Bekanntmachung eines Konsens-Dokuments der Bund-Länder-Arbeitsgruppe Gute Laborpraxis (GLP) zum Thema "Gute Laborpraxis (GLP) und Datenverarbeitung"

Vom 28. Oktober 1996

Durch das Chemikaliengesetz (ChemG) in der Fassung der Bekanntmachung vom 14. März 1990 (BGBl. I S.521) wurden die Grundsätze der Guten Laborpraxis in das deutsche Chemikalienrecht übernommen.
Das vorliegende Konsens-Dokument (Anlage) konkretisiert die Anforderungen an den Prüfungsablauf und den Bericht über die Prüfergebnisse nach Anhang 1 Nr. 8.3 und 9.1 des Chemikaliengesetzes.

Bonn, den 28.Oktober 1996

Bundesministerium
für Umwelt, Naturschutz und Reaktorsicherheit

Im Auftrag
Prof. Dr. S c h l o t t m a n n

GLP Konsensdokument:

Die Anwendung der GLP-Grundsätze auf computergestützte Systeme

Im Laufe der letzten Jahre hat die Verwendung computergestützter Systeme in Prüfeinrichtungen, die Prüfungen von Stoffen oder Zubereitungen zur Bewertung ihrer möglichen Gefahren für Mensch und Umwelt durchführen, stetig zugenommen.
Diese computergestützten Systeme werden dabei zur direkten oder indirekten Datenerfassung, Datenverarbeitung, Berichterstattung und Datenspeicherung sowie zunehmend als integraler Bestandteil automatisierter Geräte verwendet. Wenn solche computergestützten Systeme bei der Durchführung von Prüfungen eingesetzt werden, deren Ergebnisse nach den entsprechenden nationalen Vorschriften einer Bewertungsbehörde im Rahmen eines Zulassungs-, Erlaubnis-, Registrierungs-, Anmelde oder Mitteilungsverfahrens vorzulegen sind, ist es erforderlich, dass sie in Übereinstimmung mit den OECD-Grundsätzen der Guten Laborpraxis (GLP) entwickelt, validiert, betrieben und gewartet werden.

Anwendungsbereich

Alle computergestützten Systeme, die zur Erzeugung, Messung oder Auswertung von Daten eingesetzt werden, die nach entsprechenden nationalen Vorschriften einer Bewertungsbehörde im Rahmen eines Zulassungs-, Erlaubnis-, Registrierungs-, Anmelde- oder Mitteilungsverfahrens vorzulegen sind, sollen in Übereinstimmung mit den GLP-Grundsätzen entwickelt, validiert, betrieben und gewartet werden.
Während der Planung, Durchführung und Berichterstattung von Prüfungen werden computergestützte Systeme möglicherweise für eine Reihe unterschiedlicher Zwecke verwendet. Diese sind beispielsweise die direkte oder indirekte Datenerfassung durch automatisierte Geräte, der Betrieb/die Steuerung automatisierter Ausrüstung und die

Verarbeitung und Speicherung der Daten sowie die Berichterstattung. Unter computergestützten Systemen sind in diesem Zusammenhang sowohl programmierbare analytische Geräte als auch Personal-Computer sowie Laborinformations- und Managementsysteme (LIMS) mit einer Vielzahl von Funktionen zu verstehen.
Die GLP-Grundsätze sind immer anzuwenden, unabhängig davon, wie umfangreich der Computereinsatz ist.

Vorgehensweise

Computergestützte Systeme, die bei der Durchführung von Prüfungen zum Einsatz kommen, deren Ergebnisse einer Bewertungsbehörde im Rahmen eines Zulassungs-, Erlaubnis-, Registrierungs-, Anmelde- oder Mitteilungsverfahrens vorgelegt werden, sollen zweckmäßig konstruiert sein, über eine ausreichende Leistungsfähigkeit verfügen und für ihre beabsichtigte Verwendung geeignet sein. Es sollen geeignete Verfahren zur Überprüfung und Wartung dieser Systeme vorhanden sein, und die Systeme sollen in Übereinstimmung mit den GLP-Grundsätzen entwickelt, validiert und betrieben werden.
Der Nachweis, dass ein computergestütztes System für die beabsichtigte Verwendung geeignet ist, ist von grundlegender Bedeutung und wird als Computer-Validierung bezeichnet. Der Validierungsprozess stellt weitgehend sicher, dass ein computergestütztes System den vorgegebenen Spezifikationen entspricht. Die Validierung soll anhand eines formalen Validierungsplanes durchgeführt werden, bevor das System bei Prüfungen eingesetzt wird.

Die Anwendung der GLP-Grundsätze auf computergestützte Systeme

Die folgenden Erwägungen erleichtern die Anwendung GLP-Grundsätze auf computergestützte Systeme, wie sie oben beschrieben wurden:

1. Verantwortlichkeiten

a) Die Leitung der Prüfeinrichtung trägt die Gesamtverantwortung für die Einhaltung der GLP-Gundsätze. Diese Verantwortung schließt die Benennung und wirkungsvolle Organisation einer ausreichenden Anzahl entsprechend qualifizierten und erfahrenen Personals ebenso ein, wie die Sicherstellung eines angemessenen Standards für Räumlichkeiten, Ausrüstung und Verfahren für die Datenverarbeitung.
   Die Leitung hat sicherzustellen, dass computergestützte Systeme für die beabsichtigte Verwendung geeignet sind. Sie hat allgemeine Leitlinien und Verfahren für den Einsatz von Computern festzulegen, um sicherzustellen, dass Systeme in Übereinstimmung mit den GLP-Grundsätzen entwickelt, validiert, betrieben und gewartet werden. Die Leitung soll auch sicherstellen, dass diese allgemeinen Leitlinien und Verfahren verstanden und befolgt werden und dass ihre Einhaltung wirksam überwacht wird.
   Die Leitung soll ferner Personal benennen, bei dem die jeweilige Verantwortung für die Entwicklung, Validierung, den Betrieb und die Wartung computergestützter Systeme liegt. Dieses Personal soll angemessen qualifiziert sein und über einschlägige Erfahrung und Ausbildung verfügen, um seine Aufgaben in Übereinstimmung mit den GLP-Grundsätzen zu erfüllen.
b) Prüfleiter sind nach den GLP-Grundsätzen für die Gesamtleitung ihrer Prüfungen verantwortlich. Da für viele dieser Prüfungen computergestützte Systeme benutzt werden, ist es wichtig, dass Prüfleiter sich über den Einsatz jedes computergestützten Systems in Prüfungen, die unter ihrer Leitung durchgeführt werden, bewusst sind.

Die Verantwortlichkeit des Prüfleiters für elektronisch und auf Papier aufgezeichnete Daten ist die gleiche. Aus diesem Grund sind nur validierte Systeme bei Prüfungen nach den GLP-Grundsätzen einzusetzen.

c) Personal: Personal, das computergestützte Systeme benutzt, ist verantwortlich dafür, diese Systeme in Übereinstimmung mit den GLP-Grundsätzen zu betreiben. Personal, das computergestützte Systeme entwickelt, validiert, betreibt und wartet, ist dafür verantwortlich, diese Tätigkeiten in Übereinstimmung mit den GLP-Grundsätzen und anerkannten technischen Standards durchzuführen.

d) Die Verantwortlichkeiten der Qualitätssicherung (QS) für computergestützte Systeme sind von der Leitung der Prüfeinrichtung zu definieren und in Leitlinien und Anweisungen schriftlich niederzulegen. Das Qualitätssicherungsprogramm soll Anweisungen und Anleitungen beinhalten, die sicherstellen, dass alle Phasen der Validierung, des Betriebs und der Wartung computergestützter Systeme nach eingeführten Standards durchgeführt werden. Zur Einführung erworbener computergestützter Systeme und für die Eigenentwicklung solcher Systeme sollen ebenfalls Anweisungen und Anleitungen vorhanden sein.
QS-Personal hat die GLP-Konformität computergestützter Systeme zu überwachen und soll in dafür erforderlichen Techniken ausgebildet werden. Es soll mit solchen Systemen genügend vertraut sein, um objektive Aussagen treffen zu können; in bestimmten Fällen kann zusätzlich die Benennung spezialisierter Auditoren erforderlich sein.
Falls Daten in einem computergestützten System gespeichert werden, ist dem QS-Personal zu deren Überprüfung der direkte Lesezugriff auf die Daten zu gewähren.

2. Aus und Fortbildung

Die GLP-Grundsätze fordern, dass eine Prüfeinrichtung über angemessen qualifiziertes und erfahrenes Personal verfügt und dass ein dokumentiertes Aus- und Fortbildungsprogramm existiert, das die Bereiche der aufgabenbezogenen Aus- und Fortbildung und, wo angebracht, die Teilnahme an externen Kursen dokumentiert. Nachweise dieser Ausbildungen sind aufzubewahren.
Die genannten Maßnahmen sind auch auf Personal anzuwenden, das mit computergestützten Systemen arbeitet.

3. Einrichtungen und Ausrüstung

Für die ordnungsgemäße Durchführung von Prüfungen nach den GLP-Grundsätzen sollen geeignete Räumlichkeiten und Ausrüstung vorhanden sein. Für computergestützte Systeme sind eine Reihe spezifischer Aspekte zu berücksichtigen:

a) Einrichtungen
Die Standorte für Computerhardware, periphere Komponenten, Kommunikationsausrüstung und elektronische Speichermedien sind mit besonderer Sorgfalt zu wählen. Extreme Temperaturen und Luftfeuchtigkeit, Staub, elektromagnetische Störungen und die Nähe zu Hochspannungskabeln sind zu vermeiden, wenn die Ausrüstung nicht speziell zum Einsatz unter solchen Bedingungen geeignet ist.
Der Stromversorgung für Computerausrüstung und, wenn deren plötzlicher Ausfall die Ergebnisse der Prüfung beeinträchtigen kann, der Notwendigkeit einer doppelt ausgelegten oder unterbrechungsfreien Stromversorgung für computergestützte Systeme ist ebenfalls Aufmerksamkeit zu widmen.

Es sollen geeignete Einrichtungen für die sichere Aufbewahrung elektronischer Speichermedien vorhanden sein.

b) Ausrüstung

i) Hardware und Software

Ein computergestütztes System ist definiert als eine Kombination von Hardware-Komponenten und zugehöriger Software, die zur Ausführung einer speziellen Funktion oder mehrerer Funktionen entworfen und entsprechend eingerichtet wurden.

Hardware sind die physischen Komponenten eines computergestützten Systems. Die Hardware umfasst den Computer selbst und seine peripheren Komponenten.

Software ist das Programm oder die Programme, die den Betrieb des computergestützten Systems ermöglichen.

Alle GLP-Grundsätze, die für Ausrüstung zutreffen, gelten auch für Hard- und Software.

ii) Kommunikation

Im Zusammenhang mit computergestützten Systemen fällt Kommunikation grundsätzlich in zwei Kategorien: Kommunikation zwischen Computern oder Kommunikation zwischen Computer und peripheren Komponenten.

Alle Kommunikationsverbindungen sind potentielle Fehlerquellen und können zum Verlust oder zur Verfälschung von Daten führen. Geeignete Vorkehrungen für die Sicherheit und Systemintegrität müssen daher in angemessener Weise während der Entwicklung, Validierung, des Betriebs und der Wartung jedes computergestützten Systems getroffen werden.

4. Wartung und Wiederherstellung der Funktion nach Systemausfällen

Alle computergestützten Systeme sind so zu installieren und zu warten, dass die korrekte Funktion dauerhaft gewährleistet wird.

a) Wartung

Sowohl für routinemäßige vorbeugende Wartungsarbeiten als auch zur Behebung von Störungen sollen dokumentierte Verfahren vorhanden sein. Diese Verfahren sollen die Aufgaben und Verantwortlichkeiten des dazu eingesetzten Personals verständlich und detailliert beschreiben. Wenn derartige Wartungsarbeiten Änderungen der Hardware und/oder der Software erforderlich machen, kann es nötig werden, das System erneut zu validieren. Über alle Probleme oder bemerkte Unregelmäßigkeiten, die während des täglichen Betriebs des Systems aufgetreten sind, sowie über die daraufhin durchgeführten Maßnahmen sind Aufzeichnungen anzufertigen und aufzubewahren.

b) Wiederherstellung der Funktion nach Systemausfällen
(Disaster Recovery)

Verfahren sollen vorliegen, die für den Fall des teilweisen oder totalen Ausfalls des computergestützten Systems zu treffende Maßnahmen beschreiben. Diese Maßnahmen können von geplanter Hardware-Redundanz bis zum Rückgriff auf Papierformulare reichen. Ausweichpläne zur Fortsetzung der Prüfung nach Systemausfällen müssen validiert und ausreichend gut dokumentiert sein, die Datenintegrität in allen Phasen sicherstellen und dürfen die Prüfung nicht verfälschen. Personal, das an der Durchführung von Prüfungen nach den GLP-Grundsätzen beteiligt ist, soll diese Ausweichpläne kennen. Die zur Wiederherstellung der Funktion eines ausgefallenen computergestützten Systems erforderlichen Verfahren hängen von der Bedeutung des Systems für die Prüfung ab. Wesentlich ist, dass Sicherungskopien aller eingesetzter Software aufbewahrt werden.

Falls Wiederherstellungsverfahren Änderungen an Hard- und Software zur Folge haben, kann es erforderlich sein, das System erneut zu validieren.

5. Daten

Die GLP-Grundsätze definieren Rohdaten als alle ursprünglichen Laboraufzeichnungen und Unterlagen, einschließlich der Daten, die durch ein Geräteinterface direkt in einen Computer gelangen, die als Ergebnis der ursprünglichen Beobachtungen oder Tätigkeiten bei einer Prüfung anfallen und die zur Rekonstruktion und Bewertung des Abschlußberichtes dieser Prüfung erforderlich sind.
Im Zusammenhang mit computergestützten Systemen, die in Übereinstimmung mit den GLP-Grundsätzen betrieben werden, können Rohdaten in unterschiedlichster Form auftreten, beispielsweise auf elektronischen Speichermedien, als Computer- oder Geräteausdrucke und als Mikrofilm/fiches. Es ist erforderlich, dass Rohdaten für jedes computergestützte System definiert werden.
Wenn computergestützte Systeme zur Rohdatenerfassung und –verarbeitung, Berichterstattung oder Rohdatenspeicherung verwendet werden, soll die Auslegung des Systems stets die Erzeugung und die Aufbewahrung eines vollständigen Audit Trails ermöglichen, um alle Änderungen der Daten zurückverfolgen zu können, ohne die Originaldaten unkenntlich zu machen. Durch die Verwendung von mit Datum und Uhrzeit versehenen (elektronischen) Unterschriften soll es möglich sein, alle Datenänderungen auf die Personen zurückzuführen, die diese Änderungen vorgenommen haben. Gründe für die Änderungen sind anzugeben.
Wenn Rohdaten elektronisch gespeichert werden, ist es erforderlich, geeignete Maßnahmen für deren Langzeitaufbewahrung zu treffen, die abhängig von der Art der aufzubewahrenden Daten und der zu erwartenden Nutzungsdauer des computergestützten Systems sind. Der Wechsel der Hard- und Software muss den weiteren Zugriff zu den Rohdaten und deren weitere Aufbewahrung ohne Integritätsrisiken ermöglichen.
Mit der Prüfung zusammenhängende Informationen wie Wartungs- und Kalibrierungsaufzeichnungen, die erforderlich sind, um die Validität der Rohdaten zu belegen oder die Rekonstruktion eines Verfahrens oder einer Prüfung zu ermöglichen, sind in den Archiven aufzubewahren.
Anweisungen für den Betrieb von computergestützten Systemen sollen auch die alternativen Datenerfassungsverfahren beschreiben, die im Falle eines Systemausfalls anzuwenden sind. In solchen Fällen sollen alle manuell aufgezeichneten Daten, die danach in den Computer eingegeben wurden, deutlich als solche gekennzeichnet und als Rohdaten aufbewahrt werden. Manuelle Back-up-Verfahren dienen dazu, das Risiko eines Datenverlusts zu minimieren und stellen sicher, dass diese alternativen Aufzeichnungen aufbewahrt werden.
Wenn die Außerbetriebnahme eines Systems die Übernahme elektronischer Rohdaten in ein Nachfolgesystem erforderlich macht, muss das Übernahmeverfahren ausreichend dokumentiert und seine Integrität überprüft sein. Wenn eine Übernahme in das Nachfolgesystem nicht praktikabel ist, müssen die Rohdaten auf ein anderes Medium übertragen werden und es muss verifiziert werden, dass es sich um eine exakte Kopie handelt, bevor die elektronische Originalaufzeichnung vernichtet werden darf.

6. Sicherheit

Dokumentierte Verfahren für die Sicherheit und den Schutz von Hardware, Software und Daten vor Verfälschung, unbefugter Änderung oder Verlust sollen vorhanden sein. Der Begriff Sicherheit schließt in diesem Zusammenhang die Verhinderung des unbefugten Zugriffs oder von Änderungen am computergestützten System ebenso ein, wie an den im System geführten Daten. Die Gefahr der Verfälschung der Daten durch Viren oder sonstige Störfaktoren ist ebenfalls zu berücksichtigen. Zur Sicherung der Datenintegrität für den Fall kurz- oder langzeitiger Systemausfälle sind gleichfalls Sicherheitsmaßnahmen zu treffen.

a) Physische Sicherheit
   Zur Beschränkung des Zugangs zu Computerhardware, Kommunikationsausrüstung, peripheren Komponenten und elektronischen Speichermedien auf befugtes Personal sind physische Sicherheitsmaßnahmen zu treffen. Für Geräte, die nicht innerhalb spezieller „Computerräume“ aufgestellt sind (beispielsweise Personal-Computer und Terminals), ist es mindestens erforderlich, die in Prüfeinrichtungen üblichen Zugangsbeschränkungen einzuhalten. Wenn solche Ausrüstung außerhalb der Prüfeinrichtung betrieben wird (beispielsweise tragbare Geräte und Geräte mit Modemverbindung zum lokalen computergestützten System), sind zusätzliche Sicherheitsmaßnahmen erforderlich.
b) Logische Sicherheit
   Für jedes computergestützte System oder jede Anwendung müssen logische Sicherheitsvorkehrungen vorhanden sein, die sowohl seine Bedienung als auch den Zugriff auf Anwendungen und Daten durch Unbefugte verhindern. Es ist erforderlich, sicherzustellen, dass nur genehmigte Programmversionen und validierte Software verwendet werden. Logische Sicherheitsmaßnahmen sind beispielsweise die Eingabe einer eindeutigen Benutzerkennzeichnung, verbunden mit einem Passwort. Die Übernahme von Daten oder Software aus externen Quellen ist zu überwachen. Diese Überwachungsmaßnahmen können durch das Computer-Betriebssystem, durch spezielle Sicherheitsroutinen, durch Routineverfahren, die die Anwendungen bereitstellen oder durch eine Kombination dieser Möglichkeiten realisiert sein.
c) Datenintegrität
   Da die Bewahrung der Datenintegrität ein Hauptanliegen der GLP-Grundsätze ist, ist es wichtig, dass jeder, in dessen Arbeitsbereich ein computergestütztes System betrieben wird, sich der Notwendigkeit der oben genannten Sicherheitserwägungen bewusst ist. Die Leitung der Prüfeinrichtung hat sicherzustellen, dass sich das Personal über die Bedeutung der Datensicherheit, der zur Gewährleistung der Systemsicherheit entwickelten und durch das System unterstützten Verfahren sowie der Auswirkungen von Verstößen gegen die Sicherheitsmaßnahmen bewusst ist. Vom System unterstützte Verfahren können beispielsweise eine routinemäßige Systemzugangskontrolle, Dateiüberprüfungsroutinen und die Protokollierung von unplausiblen Werten und/oder des langfristigen Trends einschließen.
d) Datensicherung (Back-up)
   Bei der Verwendung computergestützter Systeme ist es gängige Praxis, Back-up-Kopien der Software und der Daten anzufertigen, um das System im Falle einer Fehlfunktion, die seine Integrität beeinträchtigt, wie z. B. Plattendefekte, wiederherstellen zu können. Dadurch würde die Datensicherungskopie selbst zum Rohdatum und muss deshalb als solche behandelt werden.

7. Validierung computergestützter Systeme

Computergestützte Systeme müssen für die beabsichtigte Verwendung geeignet sein. Die folgenden Gesichtspunkte sind daher zu berücksichtigen:

a) Akzeptanz
Computergestützte Systeme sind so zu entwerfen, dass sie den GLP-Grundsätzen entsprechen und in einer vorausgeplanten Weise in Betrieb zu nehmen sind. Dazu soll eine ausreichende Dokumentation vorhanden sein, die belegt, dass das System in kontrollierter Weise und vorzugsweise nach anerkannten Qualitäts- und technischen Standards (wie ISO 9001) entwickelt wurde. Ferner ist der Nachweis zu erbringen, dass das System durch die Prüfeinrichtung auf Übereinstimmung mit den Akzeptanzkriterien überprüft wurde, bevor es für Prüfungen nach den GLP-Grundsätzen routinemäßig eingesetzt wird. Der formale Akzeptanztest beinhaltet die Durchführung der erforderlichen Tests nach einem vordefinierten Plan und die Aufbewahrung der Dokumentation sämtlicher Testverfahren, Testdaten, Testergebnisse, einer formalen Zusammenfassung des Tests und der formalen Akzeptanzerklärung.
Im Falle fremdbezogener Systeme verbleibt ein Großteil der während der Entwicklung erstellten Dokumentation wahrscheinlich beim Hersteller. In diesem Fall soll der Nachweis einer formalen Einschätzung der Zuverlässigkeit und/oder einer Überprüfung der Arbeitsweise des Herstellers in der Prüfeinrichtung vorhanden sein.

b) Nachträgliche Evaluierung
Wenn Systeme verwendet werden, bei deren Einführung die Notwendigkeit der Einhaltung der GLP-Grundsätze nicht vorhersehbar war oder nicht im einzelnen beschrieben wurde, soll eine dokumentierte Begründung für den Einsatz des Systems vorhanden sein. Diese soll eine nachträgliche Systemevaluierung einschließen, um dessen Eignung zu belegen.
Die nachträgliche Evaluierung beginnt mit der Zusammenstellung sämtlicher historischer Aufzeichnungen des computergestützten Systems. Diese Aufzeichnungen werden anschließend ausgewertet und ein schriftlicher Bericht angefertigt. Dieser Bewertungsbericht beschreibt, welche Nachweise für die Validität des computergestützten Systems vorhanden sind und welche Maßnahmen noch zusätzlich erforderlich sind, um seine Validität künftig sicherzustellen.

c) Verfahren der kontrollierten Systemänderung
(Change Control)
Das Verfahren der kontrollierten Systemänderung von Hard- und Software (change control) besteht aus der formalen Genehmigung der Durchführung und der Dokumentation jeder Änderung eines computergestützten Systems während seines Einsatzes. Ein Verfahren der kontrollierten Systemänderung ist erforderlich, wenn eine beabsichtigte Änderung des Systems seine Validität beeinflussen könnte. Verfahren der kontrollierten Systemänderung müssen in Kraft gesetzt sein, bevor das computergestützte System für Prüfungen nach den GLP-Grundsätzen benutzt wird.
Das Verfahren soll die Bewertungsmethode beschreiben, mit der der erforderliche Umfang einer erneuten Systemüberprüfung zur Erhaltung der Systemvalidität ermittelt wird. Die für die Entscheidung über die Notwendigkeit eines kontrollierten Systemänderungsverfahrens sowie für die Genehmigung zu dessen Durchführung verantwortlichen Personen sind namentlich zu benennen.
Unabhängig von der Änderungsursache (und ob es sich um ein durch einen externen Hersteller oder ein selbst entwickeltes System handelt) sind ausreichende Informationen ein Teil des Verfahrens der kontrollierten Systemänderung. Das Verfahren der kontrollierten Systemänderung muss die Datenintegrität gewährleisten.

d) Unterstützende Maßnahmen
Es sollen unterstützende Maßnahmen vorhanden sein, die sicherstellen, dass das computergestützte System einwandfrei funktioniert und korrekt benutzt wird, damit es für seine beabsichtigte Verwendung geeignet bleibt. Unterstützende Verfahren können beispielsweise beinhalten: Systemverwaltung, Aus- und Fortbildung, Wartung, technische Unterstützung, Überprüfung und/oder Systemleistungsbeurteilung.
Die Systemleistungsbeurteilung ist die formale Überprüfung eines Systems in regelmäßigen Zeitabständen, um sicherzustellen, dass es die festgelegten Leistungskriterien wie Zuverlässigkeit, Ansprechverhalten, Kapazität erfüllt.

8. Dokumentation

Die nachstehend aufgeführten Punkte sind eine Orientierungshilfe für die Minimaldokumentation über die Entwicklung, Validierung, Betrieb und Wartung computergestützter Systeme.

a) Leitlinien
Es sollen schriftliche Leitlinien der Leitung vorhanden sein, die, unter anderem, Beschaffung, Anforderungen, Konzipierung, Validierung, Test, Installation, Betrieb, Wartung, Personalausstattung, Verfahrens- und Einzelüberprüfung, Überwachung und Außerbetriebnahme von computergestützten Systemen beschreiben.

b) Beschreibung der Anwendungssoftware
Die für alle Anwendungen erforderliche Dokumentation beinhaltet:
- Den Namen der Anwendungssoftware oder ihren Identifikationscode und eine detaillierte und verständliche Beschreibung ihres Zwecks.
- Die Hardware (mit Modellnummern), auf der die Anwendungssoftware läuft.
- Das Betriebssystem und andere Systemsoftware (beispielsweise Werkzeuge), die im Zusammenhang mit der Anwendung verwendet wird.
- Die für die Anwendung verwendete (n) Programmiersprache (n) und/oder Datenbankwerkzeuge.
- Die wesentlichen Funktionen der Anwendung
- Eine Übersicht über Datentypen und –fluss und des Datenbankdesigns in Zusammenhang mit der Anwendung.
- Filestrukturen, Fehler- und Alarmmeldungen und Algorithmen, die in Zusammenhang mit der Anwendung stehen.
- Die Komponenten der Anwendungssoftware mit Versionsnummern.
- Konfiguration und Kommunikationsverbindungen zwischen den Anwendungsmodulen und zur Anlage sowie anderen Systemen.

c) Quellcode
Einige OECD-Mitgliedstaaten schreiben vor, dass der Quellcode der Anwendungssoftware in der Prüfeinrichtung verfügbar ist oder durch diese abrufbar sein muss.

d) Standard-Arbeitsanweisungen (SOPs)
Ein Großteil der Dokumentation, die die Benutzung des computergestützten Systems beschreibt, wird in Form von SOPs vorliegen. Diese sollen mindestens folgende Gesichtspunkte abdecken:
- Verfahren zum Betrieb des computergestützten Systems (Hardware/Software) und den Verantwortlichkeiten des betroffenen Personals.

- Verfahren für Sicherheitsmaßnahmen, um unbefugten Zugang und nicht genehmigte Programmänderungen zu bemerken und zu verhindern.
- Verfahren und Befugnis zur Änderung von Programmen und deren Dokumentation.
- Verfahren und Befugnis für Systemänderungen (Hardware/Software) einschließlich gegebenenfalls erforderlicher Tests vor der erneuten Inbetriebnahme.
- Verfahren zur periodischen Überprüfung der korrekten Funktion des gesamten Systems oder einzelner Komponenten und deren Dokumentation.
- Verfahren für Wartungsverfahren computergestützter Systeme und der zugehörigen Ausstattung.
- Verfahren für die Softwareentwicklung und Anweisungen zur Durchführung von Akzeptanztests und deren Dokumentation.
- Back-up-Verfahren für die gespeicherten Daten und Ausweichpläne zur Fortsetzung der Prüfung im Fall von Systemausfällen.
- Verfahren zur Archivierung und Verfahren, um alle Dokumente, Software und elektronisch aufgezeichnete Daten wiederaufzufinden und lesbar zu machen.
- Verfahren für die Überprüfung computergestützter Systeme.

9. Archive

Die GLP-Grundsätze zur Archivierung von Daten müssen einheitlich auf alle Datenarten angewandt werden. Es ist daher erforderlich, dass für die Aufbewahrung elektronischer Daten äquivalente Verfahren für Zugangskontrolle, Indexierung sowie Wiederauffindung und Lesbarmachung nach Ausfällen eingeführt werden ebenso wie andere Daten.
Wenn elektronische Daten aus mehr als einer Prüfung auf einem einzelnen Speichermedium (beispielsweise auf Platte oder Band) gespeichert werden, ist ein detaillierter Index anzulegen. Zur Sicherstellung der Integrität elektronisch gespeicherter Daten kann es erforderlich sein, Räumlichkeiten mit speziellen Systemen zur Aufrechterhaltung bestimmter Lagerbedingungen auszustatten. Falls dafür zusätzliche Archivierungseinrichtungen erforderlich sind, hat die Leitung der Prüfeinrichtung sicherzustellen, dass Personal für die verantwortliche Führung der Archive benannt und der Zugang auf befugtes Personal beschränkt ist. Zusätzlich ist erforderlich, Verfahren einzuführen, die die Langzeitintegrität der elektronisch gespeicherten Daten garantieren. Wenn Probleme mit der Verwendbarkeit der Daten für die Dauer der Aufbewahrung zu erwarten sind oder wenn computergestützte Systeme außer Betrieb gesetzt werden müssen, sollen Verfahren festgelegt werden, die die dauerhafte Verwendbarkeit der Daten sicherstellen. Dabei kann es sich beispielsweise um die Anfertigung von Papierausdrucken oder die Übertragung der Daten in ein anderes System handeln.
Elektronisch gespeicherte Daten dürfen nicht ohne Genehmigung durch die Leitung der Prüfeinrichtung und entsprechende Dokumentation vernichtet werden. Andere Daten, die zusätzliche nützliche oder erläuternde Angaben zum computergestützten System machen, wie Quellcode und Aufzeichnungen zu Entwicklung, Validierung, Betrieb, Wartung und Überwachung, sollen mindestens solange aufbewahrt werden, wie die Aufzeichnung zu Prüfungen, für die das System verwendet wurde.

Begriffsbestimmungen [1])

Akzeptanzkriterien:
Dokumentierte Kriterien, die erfüllt werden müssen, um eine Testphase erfolgreich abzuschließen oder um den Anforderungen für die Auslieferung zu entsprechen.

Akzeptanztest:
Formaler Test des gesamten computergestützten Systems in der voraussichtlichen Systemumgebung zur Feststellung, ob alle Akzeptanzkriterien der Prüfeinrichtung erfüllt wurden und ob das System für den Einsatz geeignet ist.

Anerkannte technische Standards:
Standards, die von nationalen oder internationalen Standardisierungsinstitutionen (ISO, IEEE, ANSI etc.) veröffentlicht wurden.

Computergestütztes System:
Eine Kombination von Hardware-Komponenten und zugehöriger Software, die zur Ausführung einer speziellen Funktion oder mehrerer Funktionen entworfen und entsprechend eingerichtet wurden.

Computer-Validierung:
Der Nachweis, dass ein computergestütztes System für die beabsichtigte Verwendung geeignet ist.

Datensicherung (Back-up):
Vorsorgliche Maßnahmen zur Wiederherstellung von Datenfiles oder Software (Sicherungskopien), zur Wiederaufnahme/Neustart der Datenverarbeitung oder der Benutzung einer Ersatz-Computeranlage nach einer Betriebsstörung oder einem Ausfall des Systems.

Elektronische Unterschrift:
Der Eintrag in Form magnetischer Impulse oder in Form von Kombinationen einer sinnvollen Folge von Zeichen (compilation), die ausgeführt, angepasst oder durch eine Person genehmigt wurde, so dass er der handschriftlichen Unterschrift der Person äquivalent ist.

Hardware:
Die physischen Komponenten eines computergestützten Systems, einschließlich des Computers selbst und seiner peripheren Komponenten.

Periphere Komponenten:
Alle angeschlossenen Geräte oder sonstigen oder externen Komponenten wie Drucker, Modems, Terminals etc.

Quellcode:
Das Original eines Computerprogramms in für den Menschen lesbarer Form (Programmiersprache) formuliert, das in eine maschinenlesbare Form übersetzt werden muss, bevor es durch den Computer ausgeführt werden kann.

[1] Weitere Begriffsbestimmungen sind in den „OECD Grundsätzen der Guten Laborpraxis“ enthalten.

Sicherheit:
Der Schutz der Computerhardware und –software vor unbeabsichtigtem Zugriff, Benutzung, Änderung, Zerstörung oder Offenlegung. Sicherheitsüberlegungen betreffen auch Personal, Daten, Kommunikation sowie den physischen und logischen Schutz der Computerinstallation.

Software (Anwendung):
Ein Programm, das zum Zweck der Steuerung von Prozessen, Datenerfassung, Datenbearbeitung, Berichterstattung und/oder Archivierung der Daten erworben oder entwickelt, angepasst oder nach den Anforderungen der Prüfeinrichtung speziell angefertigt wurde.

Software (Betriebssystem):
Ein Programm oder eine Sammlung von Programmen, Routinen und Subroutinen, die den Betrieb eines Computers steuern. Ein Betriebssystem kann Dienste wie die Zuteilung der Systemressourcen, der Rechenzeit, die Ein-/Ausgabesteuerung und die Datenverwaltung zur Verfügung stellen.

Verfahren der kontrollierten Systemänderung
(Change Control):
Laufende Evaluierung und Dokumentation der Systemfunktion, um zu bestimmen, ob ein erneuter Validierungsprozess nach einer Änderung des computergestützten Systems erforderlich ist.

Erläuterungen zur deutschen Übersetzung des OECD-Dokuments „Die Anwendung der GLP-Grundsätze auf computergestützte Systeme“

Die nachfolgenden Erläuterungen beziehen sich auf das vorstehende übersetzte OECD-Dokument. Die den Erläuterungen vorangestellten Nummern und Buchstaben sowie die im Text in eckige Klammern gesetzten Nummern verweisen auf die entsprechenden Ziffern und Buchstaben im Dokument [2]).
Die in Anführungszeichen gesetzten Textteile sind Zitate aus einer Veröffentlichung in der Zeitschrift „Die pharmazeutische Industrie“, 1996 zur Anwendung EDV-gesteuerter Systeme bei der Anwendung der GLP.

1. Verantwortlichkeiten

Die Definition von computergestützten Systemen als „eine Kombination von Hardware-Komponenten und zugehöriger Software, die zur Ausführung einer speziellen Funktion oder mehrerer Funktionen entworfen und entsprechend eingerichtet wurden“ ist sehr weitgehend und umfasst sowohl Taschenrechner – soweit mit komplexen Funktionen, insbesondere mit Statistikprogrammen ausgestattet oder programmierbar -, viele der heute üblichen Messgeräte, eigenständige oder vernetzte PCs sowie sehr komplexe LIM-Systeme. Grundsätzlich fallen alle diese Systeme unter die Erläuterungen des Konsenspapiers.

[2] Wie auch in den GLP-Grundsätzen reicht es nicht, den Abschnitt 1 „Verantwortlichkeiten“ zu lesen, um einen vollständigen Überblick zu erhalten. Viele Angaben sind auch in anderen Abschnitten implizit enthalten. In der Erläuterung wird jeweils darauf hingewiesen, wenn Bestimmungen aus anderen Abschnitten stammen.

Die Aufteilung der Verantwortlichkeiten im speziellen Fall computergestützter Systeme ist die gleiche, wie sie in den GLP-Grundsätzen in allgemeiner Weise festgelegt ist. Danach trägt die Leitung die organisatorische, der Prüfleiter die fachliche und das Personal die Verantwortung für die Ausführung. Die Qualitätssicherung sollte die Durchführung der verschiedenen Tätigkeiten überwachen und bei festgestellten Mängeln der Leitung der Prüfeinrichtung und gegebenenfalls dem Prüfleiter (bei GLP-pflichtigen Prüfungen) beziehungsweise dem federführend Beauftragten (bei Entwicklung, Validierung und Wartung computergestützter Systeme) darüber berichten.
Im konkreten Fall der Anwendung der GLP-Grundsätze auf computergestützte Systeme ergeben sich im einzelnen folgende Verantwortlichkeiten (siehe Fußnote 2) , wobei gegliedert wird in Leitung der Prüfeinrichtung , Prüfleiter, Personal und Qualitätssicherung und innerhalb der Funktionsgruppe „Leitung“ in die Bereiche Entwicklung, Validierung, Betrieb und Wartung.

a. Leitung der Prüfeinrichtung

Entwicklung
Erfolgt die Entwicklung von Software in der Prüfeinrichtung , so sind Leitlinien und Verfahren festzulegen, die garantieren, dass computergestützte Systeme in Übereinstimmung mit den GLP-Grundsätzen entwickelt werden [(1a)]. In diesem Fall ist Personal zu benennen, das mit der Entwicklung beauftragt wird, und nachzuweisen, dass es in dem erforderlichem Maß qualifiziert ist, um die Entwicklung durchzuführen.
Wenn computergestützte Systeme von externen Herstellern bezogen werden, sind Leitlinien und Verfahren erforderlich, die eine Bewertung der Zuverlässigkeit des Herstellers und der Qualität des Produktes ermöglichen [7]. In größeren Firmen, in denen die Prüfeinrichtung auf Serviceangebote aus anderen Bereichen zurückgreift, die nicht zur Prüfeinrichtung gehören, sind diese Bereiche wie externe Hersteller zu behandeln.
Zu den anzuwendenden Verfahren hinsichtlich der Bewertung der Zuverlässigkeit von Herstellern und ihrer Produkte wird keine konkrete Aussage getroffen, sondern auf „anerkannte technische Standards“ verwiesen [7]. Allein die Tatsache, dass ein Hersteller nach ISO 9001 zertifiziert ist, sagt noch nichts über die Qualität des zu beurteilenden Produktes aus. Bei kritischen und/oder komplexen Systemen sollten darüber hinausgehende Nachweise gefordert werden. Das können herstellereigene Qualitätssicherungsstandards und –maßnahmen sowie formale Produktzertifizierungen durch renommierte Zertifizierungsstellen [3]) sein. In der Regel bescheinigen solche Stellen jedoch nur, dass ein Produkt den schriftlichen Spezifikationen entspricht. Die Bewertung der Eignung einer Produktspezifikation hinsichtlich des vorgesehenen Anwendungsbereiches in der Prüfeinrichtung ist daher in solchen Fällen erforderlich.

Validierung
Die Entwicklung von Hard- und Software – extern oder intern – wird mit der Validierung abgeschlossen. Wenn der Nachweis erbracht ist, dass die Entwicklung ausreichende Produktqualität gewährleistet, ist bei fremdbezogenen Systemen ein Akzeptanztest [7a)] in der Prüfeinrichtung am Ort der Anwendung oder einer vergleichbaren Anwendungsumgebung (Nachweis der Vergleichbarkeit) ein weiterer Schritt der Validierung.

[3] In Deutschland beispielsweise durch die Gütegemeinschaft Software e.V. nach DIN 66285 (1990) nach RAL Gütezeichen Software (1990) oder nach den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) 1991 und 1993 verbreiteten Richtlinien Information Technology Security Evaluation Criteria (ITSEC) und Information Technology Security Evaluation Manual (ITSEM).

Für die Durchführung der Validierung sind Personen zu benennen und deren Aufgaben zu beschreiben. Es ist nachzuweisen, dass die benannten Personen ausreichend für die durchzuführenden Aufgaben qualifiziert sind [1a)].Für die notwendige Qualifikation erforderliche Aus- und Fortbildungsmaßnahmen sind durchzuführen und zu dokumentieren. Dem benannten Personal können externe Fachleute zur Seite gestellt werden.
Die Validierung wird aufgrund eines vorher entworfenen Validierungsplanes [7a)] durchgeführt, der alle auszuführenden Arbeiten, die Testdaten, eine Beschreibung, was durch die beschriebenen Testdaten gemessen werden soll, und die erwarteten Ergebnisse enthält. Die Durchführung der Validierung ist zu dokumentieren. Die Ergebnisse der Validierung sind in einer Zusammenfassung wiederzugeben [7a)].Validierungsplan, Dokumentation und Zusammenfassung sind ebenso lang aufzubewahren, wie die mit Hilfe des computergestützten Systems erzeugten Daten, die in Prüfungen nach den GLP-Grundsätzen verwendet werden (das heißt, gegebenenfalls auch über die in getrennten Regelungen veröffentlichten Aufbewahrungsfristen für Dokumente hinaus) [9].
Es ist von der Leitung in Leitlinien und Verfahren zu definieren, welche Validierungsanforderungen an unterschiedliche computergestützte Systeme vom Taschenrechner bis zum LIMS zu stellen sind.
Je nach Art, Komplexität und Größe der verwendeten EDV-Systeme sind unterschiedliche, zum Teil umfangreiche Maßnahmen erforderlich. Wichtig ist, dass entsprechende Überlegungen angestellt wurden und die Leitung der Prüfeinrichtung für alle Geräteklassen Qualitätsanforderungen definiert hat, aus denen sich der Umfang der durchzuführenden Prüfungen ableiten lässt. Im Falle von Taschenrechnern können die Maßnahmen beispielsweise in einer Überprüfung der verwendeten Geräte (z.B. Bestimmungen über die von der Prüfeinrichtung zugelassenen Modelle) und vor allem der verwendeten komplexen Funktionen bestehen. Bei LIMS am anderen Ende der Komplexitätsskala sind hingegen alle im Konsenspapier beschriebenen Punkte zu beachten.

Betrieb
Für den Betrieb von computergestützten Systemen müssen ausreichend qualifiziertes Personal, geeignete Räumlichkeiten, Ausrüstung und Verfahren vorhanden sein [1a)]. Vor Inbetriebnahme sind folgende Maßnahmen zu etablieren:
- Verfahren für die Sicherheit und den Schutz von Hardware, Software und Daten vor Verfälschung, unbefugter Änderung oder Verlust [6]. Diese umfassen physische (Zugangsschutz) und logische (Identitätsprüfung, Plausibilitätskontrollen) Verfahren [6a), b)] und die Festlegung der zu deren Verwaltung und Kontrolle erforderlichen Zuständigkeiten und Verantwortlichkeiten.Die Leitung der Prüfeinrichtung hat Sorge zu tragen, dass die persönliche Identifizierung beim Zugang zu EDV-Systemen durch Standardarbeitsanweisungen geregelt wird. Sofern Zugangsberechtigungen vergeben werden, muss die Vergabe durch eine Person (oder Personen) erfolgen, die an Prüfungen nicht beteiligt ist (sind).
- Sicherstellung der ausreichenden Schulung des Personals bezüglich Bedienung [1a)], Sicherheitsanforderungen [6c)] und Kenntnis von „Ausweichplänen“ [4b)].
- Definition von Rohdaten für alle computergestützten Systeme [5].
- Definition der Änderungen, die eine Revalidierung erforderlich machen, oder Etablierung eines Bewertungsverfahrens zur Ermittlung dieser Notwendigkeit [4a),b)].
- Definitionen der Änderungen , die ein formales Change-Control-Verfahren erforderlich machen, oder Etablierung eines Bewertungsverfahrens zur Ermittlung der Notwendigkeit sowie die Festlegung entsprechender Aufgaben und Verantwortlichkeiten [7c)].
- Bereitstellung aller erforderlichen Standardarbeitsanweisungen [8d)].

- Bereitstellung aller erforderlichen Einrichtungen und Ausrüstungen für die Aufbewahrung und Archivierung elektronisch gespeicherter Rohdaten, Dokumente und unterstützender Aufzeichnungen [9].

Wartung
Der Begriff Wartung umfasst sowohl Routinewartungsmaßnahmen als auch die Behebung von Störungen [4a)].
Für die Wartung sind die Aufgaben und Verantwortlichkeiten zu regeln, der Umfang von Wartungsarbeiten, der eine Revalidierung erforderlich macht, festzulegen und es ist für eine ausreichende Dokumentation der Wartungsarbeiten (bei Störungen Dokumentation der Störung und deren Behebung) zu sorgen [4a)].

b. Prüfleiter
Die Prüfleiter sind dafür verantwortlich, dass nur validierte computergestützte Systeme verwendet werden [1b)]. Sie haben sich daher zu vergewissern, welche Geräte bei ihren Prüfungen verwendet werden.

c. Personal
Das Personal hat alle schriftlichen Anweisungen strikt zu beachten [1c)]. Wenn Arbeiten nicht genau genug definiert sind oder die Ausbildung für eine durchzuführende Tätigkeit nicht ausreichend ist, darf das Personal nicht für solche Aufgaben eingesetzt werden. Das Personal soll seine Vorgesetzten gegebenenfalls auf Schulungs- und Fortbildungsbedarf aufmerksam machen.

d. Qualitätssicherung
Wie in anderen Bereichen der Tätigkeit nach den GLP-Grundsätzen arbeitet die Qualitätssicherung (QS) auch bei der Entwicklung, Validierung, beim Betrieb und der Wartung computergestützter Systeme nach Anweisungen der Leitung der Prüfeinrichtung [1d)]. Die QS führt nicht selbst Validierungen durch oder erstellt Validierungspläne. Es ist aber sinnvoll, sie bereits in möglichst einem frühen Stadium mit einzubeziehen. So wird die QS bereits von Anfang an mit der Gesamtplanung vertraut und lernt, Schwachstellen zu erkennen und gezielt zu überwachen. Bei der Formulierung von (Arbeits-)Anweisungen und Validierungsplänen kann sie die Überprüfbarkeit der Anweisungen untersuchen und gegebenenfalls zu besser geeigneten Verfahren raten.
Das Qualitätssicherungspersonal (QS-Personal) muss in den für die Durchführung seiner Aufgaben erforderlichen Techniken genügend gut ausgebildet sein. Das erfordert spezielle Schulungen zum Verständnis der Funktion (komplexer) computergestützter Systeme. Gegebenenfalls sollte in besonders kritischen Phasen auch ein externer Spezialist hinzugezogen werden können [1d)]. Ein prüfeinrichtungsinterner Fachmann kann nur dann beteiligt werden, wenn er nicht in Teile der Entwicklung, der aktiven Durchführung der Validierung, des Betriebs oder der Wartung involviert ist.
Die Aufgaben der QS bei der Einführung erworbener computergestützter Systeme sind ebenfalls von der Leitung der Prüfeinrichtung zu beschreiben [1d)]. Falls externe Audits/Überprüfungen des Herstellers oder Auftragnehmers erforderlich sind, muss das QS-Personal in den dazu erforderlichen Techniken geschult sein.
Da das QS-Personal die Aufgabe hat, sämtliche Tätigkeiten des in GLP-pflichtige Prüfungen involvierten Personals (einschließlich der des Datenverarbeitungs-Personals [DV-Personal]) zu überwachen, sollte das QS-Personal nicht DV-Personal sein (mögliche Ausnahme: Kleinstprüfeinrichtungen).

Benanntes DV-Personal kann in Prüfungen involviert sein. Es muss jedoch in diesem Fall durch organisatorische und/oder technische Maßnahmen sichergestellt sein, dass unbemerkte Änderungen von Zugriffsrechten oder das Umgehen von „Audit Trails“ ausgeschlossen sind.

3. Einrichtungen und Ausrüstungen

Die Standorte (oder Betriebsorte für mobile Ausstattung wie tragbare Computer [Laptops, Notebooks] und Datenerfassungsgeräte) müssen für die computergestützten Systeme geeignet sein. Als Anhaltspunkt für eine ausreichende Planung in dieser Beziehung kann gelten, dass die Herstellerangaben zu den Umgebungsbedingungen für die Systeme beachtet werden [3a)]. Auf maschinenlesbaren Medien gespeicherte Daten weisen, abhängig vom Träger, sehr unterschiedliche Ansprüche an die Betriebs- und Aufbewahrungsbedingungen auf. Diese Unterschiede müssen bedacht werden und geeignete Bedingungen geschaffen werden. Beispielsweise erfordert die Aufbewahrung magnetischer Datenträger andere Umgebungsbedingungen als die optischer oder magnetooptischer. Die Herstellerangaben für geeignete Lagerbedingungen müssen beachtet werden. Wenn bestimmte Medien zu neu sind, um solche Bedingungen zu formulieren, sind geeignete Maßnahmen durch die Leitung der Prüfeinrichtung selbst zu erarbeiten und in Kraft zu setzen. Diese Maßnahmen können beispielsweise in einer zusätzlichen Speicherung auf einem bekannten Medium und in der regelmäßigen Überprüfung des eingesetzten neuen Mediums bestehen, um Anhaltspunkte für den Zeitraum der Lagerfähigkeit zu erhalten [3a)].
Hinsichtlich der Lagerung wird auf das Konsensdokument „GLP – Aufbewahrung und Archivierung“ (Bekanntmachung vom 14. Oktober 1993, BAnz. S.10077) verwiesen.

5. Daten

Rohdaten sind alle ursprünglichen Laboraufzeichnungen oder deren überprüfte Kopien, die als Ergebnis der ursprünglichen Beobachtungen oder Tätigkeiten anfallen.
Weil bei der Anwendung von computergestützten Systemen Rohdaten in unterschiedlicher Form auftreten können, ist die Prüfeinrichtung verpflichtet, verfahrensbezogen jeweils die Rohdaten vorab in Standardarbeitsanweisungen zu definieren. Hierbei besteht die Möglichkeit, die ursprünglich anfallenden elektronischen Daten oder den ersten Computerausdruck davon in lesbarer oder bildlich verständlicher Form als Rohdaten zu akzeptieren. Die akzeptierten Daten müssen mit Zusatzinformationen verknüpft sein, die gestatten, die Durchführung z. B. einer Messung nachzuvollziehen. Nicht nur die Form, sondern auch für die inhaltliche Akzeptanz der Rohdaten sind Kriterien vorab in Standardarbeitsanweisungen festzulegen.

Auszug aus der Veröffentlichung in der Zeitschrift „Die pharmazeutische Industrie“, 1996 (im Druck):

„Für mittels Computer erzeugte Rohdaten ist Wert darauf zu legen, dass diese unabhängig von einer anwendungsspezifischen Hard- und/oder Software nachvollzogen werden können und dass sie vorzugsweise mit allgemein und langfristig verfügbaren technischen Hilfsmitteln lesbar sind. Nur wenn diese Anforderungen erfüllt werden, können computergespeicherte Daten als Rohdaten definiert werden.
Falls elektronisch gespeicherte Daten als Rohdaten definiert sind, sind Vorkehrungen zu treffen, dass sämtliche Änderungen von Daten und Methoden nachvollziehbar sind mit der Angabe, wer wann was und weshalb geändert hat (z.B. Audit-trail).

Bei der Aufbewahrung über längere Zeit oder der Archivierung von elektronisch gespeicherten Daten ist zu beachten, dass für jedes Speichermedium in Abhängigkeit von seiner Umgebung besondere Vorkehrungen zur Sicherstellung der Datenintegrität erforderlich sind [3, 6]. Weil die längerfristige Aufbewahrung bzw. die Archivierung elektronisch gespeicherter Daten erhebliche Probleme mit sich bringt (z.B. Kompatibilitätsprobleme infolge der rasanten Entwicklung von Hard- und Software, aber auch physikalische Probleme bei der langfristigen Lagerung), ist es unter Umständen zweckmäßig, die Rohdaten vor Abschluss der Prüfung oder zu einem geeigneten späteren Zeitpunkt auszudrucken. Zur Prüfung der Datenintegrität ist dann wie bei einer Rohdatenkopie zu verfahren.
Weitere Hinweise für die Praxis aus der Veröffentlichung in der Zeitschrift „Die pharmazeutische Industrie“, 1996 (im Druck):
„Die Vollständigkeit und Zuverlässigkeit der festgehaltenen Daten bei manueller Erfassung setzt Sorgfalt seitens des Laboranten voraus. Unter Umständen können ‘kritische‘ daher durch eine Zweitunterschrift vom Prüfleiter oder einer anderen Aufsichtsperson zusätzlich abgesichert werden ... Eingebaute Prüfprozeduren können das Laborpersonal bereits bei der Erfassung auf unwahrscheinliche oder außergewöhnliche Zahlen (z.B. außerhalb der Standardabweichung) hinweisen. Es sollten Verfahren bestehen, wie bei Auftreten derartiger Fälle zu verfahren ist.
Die richtige Zuordnung von erhobenen Daten zu den betreffenden Prüfungen bei handschriftlicher Datenerfassung kann durch die Verwendung von gebundenen Laborbüchern gewährleistet sein, wobei z.B. ein Buch für jede Prüfung verwendet wird, oder – bei Verwendung von Loseblattformularen – durch die sorgfältige Eintragung einer Prüfungsnummer auf den Formularen. Bei einer EDV-gestützten Datenerfassung müssen die Daten so geordnet werden können, dass der Anwender in die Lage versetzt wird, immer die richtigen Daten auswählen zu können, und dass deren Zusammenhang und Zuordnung eindeutig ersichtlich ist.
Die Zuordnung der erhobenen Daten zu einer bestimmten Person erfolgt handschriftlich, in der Regel durch Abzeichnen des Zuständigen mit seinem Namenskürzel. Bei der EDV-Erfassung müssen entsprechende Vorkehrungen (z.B. personenbezogene Rechte, Verwendung von Passworten usw.) eine analoge Zuordnung ermöglichen.
Die Nachvollziehbarkeit von evtl. nachträglichen Änderungen in Daten oder Unterlagen wird bei handschriftlich erfassten Daten beispielsweise durch das Verbot der Verwendung von Radiergummi, Bleistift oder Korrekturflüssigkeit sichergestellt. Bei EDV-Systemen müssen daher Möglichkeiten vorhanden sein, nachträgliche Änderungen der Daten exakt zu identifizieren, die ursprünglichen Daten zu erhalten und die Identifikation der ändernden Person sicherzustellen. Die retrospektive Nachvollziehbarkeit einer GLP-Studie muss auch beim Einsatz von GLP-Systemen gewährleistet sein.
Die gesicherte langfristige Aufbewahrung von Papierunterlagen ist durch die Führung eines GLP-Archivs gewährleistet. Für elektronisch erfasste Daten mit Rohdatenstatus muss ein Konzept für die Archivierung einschließlich Wiederfindung und Lesbarkeit vorliegen. Es müssen weiterhin Sicherungskonzepte existieren, die vor Datenverlust schützen (z.B. Spiegelplatten, Magnetbandkopien, Back-ups).“

6. Sicherheit

Im Zusammenhang mit der Sicherheit von computergestützten Systemen sollen insbesondere drei Punkte beachtet werden:
- Daten dürfen nicht verloren gehen.

- Daten dürfen von nicht dazu autorisierten Personen nicht verändert werden, weder absichtlich noch unabsichtlich.
- Daten dürfen auch von autorisierten Personen nicht undokumentiert verändert werden.

Durch geeignete Maßnahmen hat die Leitung der Prüfeinrichtung diese Punkte zu gewährleisten [1].

a. Physische Sicherheit

Zur Sicherstellung der physischen Sicherheit können folgende Maßnahmen herangezogen werden:

- Zugangsbeschränkung zu Gebäuden oder Räumen, in denen das computergestützte System untergebracht ist. Als Möglichkeiten bieten sich an:
  - Verteilung von Türschlüsseln nur an berechtigte Personen,
  - Zugang über maschinenlesbare Kennkarten oder Code-Schlösser. In diesem Fall können alle Personen registriert werden, die das abgeschlossene Gebäude oder den abgeschlossenen Raum betreten haben,
  - Überprüfung der Zugangsberechtigung durch Wachpersonal.
- Zugangsbeschränkung zu dem computergestützten System.

b. Logische Sicherheit

Zur Sicherstellung der logischen Sicherheit können folgende Maßnahmen herangezogen werden:

1. Zugang sowohl zu dem Computer-Betriebssystem als auch zur Applikationssoftware über persönliche Codes (Passwörter). Für die Erzeugung von Codes sollten Verfahren festgelegt sein, die die Länge der Codes, die Verwendung von Sonderzeichen, die Gültigkeitsdauer sowie das Verhalten bei Verlust regeln. Passwörter sollten in regelmäßigen Zeitabständen geändert werden.
2. Automatisches Löschen des Bildschirminhaltes nach einer vorgegebenen Dauer der Nichtbenutzung und Wiederzugang durch persönlichen Code. Dadurch wird verhindert, dass z.B. während kurzer Abwesenheit des berechtigten Benutzers nichtautorisierte Personen auf das System zugreifen können.

c. Datenintegrität

Hierfür empfiehlt sich beispielsweise die Verwendung von quersummengeschützten binären Dateien. Durch die Verwendung des Binärformats werden absichtliche Änderungen erheblich erschwert.

7. Validierung computergestützter Systeme

Der Benutzer von Software und computergestützten Systemen ist für deren Validierung verantwortlich. Teile der Validierung, z.B. Validierung während der Entwicklung, können vom Hersteller übernommen werden. In diesem Fall soll der Hersteller durch Mitlieferung einer entsprechenden Validierungserklärung schriftlich bestätigen, dass das System während des Entwicklungsablaufs validiert wurde. Es sollte ebenfalls schriftlich gewährleistet werden, dass Validierungsdokumente einschließlich des Quellcodes im Bedarfsfall Behörden zugänglich gemacht werden können.

Der Benutzer der Software oder des computergestützten Systems sollte sich vergewissern, dass es sich bei dem Hersteller um einen anerkannten Softwarelieferanten handelt. Hinweise darauf können z.B. sein:

- Reputation der Firma als Geräte- und/oder Softwarehersteller,
- Anzahl der im Einsatz befindlichen Softwarepakete,
- Einsatz eines anerkannten Qualitätssicherungssystems, z.B. ISO 9001

Falls entsprechende Hinweise nicht vorhanden sind, soll sich der Benutzer von der Zuverlässigkeit des Herstellers selbst überzeugen. Das kann zunächst durch Übersendung und Ausfüllen einer entsprechenden Checkliste erfolgen. Falls auch diese keine zuverlässigen Aussagen zulässt, ist ein direkter Audit der Herstellerfirma in Erwägung zu ziehen.

a. Akzeptanz

Akzeptanztests

In jedem Fall soll das computergestützte System im Labor des Benutzers einem Akzeptanztest unterzogen werden, bevor es für GLP-pflichtige Prüfungen eingesetzt wird. Hierdurch soll gewährleistet werden, dass das System im Benutzerlabor unter realen Arbeitsbedingungen die für den Routinebetrieb vorgesehene Leistung erbringt und für die Verwendung geeignet ist.
Fremdbezogene Software und computergestützte Systeme beinhalten häufig mehr Funktionen, als für den vorgesehenen Einsatz erforderlich sind. Da jedoch nur die Funktionen einem Akzeptanztest unterzogen werden sollten, die auch benötigt werden, sollten zunächst die vorgesehenen Funktionen definiert werden. Zur Erleichterung dieser Aufgabe ist es ratsam, dass der Lieferant eine vollständige Funktionsliste mitliefert, aus der der Benutzer die für seine Aufgaben erforderlichen Funktionen auswählen kann.
Der Umfang der Akzeptanztests hängt von der Art und Komplexität des computergestützten Systems ab. Bei computergestützten analytischen Messgeräten mit Auswerteeinheit, z.B. einem Chromatographiesystem, kann ein Akzeptanztest darin bestehen, dass komplette Analysen von einer oder mehreren Proben durchgeführt werden und die erhaltenen Ergebnisse mit erwarteten Ergebnissen verglichen werden. Falls die mit dem Gesamtsystem erhaltenen Ergebnisse den Erwartungen entsprechen, kann davon ausgegangen werden, dass die einzelnen Module, einschließlich der Software, den Anforderungen entsprechen. Bei den Tests ist darauf zu achten, dass diese auch Grenzsituationen im Anwendungsbereich beinhalten.
Bei Computersystemen mit Auswertefunktion von manuell eingegebenen Daten sowie mit Tabellenkalkulations- und Datenbankfunktion sollen die Funktionen dadurch getestet werden, dass eine Reihe von Eingabewerten mit dem Computersystem errechnet wird und die Ergebnisse mit erwarteten Werten verglichen werden. Bei der Auswahl der Eingabewerte ist darauf zu achten, dass diese realen Werten entsprechen und den gesamten Anwendungsbereich beinhalten. Falls Daten in andere Programme, wie Textverarbeitungsprogramme oder Datenbanken, elektronisch übertragen werden, sollte die korrekte Übertragung validiert oder stichprobenartig überprüft werden.
Akzeptanztests sollten nicht nur bei der Neuinstallation, sondern nach Änderungen an dem System, nach Reparaturen und in regelmäßigen zeitlichen Abständen nach einem festgelegten Plan erfolgen.

b. Nachträgliche Evaluierung

Zum 1. Absatz:
Ein Altsystem ist ein bestehendes System, das nicht nach den OECD-Vorgaben validiert ist.
Zum 2. Absatz:
Als „historische Aufzeichnungen“ sind hierbei anzusehen

- Wartungsberichte
- Kalibrierungen/Eichberichte
- Reparaturberichte
- Fehlermeldungen
- Berichte über Leistungstests
- Gerätebeschreibung, Spezifikation, Lieferant, Anschaffungsdatum

Wenn die Bewertung dieser Unterlagen ergibt, dass die Validität nicht hinreichend gewährleistet ist, sind zusätzliche Maßnahmen erforderlich. In diesem Fall muss davon

ausgegangen werden, dass gegebenenfalls die in der Vergangenheit gewonnenen Daten nicht hinreichend valide sind.
Sobald das Gerät als valide getestet ist, wird es wie ein Neugerät behandelt.

c. Verfahren der kontrollierten Systemänderung
(Change Control)

Ein Verfahren der kontrollierten Systemänderung ist immer dann nach den Vorschriften des OECD-Konsens-Papiers durchzuführen, wenn eine beabsichtigte Änderung des computergestützten Systems seine Validität beeinflussen könnte. Wann solche Verfahren durchzuführen sind, ist von der Leitung der Prüfeinrichtung festzulegen. Gleichzeitig sind die Aufgaben und Verantwortlichkeiten zu beschreiben.
Im wesentlichen wird ein solches Verfahren bei wesentlichen Änderungen des Gesamtsystems oder dessen Teilen erforderlich sein.
Solche Änderungen sind beispielsweise (Aufzählung nicht vollständig):

- Software-Versionsänderungen,
- Modulfreischaltungen (von vorher zwar vorhandenen, jedoch nicht benutzten Programm-Modulen),
- Einsatz von selbstentwickelten Ergänzungen/Erweiterungen des Systems (beispielsweise Auswertungen auf Benutzernachfrage),
- Einsatz neuer Betriebssystem-Versionen,
- Einsatz neuer Gerätetreiber/Datenübertragungsprotokolle,
- substantielle Veränderungen der Hardware wie
- Einsatz neuer Speichereinheiten
- Erweiterung des Systems (z.B. Netzwerk)
- Einsatz neuer Ausgabegeräte

d. Unterstützende Maßnahmen

Beispiele für die Ermittlung der Systemleistung

- Systemeignungstest für chromatographische Verfahren
  Systemeignungstest für chromatographische Verfahren dienen der Ermittlung kritischer Parameter, z.B. der Auflösung zwischen zwei chromatographischen Peaks oder der Standardabweichung von Peakretentionszeiten oder Peakflächen vor und eventuell während der Analysenserie. Nur wenn die ermittelten Werte innerhalb vorher definierter Grenzwerte liegen, wird die Analysenserie gestartet bzw. weitergeführt.
- Analyse von Kontrollproben und Aufzeichnung der aktuellen Werte auf Kontrollkarten für alle analytischen Verfahren
  Proben mit definierter Zusammensetzung werden vor und zwischen den unbekannten Proben in regelmäßigen Abständen vermessen. Die ermittelten Messwerte für die Mengen (Konzentrationen) werden in Kontrollkarten (Regelkarten) eingetragen. Die Abweichung der gemessenen Werte vom Sollwert soll innerhalb vorher definierter Grenzwerte liegen.
- Verarbeitung von definierten Datensätzen für Auswertesysteme aller Art
  Bekannte Datensätze werden von dem System verarbeitet und die ermittelten Ergebnisse mit den Sollwerten verglichen. Die Datensätze und die Rechenoperationen sollen dabei möglichst den Betriebsbedingungen entsprechen und auch Werte aus den Grenzbereichen enthalten.

8. Dokumentation

Quellcode
In der Regel wird es nicht als notwendig angesehen, dass die Prüfeinrichtung über den Quellcode einer Anwendungssoftware verfügt.

Die Prüfeinrichtung sollte sich jedoch vom Hersteller einer solchen Software die Zusicherung geben lassen, dass der Quellcode mindestens 12 Jahre aufbewahrt und in begründeten Fällen der Überwachungsbehörde verfügbar gemacht wird.

9. Archive

Es wird auf die Empfehlungen des Konsensdokuments „GLP Aufbewahrung und Archivierung“ (Bekanntmachung vom 14.Oktober 1993, BAnz. S. 10 077) verwiesen.