.

Das externe Unternehmen sollte keine ihm vertraglich übertragene Arbeit ohne schriftliche Zustimmung des Auftraggebers an Dritte weitergeben.

Auch wenn Aufgabenstellungen teilweise an externe Unternehmen vergeben werden, bleibt die Verantwortlichkeit für Eignung und Funktionsfähigkeit computergestützter Systeme beim Pharmazeutischen Unternehmer.

Der Pharmazeutische Unternehmer ist verantwortlich für die Beurteilung, ob das externe Unternehmen kompetent ist, die erforderlichen Arbeiten erfolgreich auszuführen. Er hat dies ggf. durch einen Audit bzw. durch Beschaffung entsprechender Unterlagen zu überprüfen.

Der Pharmazeutische Unternehmer sollte sich regelmäßig vergewissern, daß das externe Unternehmen das computergestützte System ordnungsgemäß und entsprechend der vorher spezifizierten Systembeschreibung entwickelt, wartet oder betreibt.

Das externe Unternehmen sollte über geeignete Räumlichkeiten und die erforderliche Ausrüstung, ausreichende Sachkenntnis und Erfahrung sowie über kompetentes Personal verfügen, um die ihm vom Auftraggeber übertragenen Arbeiten zufriedenstellend ausführen zu können. Auftragsarbeiten im Zusammenhang mit computergestützten Systemen sollten nur von externen Unternehmen übernommen werden, bei denen die obigen Voraussetzungen überprüft und dokumentiert nachgewiesen sind.

Der Auftraggeber sollte sicherstellen, daß der Auftragnehmer sich über alle Probleme im Klaren ist, die mit der vergebenen Aufgabenstellung in Zusammenhang stehen und die ein Risiko für die Patientensicherheit, die Arzneimittelqualität, seine Räumlichkeiten, die Ausrüstung, das Personal oder für andere Materialien oder Produkte

darstellen könnten.

Auch bei externen Unternehmen sollte für das dort eingesetzte Personal eine definierte Qualifikation nachgewiesen werden, die sich nach dem Einsatzbereich der beteiligten Mitarbeiter richtet.

Die vertraglich vereinbarten Lebenszyklusdokumente sollten dem Auftraggeber während der festgelegten Aufbewahrungsdauer zur Verfügung stehen (siehe Abschnitt 2.1 „Stilllegung“).

Der Vertrag sollte dem Auftraggeber gestatten, Einblick in die Einrichtungen und die Arbeitsmethodiken des Auftragnehmers und dessen Subunternehmer zu nehmen.

Der Auftragnehmer sollte sich darüber im Klaren sein, daß er u.U. der Inspektion durch die zuständigen Behörden unterworfen ist.

Der Vertrag sollte im Auftrag des Pharmazeutischen Unternehmers durch qualifizierte Personen überprüft werden.

2 Lebenszyklusmodell

Computergestützte Systeme sollten gemäß dem Lebenszyklusmodell entwickelt, implementiert und betrieben werden. Dabei sollten die folgenden Phasen berücksichtigt werden:

- Erstellung Projektkonzept
- Erstellung Qualitätsplan
- Erstellung Anwendungsspezifikation
- Durchführung *Risikoanalyse*
- Erstellung Entwicklungsspezifikation
- Entwicklung der Systemkomponenten (Hard- und Software)
- Erstellung der Handbücher für die Benutzung
- Installation und Inbetriebnahme
- Akzeptanztestplanung und -durchführung
- Freigabe
- Betrieb mit
 - ♦ Änderungskontrolle
 - ♦ Systemüberwachung und -wartung
 - ♦ Fehlerbehandlung
 - ♦ sowie allen in den Abschnitten 3, 4, 5, und 6 beschriebenen Annex 11-spezifischen Aktivitäten
- Stilllegung

Folgende Aktivitäten/Festlegungen sind phasenübergreifend:

- Planung und Durchführung von Tests
- Konfigurationskontrolle
- Planung und Durchführung von Audits
- Planung und Durchführung von *Reviews*

Für alle Phasen und alle phasenübergreifenden Aktivitäten sollten Arbeitsvorschriften (SOPs) vorhanden sein, die die Aktivitäten in einem für Fachleute verständlichen und ausreichenden Detaillierungsgrad beschreiben. Die erzielten Ergebnisse der Aktivitäten sollten im Rahmen von *Reviews* gegen die Arbeitsvorschriften geprüft und ggf. bis zur Übereinstimmung korrigiert werden. Dadurch wird ein formales Qualitätssicherungssystem geschaffen.

Die im folgenden dargestellten Phasen bzw. phasenübergreifenden Aktivitäten stellen eine Richtschnur dar. Sie können je nach Komplexität des CS entweder sinnvoll zusammengefaßt oder auch zusätzlich unterteilt und von unterschiedlichen Beteiligten durchgeführt werden (Pharmazeutischer Unternehmer, externe Auftragnehmer).

[2.2]
[2.3]
[5.1]
[5.2]

[7.1]

[11]

[15 - 17]

[7.1]

[4.1]

[5.2]

2.1 Phasenbezogene Aktivitäten

- Erstellung Projektkonzept

Das Projektkonzept beschreibt das geplante Projekt in kurzer Form mit den folgenden Angaben:

- ♦ Ziel und Begründung des Projekts
- ♦ Konsequenzen auf andere Systeme oder betriebliche Abläufe
- ♦ Regulatorisches Umfeld
- ♦ Hauptbeteiligte
- ♦ Lieferantenvorauswahl

[2.2]
[2.3]
[4.2]
[5.2]

- Erstellung Qualitätsplan

Der Qualitätsplan sollte die folgenden Festlegungen dokumentieren und bei Bedarf dem Projektverlauf angepaßt werden (Versionsführung):

- ♦ projektspezifische Phasen des Lebenszyklus und phasenübergreifende Aktivitäten
- ♦ Auflistung der Richtlinien und Arbeitsanweisungen (SOPs) für die Lebenszyklusaktivitäten und die phasenübergreifenden Aktivitäten
- ♦ entstehende Dokumentation
- ♦ entstehende Systemkomponenten (siehe Abschnitt 1.1)
- ♦ Kontrollmaßnahmen und -gremien
- ♦ Projektorganisation mit Verantwortlichkeiten und Zeitplänen

[2.1]
[2.2]
[2.3]
[5.2]

- Erstellung Anwendungsspezifikation

Die Anwendungsspezifikation beschreibt das System aus Sicht der Benutzer. Es sollte für die einzelnen Systemkomponenten (siehe Abschnitt 1.1) so detailliert geschrieben sein, daß daraus die Entwicklungsspezifikation erstellt werden kann.

Die Anwendungsspezifikation sollte von den Anwendern in Zusammenarbeit mit IT-Fachleuten erstellt werden.

Die Anwendungsspezifikation sollte die Grundlage für die Risikoanalyse, die Entwicklungsspezifikation und den Akzeptanztest sein und bereits im Hinblick auf diese Ziele erstellt werden.

[2.2]
[2.3]
[4.2]
[5.2]

- Durchführung *Risikoanalyse*

Die *Risikoanalyse* sollte die direkten und indirekten Auswirkungen des CS auf GMP untersuchen und bewerten. Dabei sollten die Auswirkungen jeder in der Anwendungsspezifikationen festgelegten Funktion im Hinblick auf die Erzielung eines einwandfreien und spezifikationsgerechten Arzneimittels untersucht und bewertet werden.

[2.2]
[2.3]
[4.2]
[5.2]

Zusätzlich sollten in der *Risikoanalyse* alle Daten ermittelt werden, die in Bezug auf GMP als kritisch einzustufen sind. Das sind Daten, die einen Einfluß auf die Qualität des Arzneimittels haben können.

[9.1]

Die *Risikoanalyse* sollte bei den folgenden Aktivitäten berücksichtigt werden:

[7.1]

- bei der Erstellung der Entwicklungsspezifikation
- bei der Erstellung der Testpläne der einzelnen Funktionen (siehe Abschnitt 2.2 „Testen“)
- bei der Entscheidung über eine durchzuführende Revalidierung nach Änderungen

[11]

- Erstellung Entwicklungsspezifikation

Die Entwicklungsspezifikation sollte das System aus Sicht der Systementwickler in seinen Funktionen beschreiben. Es sollte möglich sein, das System ausschließlich unter Verwendung dieser Spezifikation zu erstellen.

[2.2]
[2.3]
[4.2]
[5.2]

Die Entwicklungsspezifikation sollte von IT-Fachleuten auf Basis der Anwendungsspezifikation erstellt werden und so verfaßt werden, daß sie als Grundlage für den Modul- und Integrationstest dienen kann. Eine Rückreferenzierung auf die Anwendungsspezifikation sollte gewährleistet sein.

- Entwicklung Systemkomponenten

Die Systemkomponenten sollten auf Grundlage der Entwicklungsspezifikation entwickelt werden und schrittweise zu einem CS integriert werden. Zur Erreichung einer einheitlichen Vorgehensweise aller beteiligten Entwickler und der damit zu erzielenden sicheren Wartbarkeit eines CS sollten Arbeitsanweisungen für die Gestaltung der Entwicklung und deren strukturierte Dokumentation vorhanden sein (z.B. Coding Standards).

[2.2]
[2.3]
[5.2]

- Erstellung der Handbücher für die Benutzung

Das Benutzerhandbuch sollte die Bedienung aller Funktionen des Systems in einer dem Benutzer verständlichen Weise beschreiben. Es sollte für den Benutzer möglich sein, das System ausschließlich mit Hilfe des Benutzerhandbuches korrekt zu bedienen. Es sollte von IT-Fachleuten in Zusammenarbeit mit den Benutzern erstellt werden.

[2.2]
[2.3]
[5.2]

Das Handbuch für Systemverwalter sollte alle Arbeiten, die für den Betrieb des CS notwendig sind, beschreiben. Die im Handbuch für Systemverwalter beschriebenen Arbeiten sollten im allgemeinen von IT-Fachleuten durchgeführt werden.

- Installation und Inbetriebnahme

Für die Installation und Inbetriebnahme sollten die folgenden Anweisungen vorliegen:

[2.2]
[2.3]
[5.2]

- ♦ Installationsplan
- ♦ Schulungsplan (siehe auch Abschnitt 1.3)
- ♦ Inbetriebnahmeplan

Nach der Installation sollte deren korrekte Durchführung gemäß Installationsplan überprüft werden (IQ, Installation Qualification). Die Umgebungsbedingungen für das CS sollten beschrieben sein. Maßnahmen gegen Feuer-, Wasser-, Staub-, mechanische, elektrische und magnetische Einflüsse sollten festgelegt sein.

[3.1]

Sofern für die Betriebssysteme des vorliegenden CS die Existenz von Viren bekannt ist, sollten die Datenträger vor der Installation auf Viren geprüft werden.

- Akzeptanztestplanung und -durchführung

Siehe "Planung und Durchführung von Tests" im Abschnitt 2.2.

[2.2]
[2.3]
[5.2]
[7.1]

- Freigabe

Ein CS kann formal zur Benutzung freigegeben werden, wenn der Qualitätsplan vollständig und korrekt abgearbeitet wurde und die definierten Ergebnisse erzielt wurden. Dies sollte durch einen abschließenden Review geprüft werden. [2.2]
[2.3]
[5.2]

Wenn das CS in unkritischen Punkten (siehe "Risikoanalyse") nicht den Spezifikationen entspricht, so sollte eine Benutzung unter Hinweis auf diese Punkte und ggf. durch Einführung organisatorischer Umgehungsmaßnahmen dennoch ermöglicht werden.

Ein Parallelbetrieb des CS zu einem vorher angewendeten manuellen System sollte erwogen werden, wenn bei Einsatz einer neuen Technologie trotz ordnungsgemäßer Entwicklung nach dem Lebenszyklusmodell ein nennenswertes Restrisiko verbleibt. [2.1]
[7.2]

- Betrieb

- Änderungskontrolle

Änderungen sind von den im Qualitätsplan festgelegten Verantwortlichen zu genehmigen. [11]

Bei Änderungen an einem CS sollte seinem im Qualitätsplan definierten Lebenszyklus gefolgt werden. Für jede Änderung sollten die Eintrittsphase in den Lebenszyklus und die Austrittsphase aus dem Lebenszyklus definiert werden. Die Eintritts- und die Austrittsphase sowie alle dazwischenliegenden Phasen werden dann bei der Änderung gemäß den dafür im Qualitätsplan festgelegten Arbeitsanweisungen durchlaufen. Damit ist das Verfahren für die Änderung vorgegeben. [2.2]
[2.3]

Die Entscheidung über eine Revalidierung des Gesamtsystems nach einer Änderung sollte in jedem Einzelfall und in Abhängigkeit der Komplexität des CS und des Gewichts der Änderungen bezüglich GMP-Relevanz geprüft werden. Als Grundlage für die Entscheidung sollte die *Risikoanalyse* dienen.

<ul style="list-style-type: none">◆ Systemüberwachung und -wartung <p>Die korrekte Funktion des CS einschließlich Peripherie sollte nach einem festgelegten Plan kontinuierlich überwacht und in Logbüchern dokumentiert werden. Die Logbücher sollten als Bestandteil der Lebenszyklusdokumentation archiviert werden.</p> <p>Zur Aufrechterhaltung des Systembetriebes sollten vorbeugende Wartungsmaßnahmen beschrieben sein, die auf die spezifischen Ursachen möglicher Systemausfälle abgestimmt sind. Zu Maßnahmen für das verbleibende Restrisiko eines Systemausfalls siehe Abschnitt 6.</p>	[16]
<ul style="list-style-type: none">◆ Fehlerbehandlung <p>Zur Fehlerbehandlung siehe Abschnitt 6. Wenn die Fehlerbehebung zu einer Änderung des CS führt, ist wie unter "Änderungskontrolle" beschrieben zu verfahren.</p>	[15-17] [11]
<ul style="list-style-type: none">• Stilllegung <p>Die Stilllegung ist der formale Akt der Außerbetriebnahme eines Systems. Damit endet der Lebenszyklus. Vor der Stilllegung sollten die Auswirkungen auf bestehende Systeme und Datenbestände untersucht werden.</p> <p>Die Aufbewahrungsdauer der Dokumentation und der Daten sollte sich nach der jeweils gültigen Aufbewahrungsdauer der Herstdokumentation für die letzte vom System beeinflusste Fertigarzneimittelcharge richten.</p>	[2.2] [2.3]

2.2 Phasenübergreifende Aktivitäten

- Planung und Durchführung von Tests

Die folgenden Tests sollten geplant und durchgeführt werden:

[2.3]

Beim Modultest werden Systemkomponenten einzeln auf ihre Funktionalität gegen die Entwicklungsspezifikation geprüft.

[5.2]

[7.1]

Beim Integrationstest werden die Schnittstellen zwischen den Systemkomponenten gegen die Entwicklungsspezifikation getestet.

Beim Systemtest in der Entwicklungsumgebung wird das Zusammenwirken aller Systemkomponenten gegen die Entwicklungsspezifikation und ggf. auch gegen die Anwendungsspezifikation getestet.

Beim Systemtest in der Anwendungsumgebung (Akzeptanztest) wird das ablauffähige CS gegen die Anwendungsspezifikation und ggf. gegen die Entwicklungsspezifikation getestet.

Als *Testmethoden* sollten *Black-Box-Test*, *White-Box-Test* oder eine Kombination aus beiden Methoden in Betracht gezogen werden. Dazu sollte ein Testplan mit folgenden Punkten erstellt werden:

- ♦ Beschreibung der Testumgebung mit Bezeichnung und Version der Hard- und Software
- ♦ Benennung eines Testteams
- ♦ Beschreibung aller durchzuführenden Tests nach folgendem Schema:

Testziel 1

 Testfall 1

 Testvorschrift 1

 Testvoraussetzungen 1

 Testdaten 1

 erwartete Ergebnisse bzw. Akzeptanzkriterien 1

 Beschreibung der Ausführung 1

 Art der Protokollierung 1

 ...

 Testvorschrift n

 Testfall m

 ...

Testziel j

Die Testziele beschreiben verbal, was zu überprüfen ist und leiten sich aus den Spezifikationen des CS ab. Die Tiefe der Überprüfungen sollte sich aus der Risikoanalyse ableiten (siehe Abschnitt

2.1 „Risikoanalyse“).

Die zugehörigen Testfälle sind detailliertere verbale Beschreibungen des Testziels, sie sollten so beschrieben sein, daß sich daraus unmittelbar Testvorschriften herleiten lassen.

Testvorschrift:

Die Testvoraussetzungen für die Durchführung sollten bestimmt werden, ebenso wie die Testdaten, mit denen das Testobjekt ausgeführt wird.

Die erwarteten Ergebnisse bzw. Akzeptanzkriterien stellen die Daten oder Zustände dar, die laut Spezifikation mit den Testdaten erhalten werden sollen.

Unter Beschreibung der Ausführung werden die Aktionen nachvollziehbar beschrieben, die zu den Testergebnissen führen.

Die Art der Protokollierung gibt an, wie die Testausführung dokumentiert wird. Die Dokumentation sollte so erfolgen, daß der gesamte Testablauf durch einen sachkundigen Dritten nachvollzogen werden kann.

Zur Testauswertung werden die dokumentierten Testergebnisse mit den erwarteten Ergebnissen bzw. Akzeptanzkriterien verglichen. Die Tests sind abgeschlossen, wenn die hinreichende Erfüllung aller Akzeptanzkriterien bestätigt ist (siehe auch "Freigabe" in Abschnitt 2.1).

Die hier verwendete einheitliche Bezeichnung "Testen" schließt die im angelsächsischen Sprachgebrauch OQ (Operational Qualification) und PQ (Performance Qualification) ein.

• Konfigurationskontrolle

Es sollte ein Konfigurationsplan erstellt werden, der folgendes beschreibt:

- eine Nomenklatur für die Versionen der Systemkomponenten und Dokumente
- alle Systemkomponenten und Dokumente mit deren Versionen und Einsatzperioden
- die zu verwendenden Werkzeuge und Prozeduren, die diese Systemkomponenten in den gewünschten Versionen zum ablauffähigen CS integrieren

[4.1]
[5.2]

- Planung und Durchführung von Audits

Die Entwicklung und der Betrieb eines CS sollte periodisch einem Audit unterworfen werden. Dabei sollten die im Qualitätsplan festgelegten Aktivitäten und Dokumente stichprobenartig gegen die entsprechenden Arbeitsanweisungen geprüft werden. Die Beseitigung festgestellter Mängel sollte überwacht werden.

[5.2]

- Planung und Durchführung von *Reviews*

Form und Inhalt aller erstellten Systemkomponenten und Dokumente sollten einem *Review* durch eine weitere sachkundige Person unterzogen werden (Vier-Augen-Prinzip). Die Kriterien, gegen die geprüft wird, sollten schriftlich formuliert werden.

[5.2]

[7.1]

Für die in der *Risikoanalyse* als GMP-relevant festgestellten Funktionen sollte ein *Review* der Software (*Source-Code-Review*) durchgeführt werden.

2.3 Prospektive und Retrospektive *Validierung*

- Prospektive *Validierung*

Ein CS gilt als prospektiv validiert, wenn es formal und inhaltlich nach den Grundsätzen des Lebenszyklusmodells entwickelt wurde und betrieben wird (siehe Abschnitte 2.1 und 2.2). [2.1]
[2.2]
[2.3]

- Retrospektive *Validierung*

Für bestehende Systeme, die nicht oder nicht vollständig nach den Grundsätzen des Lebenszyklusmodells erstellt worden sind, sollte das folgende Verfahren einer retrospektiven *Validierung* angewandt werden: [2.1]
[2.2]
[2.3]

- ♦ Anfertigung eines Erfahrungsberichtes über den bisherigen Betrieb des CS
- ♦ Beurteilung der Vollständigkeit der Dokumentation gegen den Lebenszyklus sowie Beurteilung der Qualität der Dokumentation (dazu ist ggf. ein Audit beim Hersteller erforderlich)
- ♦ Durchführung einer *Risikoanalyse* zur Ermittlung der GMP-relevanten Systemteile
- ♦ Erstellung des Qualitätsplans mit Aktivitäten und Verantwortlichkeiten
- ♦ Erstellung/Überarbeitung der Dokumentation, die als Basis für die Tests des CS dienen soll
- ♦ Testen der in der *Risikoanalyse* als GMP-relevant ermittelten Teile des CS [7.1]
- ♦ Freigabe des CS mit ggf. zusätzlich notwendigen organisatorischen QS-Maßnahmen
- ♦ Einführung aller am existierenden System anwendbaren phasenübergreifenden Aktivitäten/Festlegungen wie beim Lebenszyklusmodell (siehe Abschnitt 2.2)
- ♦ Einfrieren des erreichten Systemzustandes oder Weiterentwicklung gemäß Lebenszyklus

3 Zugriffsautorisierung

Jeder Benutzer sollte nur die entsprechend seiner Aufgabenstellung und Ausbildung notwendigen Rechte zur Eingabe, Löschung oder Änderung von Daten erhalten. Die Verfahren zur Vergabe dieser Rechte sollten festgelegt sein. [8.1]
[8.3]
[10.2]

Geeignete Maßnahmen zum Schutz vor unerlaubter Dateneingabe, -änderung und -löschung sind die Identifizierung des Benutzers in Verbindung mit einer Authentisierung. Dies kann zum Beispiel durch physikalische Methoden wie die Vergabe von Schlüsseln und Kennkarten oder durch persönliche Codes sowie zusätzlich durch die Beschränkung des Zugangs zu Computerterminals erfolgen. [8.2]

Für diese Methoden sollte festgelegt sein: [8.3]

- das Einzugsverfahren
- der Ersatz bei Beschädigung oder Verlust
- das Verhalten, wenn der persönliche Code nicht mehr verfügbar ist
- das Führen einer Verteilerliste

Die Regeln zur Erzeugung der persönlichen Codes sollten die folgenden Angaben enthalten: [8.3]

- Länge
- Verwendung von Sonderzeichen und Zeichenkombinationen
- Gültigkeitsdauer
- Historie
- Verbotliste

Der Zugriff auf firmeninterne computergestützte Systeme durch nicht autorisierte, externe Personen über Datenübertragungsleitungen und Netze sollte ausgeschlossen werden.

Zugangsversuche von nicht ermächtigten Personen sollten erfaßt werden. Dabei sollte festgehalten werden, zu welchem Zeitpunkt und über welche Zugangsmöglichkeit der mißlungene Zugangsversuch erfolgte. Die so anfallenden Daten sollten regelmäßig überprüft werden. [8.4]

4 Dateneingabe

- Plausibilitätskontrollen

Soweit technisch möglich, sollte das System bei der Eingabe und Bearbeitung von Daten Plausibilitätskontrollen durchführen. Durch systemseitigen Vergleich der Eingabedaten gegen vordefinierte Grenzen sollte der Benutzer bereits bei der Eingabe der Daten auf mögliche Fehler hingewiesen werden. Hierbei sollte kein Unterschied zwischen manueller Eingabe durch den Benutzer und Datenübernahme von einem anderen System bestehen.

[6.1]

[9.2]

In gleicher Weise sollten Verarbeitungsoperationen, die das System durchführt, durch das System selbst überprüft werden.

- Kritische Daten

Kritische Daten sollten im Rahmen der *Risikoanalyse* festgelegt werden (siehe Abschnitt 2.1 „*Risikoanalyse*“). Als kritische Daten sollten alle für die Produktqualität relevanten Daten angesehen werden.

[9.1]

Die Eingabe kritischer Daten und ihre Bestätigung sollte mit den folgenden Angaben protokolliert werden

- Datum
- Uhrzeit
- Benutzeridentifikation
- Art der Aktion

Die Änderung solcher Daten sollte, ebenso wie der Grund und die Genehmigung der Änderung, durch eine zweite Person mit den o.a. Angaben im CS protokolliert werden (Audit Trail). Dieses Protokoll sollte in regelmäßigen Abständen überprüft werden.

[10]

Die manuelle Eingabe kritischer Daten sollte durch den Einsatz automatischer Erfassungssysteme auf ein Minimum beschränkt sein (z.B. Eingabe einer Chargennummer über Barcode; Eingabe eines Substanzgewichts durch Übernahme des Waagensignals). Die Kontrolle kritischer Daten sollte durch das System bzw. eine entsprechende Systemumgebung erfolgen.

[9.2]

- Chargenfreigabe

Wenn die Freigabe von Chargen zum Inverkehrbringen computer-gestützt erfolgt, sollte das System sicherstellen, daß nur befugte Personen Chargen freigeben dürfen. Die dafür erforderliche eindeutige Autorisierung sollte mit einem der folgenden Verfahren durchgeführt werden:

[19]

- mit einer Kombination eines physikalischen Schlüssels (z.B. Chipkarte, "echter" Schlüssel) und eines Software-Schlüssels (persönlicher Code oder anderen Verfahren zur eindeutigen Identifizierung)
- durch eine zur Zugangsberechtigung (siehe Abschnitt 3) zusätzliche Identifikation mit einem weiteren Software-Schlüssel, der bei jeder Chargenfreigabe einzugeben ist.

Alle zur Autorisierung angewendeten Verfahren, insbesondere auch Regelungen für den Vertretungsfall, sollten festgelegt sein.

Nach einer Chargenfreigabe sollten Änderungen an den gespeicherten Daten nur noch durch den Freigebenden und eine festgelegte zweite Person möglich sein. Die ursprünglichen Daten müssen im System nachvollziehbar dokumentiert werden.

5 Datenablage und Datensicherung

- Datenablage

Im Falle elektronischer Speicherung sollte zusätzlich zu den Daten auch die Information abgelegt werden, in welchem Format sie gespeichert wurden. Ein lauffähiges Druckprogramm zur Erzeugung aussagekräftiger Ausdrücke sollte zu jedem in der elektronischen Datenablage vorhandenen Format verfügbar sein. [12.1]

Vor jedem Austausch von Hardware und/oder Software sollte durch Anwendung der Änderungskontrolle sichergestellt werden, daß die betroffenen Daten auch in der neuen Konfiguration ausgedruckt werden können. [13.3]

Sollte ein notwendiger Wechsel von Hardware und/oder Software dazu führen, daß gespeicherte Daten in der neuen Systemkonfiguration nicht mehr gedruckt werden können, so sollte eines der folgenden Verfahren angewendet werden:

- der Datenbestand wird in Formate konvertiert, die in der neuen Systemkonfiguration ausgedruckt werden können
- die zum Ausdruck benötigten Komponenten der alten Hardware und/oder Software-Konfiguration werden konserviert. In diesem Falle sollte auch für den Ausfall des konservierten Systems die Verfügbarkeit eines geeigneten Ersatzsystems sichergestellt sein
- die Konvertierung in ein anderes Medium wird durchgeführt

Die elektronisch gespeicherten Daten sollten regelmäßig auf ihre Verfügbarkeit und Integrität geprüft werden. [13.2]

- Datensicherung

Um die Verfügbarkeit der gespeicherten Daten sicherzustellen, sollten regelmäßig Sicherungskopien derjenigen Daten angefertigt werden, die zur Rekonstruktion der GMP-Dokumentation erforderlich sind. Dies sollte auch für die benötigten Systemprogramme zur Rückspeicherung und Lesbarmachung gelten. [14.1]

Die Sicherungsprozedur muß die Integrität der Daten gewährleisten. Jede Datensicherung sollte auf fehlerfreie Durchführung kontrolliert werden.

Es sollten mindestens zwei Generationen von Sicherungskopien aufbewahrt werden. Die Sicherungskopien sollten durch ein geeignetes System verwaltet werden, um die Verfügbarkeit der Daten in einem angemessenen Zeitrahmen sicherzustellen. Häufigkeit und Umfang der Sicherungen sollten sich am Aufwand der Wiederbeschaffung orientieren. Dies sollte bereits in der Spezifikation des CS definiert werden.

[14.1]

Daten, die nicht wiederbeschafft werden können, sollten während des Betriebes des CS gleichzeitig auf zwei Speichermedien gespeichert werden.

Die Sicherungskopien sollten an einem Ort aufbewahrt werden, der in einem vom CS gesonderten Brandschutzabschnitt liegt. Dieser Ort sollte bezüglich der Sicherheit mindestens die Zugangsanforderungen erfüllen, die für das CS beschrieben wurden. Umgebungsanforderungen für eine sachgemäße Lagerung der Speichermedien sollten berücksichtigt werden. Vor Ablauf der für das Medium zu erwartenden Verfallzeit der Daten sollten diese umkopiert werden.

[13.1]
[14.2]

Die Sicherungskopien werden so lange aufbewahrt wie die Originaldaten.

Nach Systemänderungen sollte im Rahmen der Änderungskontrolle die *Verfügbarkeit* und *Integrität* der Daten auf den Sicherungskopien sichergestellt werden. Dies sollte durch Rückspeicherung von Probedaten überprüft werden.

6 Fehlerbehandlung und Systemausfall

Ein Ausfall des CS ist gekennzeichnet durch Störungen oder Ausfälle in Systemkomponenten, die eine geordnete Nutzung des Systems längerfristig, z.T. auf nicht absehbare Zeit, unmöglich machen. Um auf wichtige Datenbestände auch in solchen Perioden überbrückend zugreifen zu können, sollten Ersatzsysteme oder alternative Verfahren zur Datenpräsentation bereitgehalten werden.

[15-17]

An solche Systeme oder Verfahren sind Anforderungen wie

- Verfügbarkeit
- Praktikabilität
- Angemessenheit
- Wirksamkeit
- Verlässlichkeit
- Vollständigkeit

zu stellen. Diese Anforderungen sollten für jeden Datenbestand entsprechend seiner Bedeutung und Verwendung vorab definiert und daraus die vorzusehenden Ersatzverfahren abgeleitet werden. Dabei sollte der zulässige Zeitaufwand zur Inbetriebnahme des Verfahrens aus den Anforderungen und Erfahrungen der betrieblichen Praxis abgeleitet, festgeschrieben und gegebenenfalls vertraglich vereinbart werden.

Für den Fall eines Systemausfalls sollte ein Verfahren existieren, das die betroffene Hardware oder Software aus jeder Situation wieder in einen funktionierenden, einwandfreien Grundzustand bringt und die zugehörigen Daten zuverlässig rekonstruiert.

Mit wachsender Betriebserfahrung mit einem CS sollten für bekannte, wohldefinierte Fälle von Systemausfällen detaillierte Einzellösungen etabliert werden.

Zur zügigen Behebung oder Vermeidung von Systemfehlern sollten im laufenden Betrieb geeignete Kontrollmaßnahmen vorgesehen werden, um einen sich anbahnenden Ausfall frühzeitig erkennen und dessen Behebung einleiten zu können.

-

Ein Verfahren zur Behebung von Systemfehlern sollte folgende Punkte berücksichtigen:

- Durchführung der Fehleranalyse
- Reparaturbeauftragung und -durchführung
- Zusätzliche organisatorische Maßnahmen (Umgehungslösung)
- Test der Softwarekomponenten
- Überprüfung von gespeicherten Daten
- Rekonstruktion von Daten
- Systemfreigabe zur Wiederverwendung
- Dokumentationsanweisungen

Die Aussagefähigkeit der anzuwendenden Tests und Überprüfungsverfahren sollte nachgewiesen werden.

-

7 Anhang

7.1 Ergänzende Leitlinien für computergestützte Systeme¹

Begriffsbestimmungen

Computergestütztes System:

[0.1] Ein System zur Eingabe, elektronischen Verarbeitung und Ausgabe von Informationen, die entweder zur Dokumentation oder zur automatischen Steuerung verwendet werden.

System:

[0.2] Definiertes Muster von zusammenwirkenden Aktivitäten und Techniken, die so miteinander verknüpft werden, daß sie ein strukturiertes Ganzes bilden.

Grundsätze

[0.3] Die Einführung von computergestützten Systemen in die Herstellung einschließlich Lagerhaltung, Verteilung und Qualitätskontrolle ändert nichts an der Notwendigkeit zur Einhaltung der im Leitfaden einer Guten Herstellungspraxis festgelegten einschlägigen Grundsätze. [0.4] Wenn ein computergestütztes System an die Stelle eines manuellen Vorgangs tritt, dürfen weder die Qualität der Produkte noch die Qualitätssicherung beeinträchtigt werden. [0.5] Die Gefahr, daß durch eine verringerte Beteiligung des Bedienungspersonals bestimmte Gesichtspunkte des früheren Systems verlorengehen, sollte berücksichtigt werden.

Personal

1. [1.1] Es ist von entscheidender Bedeutung, daß das Personal in Schlüsselstellungen sehr eng mit dem an den Computersystemen arbeitenden Personal zusammenarbeitet. [1.2] Personen in verantwortlichen Stellungen sollten in bezug auf die Planung und Verwendung von Computersystemen innerhalb ihres Verantwortungsbereichs angemessen ausgebildet sein. [1.3] Damit sollte auch sichergestellt werden, daß die erforderliche Sachkenntnis für die Beratung vorhanden ist für die Auslegung, Validierung, Installation und den Betrieb von computergestützten Systemen.

Validierung

¹Die Numerierung der Sätze in eckigen Klammern wurde von den Autoren vorgenommen, um eine genauere Referenzierung zu ermöglichen

2. [2.1] Der Umfang der notwendigen Validierung hängt von einer Reihe von Faktoren ab; hierzu gehören der Verwendungszweck des Systems, die Frage, ob es sich um ein prospektives oder retrospektives System handelt und ob neue Elemente eingeführt werden. [2.2] Die Validierung sollte als Teil des gesamten Lebenszyklus eines Computersystems angesehen werden. [2.3] Dieser Zyklus umfaßt die Stadien Planung, Spezifizierung, Programmierung, Prüfung, Inbetriebnahme, Dokumentation, Betrieb, Kontrolle und Änderungen.

System

3. [3.1] Es sollte darauf geachtet werden, daß die Geräte in einer geeigneten Umgebung aufgestellt werden, damit externe Faktoren das System nicht negativ beeinflussen können.
4. [4.1] Eine ausführliche Beschreibung des Systems sollte erstellt (gegebenenfalls mit Diagrammen) und ständig aktualisiert werden. [4.2] Diese Beschreibung sollte Grundsätze, Zielsetzungen, Sicherheitsmaßnahmen und Einsatzbereich des Systems umfassen und aufzeigen, wie der Computer eingesetzt wird und ob Wechselwirkungen mit anderen Systemen und Verfahren bestehen.
5. [5.1] Software ist eine kritische Komponente eines computergestützten Systems. [5.2] Der Benutzer solcher Software sollte alle erforderlichen Maßnahmen treffen, um sicherzustellen, daß sie in Übereinstimmung mit einem Qualitätssicherungssystem erstellt worden ist.
6. [6.1] Das System sollte, soweit erforderlich, Eingabe und Verarbeitung der Daten auf ihre Richtigkeit überprüfen.
7. [7.1] Bevor ein computergestütztes System eingesetzt wird, sollte es gründlich geprüft und für den vorgesehenen Einsatz als geeignet befunden werden. [7.2] Wird ein manuelles System ersetzt, sollten beide Systeme als Teil dieser Prüfung und Validierung über einen bestimmten Zeitraum parallel betrieben werden.
8. [8.1] Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die dazu ermächtigt sind. [8.2] Geeignete Maßnahmen zum Schutz vor unerlaubter Dateneingabe sind die Verwendung von Schlüsseln, Kennkarten, persönlichen Codes sowie die Beschränkung des Zugangs zu Computerterminals. [8.3] In einem Verfahren sollte die Ausgabe, Annullierung und Veränderung der Ermächtigung zur Eingabe und Änderung von Daten einschließlich der Änderung der persönlichen Codes genau festgelegt sein. [8.4] Systeme sollten in Betracht gezogen werden, die Zugangsversuche von nicht ermächtigten Personen dokumentieren.
9. [9.1] Wenn kritische Daten manuell eingegeben werden (z.B. Gewicht und Chargennummer eines Wirkstoffs bei der Dispensation), sollten diese einer zusätzlichen Prüfung auf ihre Richtigkeit unterzogen werden. [9.2] Diese Prüfung könnte durch einen zweiten Bediener oder eine validierte elektronische Methode erfolgen.

10. [10.1] Das System sollte die Identität des Bedieners, der die kritischen Daten eingibt oder bestätigt, prüfen. [10.2] Die Erlaubnis zur Änderung eingegebener Daten sollte auf namentlich festgelegte Personen beschränkt sein. [10.3] Jede Änderung eingegebener Daten sollte eigens genehmigt und zusammen mit dem Grund der Änderung protokolliert werden. [10.4] Hierzu sollte ein System eingesetzt werden, das ein vollständiges Protokoll sämtlicher Eingaben und Änderungen (audit trail) bietet.
11. [11.1] Änderungen an einem System oder einem Computerprogramm sollten nur gemäß einem festgelegten Verfahren durchgeführt werden, das Bestimmungen zur Validierung, Prüfung, Genehmigung und Einführung der Änderung enthält. [11.2] Eine solche Änderung sollte nur mit Zustimmung der Person ausgeführt werden, die für den betreffenden Systemteil verantwortlich ist. [11.3] Diese Änderung sollte dokumentiert werden. [11.4] Jede wesentliche Änderung sollte validiert werden.
12. [12.1] Zu Zwecken der Qualitätsüberprüfung muß es möglich sein, einen aussagekräftigen Ausdruck der elektronisch gespeicherten Daten zu erhalten.
13. [13.1] In Übereinstimmung mit Absatz 4.9. des Leitfadens einer Guten Herstellungspraxis sollten die Daten physisch oder elektronisch gegen absichtliche und unbeabsichtigte Beschädigung gesichert werden. [13.2] Gespeicherte Daten sollten auf ihre Verfügbarkeit, Beständigkeit und Genauigkeit geprüft werden. [13.3] Werden Änderungen an Computer-Geräten oder Programmen vorgeschlagen, sollten die oben genannten Prüfungen so oft durchgeführt werden, wie dies für das eingesetzte Speichermedium angemessen ist.
14. [14.1] Daten sollten durch regelmäßig erstellte Sicherungskopien geschützt werden. [14.2] Diese Sicherungskopien sollten so lange wie nötig an einem gesonderten und sicheren Ort gelagert werden.
15. [15.1] Es sollten geeignete alternative Verfahren für Systeme vorgesehen werden, die bei einem Ausfall eingesetzt werden müssen. [15.2] Der Zeitaufwand der zur Inbetriebnahme diese alternativen Verfahren benötigt wird, sollte der Dringlichkeit ihres Einsatzes angemessen sein. [15.3] Beispielsweise müssen Informationen die für einen Rückruf benötigt werden, kurzfristig verfügbar sein.
16. [16.1] Die im Fall eines Systemfehlers oder -ausfalls anzuwendenden Verfahren sollten festgelegt und validiert werden. [16.2] Sämtliche Fehler und Maßnahmen zu deren Behebung sollten dokumentiert werden.
17. [17.1] Ein Verfahren zur Dokumentation und Analyse von Fehlern und zu deren Behebung sollte bestehen.
18. [18.1] Wenn externe Unternehmen mit Dienstleistungen für die Computer beauftragt werden, sollte eine formelle Vereinbarung geschlossen werden, in der die Verantwortlichkeiten des externen Unternehmens klar festgelegt sind (siehe Kapitel 7).
19. [19.1] Wenn die Freigabe von Chargen zum Inverkehrbringen computergestützt erfolgt, sollte das System erkennen können, daß nur befugte Personen Chargen

-

freigeben dürfen. [19.2] Das System sollte diese Personen eindeutig identifizieren und dokumentieren.

7.2 Glossar

Audit Trail

Systemseitiger Kontrollmechanismus, der es ermöglicht, jede Dateneingabe bzw. Weiterverarbeitung von Daten durch das System auf die Originaldaten zurückzuführen.

CS

Computergestütztes System analog den "Begriffsbestimmungen" des Annex 11.

Review

Vollständige Überprüfung einer Systemkomponente oder eines Dokumentes hinsichtlich Form und Inhalt durch eine weitere sachkundige Person.

Risikoanalyse

Methodische Vorgehensweise, bei der Prozesse, Systeme oder Programme in einem ausreichend hohen Detaillierungsgrad analysiert werden und die dabei entstehenden Untereinheiten hinsichtlich ihrer Ergebnisse und Auswirkungen auf ein (pharmazeutisches) Produkt untersucht werden.

Validierung

Dokumentierte Beweisführung in Übereinstimmung mit den Grundsätzen der Guten Herstellungspraxis, daß Verfahren, Prozesse, Ausrüstungsgegenstände, Materialien, Arbeitsgänge oder Systeme tatsächlich zu den erwarteten Ergebnissen führen.

Testmethoden

Beim Black-Box-Test werden die Testfälle allein aus der Beschreibung des Testobjekts abgeleitet, die innere Struktur des Objekts bleibt damit bei der Testplanerstellung unberücksichtigt.

Beim White-Box-Test werden die Testfälle allein aus der Struktur des Testobjekts abgeleitet.

Beim Source-Code Review wird der Source Code von einem oder mehreren Experten gegen die systembeschreibenden Dokumente intellektuell überprüft.

Sicherheit

Sicherheit von CS ergibt sich aus der Vertraulichkeit, der Integrität und der Verfügbarkeit des Systems.

Integrität

Schutz vor unbefugter Änderung von Information

Verfügbarkeit

Schutz vor unbefugter Zurückhaltung von Information

7.3 Literatur

Zur Erstellung dieser APV-Richtlinie wurden die Erfahrungen der Fachgruppen-Mitglieder sowie die folgenden Quellen herangezogen:

1. Feiden K. (Hrsg)
Betriebsverordnung für Pharmazeutische Unternehmer
Deutscher Apotheker Verlag, Stuttgart 4.Aufl. 1995
2. Die Regelung der Arzneimittel in der Europäischen Gemeinschaft; Band IV; Leitfaden einer Guten Herstellungspraxis für Arzneimittel; Kommission der Europäischen Gemeinschaften; 1992
bzw.
EU Leitfaden einer Guten Herstellungspraxis für Arzneimittel (III/2244/87 Rev 3, Jan 1989)
in: Auterhoff G. (Hrsg)
EG-Leitfaden einer Guten Herstellungspraxis für Arzneimittel
2. Aufl. , Editio Cantor Aulendorf 1993
3. EC-Commission
Working Party on "Control of Medicines and Inspections"
Supplementary guidelines for computerized systems
(III/8263/89-EN) Final Draft 1991 (Part of Guide to GMP)
4. Leitfaden einer Guten Herstellungspraxis der PIC
Bekanntmachung von ergänzenden Leitlinien zum Leitfaden der Guten Herstellungspraxis der Pharmazeutischen Inspektions Convention:
Ergänzende Leitlinien für computergestützte Systeme
BAnz Nr 18, S 466 v. 28.1.92
5. ISO 9000 Teil 3
Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung, Lieferung und Wartung von Software, Beuth Verlag, Berlin 1992
6. DGQ-NTG Schrift Nr. 12-51
Software-Qualitätssicherung
Beuth Verlag, Berlin, Köln 1986
7. DGQ-ITG Schrift Nr. 12-52
Methoden und Verfahren der Software-Qualitätssicherung
Beuth Verlag, Berlin 1992
8. Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC); Vorläufige Form der harmonisierten Kriterien; Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften; 1991

9. UK Pharmaceutical Industry Computer Systems Validation Forum
Good Automated Manufacturing Practices
Supplier Guide for Validation of Automated Systems in Pharmaceutical
Manufacture, 2nd Draft January 1995
10. Therapeutic Goods Administration
Use of Computers
Australian Code of GMP for Therapeutic Goods - Medicinal Products -
Part 1, Section 9, January 1993
11. Matsuda T.
Guideline on Control of Computerized Systems in Drug Manufacturing
J Pharm Sci & Technol 48, 11 (1994)
12. FDA
Code of Federal Regulations CFR21
April 1988
13. FDA
Guide to Inspection of computerized systems in drug processing ("blue
book")
Reference Materials and Training Aids for Investigators
US Dept. of Health and Human Services, FDA, Feb. 1983
14. FDA
Draft Guide to the Inspection of Software Development Activities
Reference Materials and Training Aids for Investigators
US Dept. of Health and Human Services, FDA, 1987
15. FDA: COMPLIANCE POLICY GUIDE 7132a07
Computerized drug processing -- input/output checking
National Technical Information Service, Springfield, 1988
16. FDA: COMPLIANCE POLICY GUIDE 7132a08
Computerized drug processing -- i.d. of "persons"
National Technical Information Service, Springfield, 1988
17. FDA: COMPLIANCE POLICY GUIDE 7132a11
cGMP applicability to hardware and software
National Technical Information Service, Springfield, 1988
18. FDA: COMPLIANCE POLICY GUIDE 7132a12
Computerized Drug Processing; Vendor Responsibility
National Technical Information Service, Springfield, 1988

19. FDA: COMPLIANCE POLICY GUIDE 7132a15
Source code for process control application programs
National Technical Information Service, Springfield, 1988