

Anlage 2 zur Bekanntmachung des Bundesministeriums für Gesundheit
zu § 2 Nummer 3 der Arzneimittel- und Wirkstoffherstellungsverordnung
vom 8. August 2011 (BAnz Nr. 125, S. 2901-2906)

Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis

Computergestützte Systeme

Rechtsgrundlage zur Veröffentlichung dieses Leitfadens:

Artikel 47 der Richtlinie 2001/83/EG zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel und Artikel 51 der Richtlinie 2001/82/EG zur Schaffung eines Gemeinschaftskodexes für Tierarzneimittel. Dieses Dokument bietet eine Anleitung für die Auslegung der Grundsätze und Leitlinien der Guten Herstellungspraxis (GMP) für Arzneimittel entsprechend der Richtlinie 2003/94/EG für Humanarzneimittel und der Richtlinie 91/412/EWG für Tierarzneimittel.

Status des Dokuments: Revision 1

Grund der Änderung: Der Anhang wurde als Reaktion auf den verstärkten Einsatz computergestützter Systeme und die zunehmende Komplexität dieser Systeme überarbeitet. In der Folge wurden auch für Kapitel 4 des GMP-Leitfadens Änderungen vorgeschlagen.

Termin des Inkrafttretens: 30. Juni 2011

Grundsätze

Der vorliegende Anhang gilt für alle Arten computergestützter Systeme, die als Bestandteil von GMP-pflichtigen Vorgängen eingesetzt werden. Ein computergestütztes System ist eine Kombination aus Software- und Hardwarekomponenten, die zusammen bestimmte Funktionen erfüllen.

Die Anwendung sollte validiert, die IT Infrastruktur sollte qualifiziert sein.

Wird eine manuelle Tätigkeit durch ein computergestütztes System ersetzt, darf es in der Folge nicht zu einer Beeinträchtigung der Produktqualität, der Prozesskontrolle oder der Qualitätssicherung kommen. Dabei darf sich das Gesamtrisiko des Prozesses nicht erhöhen.

Allgemeines

1. *Risikomanagement*

Ein Risikomanagement sollte über den gesamten Lebenszyklus des computergestützten Systems unter Berücksichtigung von Patientensicherheit, Datenintegrität und Produktqualität betrieben werden. Als Teil eines Risikomanagementsystems sollten Entscheidungen über den Umfang der Validierung und die Sicherstellung der Datenintegrität auf einer begründeten und dokumentierten Risikobewertung des computergestützten Systems basieren.

2. *Personal*

Es sollte eine enge Zusammenarbeit zwischen maßgeblichen Personen, wie z.B. Prozesseignern, Systemeignern und Sachkundigen Personen sowie der IT stattfinden. Alle Personen sollten über eine geeignete Ausbildung und Zugriffsrechte sowie festgelegte Verantwortlichkeiten zur Wahrnehmung der ihnen übertragenen Aufgaben verfügen.

3. *Lieferanten und Dienstleister*

3.1 Werden Dritte (z.B. Lieferanten, Dienstleister) herangezogen, um z.B. ein computergestütztes System bereitzustellen, zu installieren, zu konfigurieren, zu integrieren, zu validieren, zu warten (z.B. Fernwartung), zu modifizieren oder zu erhalten, Daten zu verarbeiten oder im Zusammenhang stehende Serviceleistungen zu erbringen, müssen formale Vereinbarungen abgeschlossen sein, in denen die Verantwortlichkeiten des Dritten eindeutig beschrieben sind. IT-Abteilungen sollten analog zu Dritten behandelt werden.

3.2 Kompetenz und Zuverlässigkeit des Lieferanten sind Schlüsselfaktoren bei der Auswahl eines Produktes oder eines Dienstleisters. Die Notwendigkeit eines Audits sollte auf einer Risikobewertung basieren.

3.3 Die bei kommerziell erhältlichen Standardprodukten bereitgestellte Dokumentation sollte durch Nutzer im regulierten Umfeld dahingehend überprüft werden, ob die Benutzeranforderungen erfüllt sind.

3.4 Die Informationen zum Qualitätssystem und zu Audits, die Lieferanten oder Entwickler von Software und verwendeten Systemen betreffen, sollten Inspektoren auf Nachfrage zur Verfügung gestellt werden.

Projektphase

4. Validierung

4.1 Die Validierungsdokumentation und -berichte sollten die maßgeblichen Phasen des Lebenszyklus abbilden. Hersteller sollten in der Lage sein, ihre Standards, Pläne, Akzeptanzkriterien, Vorgehensweisen und Aufzeichnungen basierend auf ihrer Risikobewertung zu begründen.

4.2 Die Validierungsdokumentation sollte, sofern zutreffend, Aufzeichnungen im Rahmen der Änderungskontrolle und Berichte über alle während der Validierung beobachteten Abweichungen beinhalten.

4.3 Eine aktuelle Liste aller maßgeblichen Systeme und ihrer GMP-Funktionen (Inventar) sollte zur Verfügung stehen.

Für kritische Systeme sollte eine aktuelle Systembeschreibung vorliegen, welche die technische und logische Anordnung, den Datenfluss sowie Schnittstellen zu anderen Systemen oder Prozessen, sämtliche Hard- und Softwarevoraussetzungen und die Sicherheitsmaßnahmen detailliert wiedergibt.

4.4 Die Benutzeranforderungen sollten die erforderlichen Funktionen des computergestützten Systems beschreiben und auf einer dokumentierten Risikobewertung sowie einer Betrachtung der möglichen Auswirkungen auf das GMP System basieren. Die Benutzeranforderungen sollten über den Lebenszyklus des Systems verfolgbar sein.

4.5 Der Nutzer im regulierten Umfeld sollte alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass das System in Übereinstimmung mit einem geeigneten Qualitätsmanagementsystem entwickelt wurde. Der Lieferant sollte angemessen bewertet werden.

4.6 Für die Validierung maßgeschneiderter Systeme oder für den Kunden spezifisch angepasster computergestützter Systeme sollte ein Verfahren vorliegen, das die formelle Be-

wertung und Berichterstellung zu Qualitäts- und Leistungsmerkmalen während aller Abschnitte des Lebenszyklus des Systems gewährleistet.

4.7 Die Eignung von Testmethoden und Testszenarien sollte nachgewiesen werden. Insbesondere Grenzwerte für System- / Prozessparameter, Datengrenzen und die Fehlerbehandlung sollten betrachtet werden. Für automatisierte Testwerkzeuge und Testumgebungen sollte eine dokumentierte Bewertung ihrer Eignung vorliegen.

4.8 Werden Daten in ein anderes Datenformat oder System überführt, sollte im Rahmen der Validierung geprüft werden, dass der Wert und die Bedeutung der Daten im Rahmen dieses Migrationsprozesses nicht verändert werden.

Betriebsphase

5. *Daten*

Um Risiken zu minimieren sollten computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, geeignete Kontrollmechanismen für die korrekte und sichere Eingabe und Verarbeitung der Daten enthalten.

6. *Prüfung auf Richtigkeit*

Werden kritische Daten manuell eingegeben, sollte die Richtigkeit dieser Dateneingabe durch eine zusätzliche Prüfung abgesichert werden. Diese zusätzliche Prüfung kann durch einen zweiten Anwender oder mit Hilfe einer validierten elektronischen Methode erfolgen. Die Kritikalität und möglichen Folgen fehlerhafter oder inkorrekt eingegebener Daten für das System sollten im Risikomanagement berücksichtigt sein.

7. *Datenspeicherung*

7.1 Daten sollten durch physikalische und elektronische Maßnahmen vor Beschädigung geschützt werden. Die Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten sollten geprüft werden. Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein.

7.2 Es sollten regelmäßige Sicherungskopien aller maßgeblichen Daten erstellt werden. Die Integrität und Richtigkeit der gesicherten Daten sowie die Möglichkeit der Datenwiederherstellung sollten während der Validierung geprüft und regelmäßig überwacht werden.

8. *Ausdrucke*

8.1 Es sollte möglich sein, klar verständliche Kopien von elektronisch gespeicherten Daten zu erhalten.

8.2 Von Protokollen, die zur Chargenfreigabe herangezogen werden, sollten Ausdrucke generiert werden können, die eine Veränderung der Daten nach ihrer Ersteingabe erkennen lassen.

9. *Audit Trails*

Basierend auf einer Risikobewertung sollte erwogen werden, die Aufzeichnung aller GMP-relevanten Änderungen und Löschungen in das System zu integrieren (ein systemgenerierter „Audit Trail“). Bei der Änderung oder Löschung GMP-relevanter Daten sollte der Grund dokumentiert werden. Audit Trails müssen verfügbar sein, in eine allgemein lesbare Form überführt werden können und regelmäßig überprüft werden.

10. *Änderungs- und Konfigurationsmanagement*

Jede Änderung an einem computergestützten System einschließlich der Systemkonfigurationen sollte kontrolliert und nach einem festgelegten Verfahren erfolgen.

11. *Periodische Evaluierung*

Computergestützte Systeme sollten periodisch evaluiert werden, um zu bestätigen, dass sie sich noch im validen Zustand befinden und die GMP-Anforderungen erfüllen. Solche Evaluierungen sollten, sofern sachgerecht, den derzeitigen Funktionsumfang, Abweichungsaufzeichnungen, Vorfälle, Probleme, Aktualisierungen, Leistung, Zuverlässigkeit, Sicherheit und Berichte zum Validierungsstatus umfassen.

12. *Sicherheit*

12.1 Es sollten physikalische und / oder logische Maßnahmen implementiert sein, um den Zugang zu computergestützten Systemen auf autorisierte Personen zu beschränken. Geeignete Maßnahmen zur Vermeidung unerlaubten Systemzugangs können die Verwendung von Schlüsseln, Kennkarten, persönlichen Codes mit Kennworten, biometrische Verfahren sowie den eingeschränkten Zugang zu Computern mit zugehöriger Ausrüstung und Datenspeicherungsbereichen einschließen.

12.2 Der Umfang der Sicherheitsmaßnahmen ist von der Kritikalität des computergestützten Systems abhängig.

12.3 Erteilung, Änderung und Entzug von Zugriffsberechtigungen sollten aufgezeichnet werden.

12.4 Systeme zur Verwaltung von Daten und Dokumenten sollten die Identität des Anwenders, der Daten eingibt, ändert, bestätigt oder löscht, mit Datum und Uhrzeit aufzeichnen.

13. *Vorfallmanagement*

Alle Vorfälle, nicht nur Systemausfälle und Datenfehler, sollten berichtet und bewertet werden. Die Ursache eines kritischen Vorfalls sollte ermittelt werden und die Basis für Korrektur- und Vorbeugemaßnahmen sein.

14. *Elektronische Unterschrift*

Elektronische Aufzeichnungen können elektronisch signiert werden. Von elektronischen Unterschriften wird erwartet, dass sie

- a) im Innenverhältnis eines Unternehmens die gleiche Bedeutung haben wie handschriftliche Signaturen,
- b) dauerhaft mit dem zugehörigen Dokument verbunden sind,
- c) die Angabe des Datums und der Uhrzeit der Signatur beinhalten.

15. *Chargenfreigabe*

Wird ein computergestütztes System zur Aufzeichnung der Chargenzertifizierung und -freigabe eingesetzt, sollte durch das System sichergestellt werden, dass nur Sachkundige Personen die Chargenfreigabe zertifizieren können. Das System sollte diese Personen eindeutig identifizieren und die Identität der zertifizierenden oder freigebenden Person dokumentieren. Eine elektronische Chargenzertifizierung oder -freigabe sollte mittels elektronischer Unterschrift erfolgen.

16. *Kontinuität des Geschäftsbetriebes*

Wenn computergestützte Systeme kritische Prozesse unterstützen, sollten Vorkehrungen getroffen sein, um die fortlaufende Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z.B. durch ein manuelles oder ein alternatives System). Der erforderliche Zeitaufwand zur Inbetriebnahme dieser alternativen Verfahren sollte jeweils für ein bestimmtes System und die unterstützten Prozesse risikoabhängig festgelegt werden. Diese Verfahren sollten angemessen dokumentiert und getestet werden.

17. *Archivierung*

Daten können archiviert werden. Diese Daten sollten auf Verfügbarkeit, Lesbarkeit und Integrität geprüft werden. Sind maßgebliche Änderungen am System erforderlich (z.B. Computer und zugehörige Ausrüstung oder Programme), sollte sichergestellt und getestet werden, ob die Daten weiterhin abrufbar sind.

Glossar

Anwendung: Software, die auf einer definierten Plattform/Hardware installiert ist und spezifische Funktionen bietet.

Dritter: Nicht direkt vom Inhaber der Herstellungs- oder Einfuhrerlaubnis geführte Einrichtung.

IT Infrastruktur: Hardware und Software wie Netzwerksoftware und Betriebssysteme, die für die Funktionsfähigkeit der Anwendung erforderlich sind.

Kommerziell erhältliche Standardsoftware: Software die kommerziell verfügbar ist und deren Eignung für den vorgesehenen Zweck durch ein breites Spektrum von Anwendern belegt ist.

Kundenspezifische / für den Kunden spezifisch angepasste computergestützte Systeme: Ein computergestütztes System angepasst an einen spezifischen Geschäftsprozess.

Lebenszyklus: Alle Phasen der Systemlebensdauer von den initialen Anforderungen bis zur Stilllegung einschließlich Design, Spezifikation, Programmierung, Testung, Installation, Betrieb und Wartung.

Prozesseigner: Die für den Geschäftsprozess verantwortliche Person.

Systemeigner: Die für die Verfügbarkeit und Wartung eines computergestützten Systems und die Sicherheit der auf dem System gespeicherten Daten verantwortliche Person.