SERIE OCDE SUR LES PRINCIPES DE BONNES PRATIQUES DE LABORATOIRE ET LA VERIFICATION DU RESPECT DE CES PRINCIPES - NUMERO 10

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING - NUMBER 10

Application des Principes de BPL aux systèmes informatiques
The Application of the Principles of GLP to Computerised Systems

Ceci est la traduction allemande du même document déjà diffusé en anglais et en français
This is the German translation of the same document which has already been distributed in English and in French

ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Paris

63057

OECD-Schriftenreihe
über
Grundsätze der Guten Laborpraxis
und Überwachung Ihrer Einhaltung

Nummer 10

GLP-Konsensdokument

Die Anwendung der Glp-Grundsätze auf Computergestützte Systeme

Umweltmonoraphie Nr. 116

Umweltdirektorat

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

Paris 1995

Auch in OECD-Schriftenreihe über Grundsätze der Guten Laborpraxis und Überwachung Ihrer Einhaltung veröffentlicht:

No. 1, *OECD Principles of Good Laboratory Practice, as revised in 1997*

No. 2, *Revised Guides for Compliance Monitoring Procedures for Good Laboratory Practice* (1995)

No. 3, *Revised Guidance for the Conduct of Laboratory Inspections and Study Audits* (1995)

No. 4, *Quality Assurance and GLP* (1992)

No. 5, *Compliance of Laboratory Suppliers with GLP Principles* (1992)

No. 6, *The Application of the GLP Principles to Field Studies* (1992)

No. 7, *The Application of the GLP Principles to Short-term Studies* (1993)

No. 8, *The Role and Responsibilities of the Study Director in GLP Studies* (1993)

No. 9, *Guidance for the Preparation of GLP Inspection Reports* (1995)

No. 11, *The Role and Responsibilities of the Sponsor in the Application of the Principles of GLP*

Über die OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist eine internationale Organisation, in der die Vertreter von 29 Industriestaaten in Nordamerika, Westeuropa und im Pazifik sowie Vertreter der Europäischen Kommission zusammentreffen, um ihre Politiken zu koordinieren und zu harmonisieren sowie Themen von gemeinsamem Interesse zu erörtern und mit dem Ziel zusammenzuarbeiten, Lösungen für internationale Probleme zu finden. Der überwiegende Teil der Arbeit der OECD wird von mehr als 200 Fachausschüssen und sonstigen Gremien geleistet, die sich aus Delegierten der Mitgliedsländer zusammensetzen. Beobachter aus mehreren Ländern, die bei der OECD einen Sonderstatus haben, und Vertreter interessierter internationaler Organisationen nehmen an zahlreichen OECD-Workshops und anderen Tagungen teil. Die Ausschüsse und sonstigen Gremien werden vom OECD-Sekretariat in Paris unterstützt, das sich in Direktionen und Abteilungen untergliedert.

Die Abteilung Umweltsicherheit und -hygiene (EHS) veröffentlicht sechs unterschiedliche Reihen von Dokumenten: **Testing and Assessment; Good Laboratory Practice and Compliance Monitoring; Pesticides; Risk Management; Hamonization of Regulatory Oversight in Biotechnology,** ergänzt durch die neue Reihe **Chemical Accidents**. Weitere Informationen über das Programm Umweltsicherheit und -hygiene und die EHS-Publikationen sind über den World Wide Web-Site der OECD (siehe nächste Seite) erhältlich.

Diese vorliegende Veröffentlichung wurde im Rahmen des Inter-Organization Programme for the Sound Management of Chemicals (IOMC) erstellt.

Das Inter-Organization Programme for the Sound Management of Chemicals (IOMC) wurde 1995 von UNEP, ILO, FAO, WHO, UNIDO und OECD (d.h. den Teilnehmerorganisationen) gemäß den Empfehlungen der UN-Konferenz über Umwelt und Entwicklung von 1992 eingerichtet, um die Zusammenarbeit zu stärken und die internationale Koordinierung im Bereich der Sicherheit von Chemikalien zu verbessern. UNITAR schloß sich 1997 als siebte Teilnehmerorganisation der IOMC an. Ziel der IOMC ist es, die Koordinierung der von den Teilnehmerorganisationen gemeinsam oder einzeln verfolgten Politiken und Aktivitäten zu fördern, um zu einem im Hinblick auf die menschliche Gesundheit und die Umwelt sachgemäßen Umgang mit Chemikalien beizutragen.

Diese Veröffentlichung kann kostenlos on-line abgerufen werden.

Der ungekürzte Text sowie zahlreiche weitere Veröffentlichungen zum Thema Umweltsicherheit und -hygiene sind über den World Wide Web-Site der OECD (http://www.oecd.org/ehs/) verfügbar

bzw. können direkt angefordert werden bei:

OECD Environment Directorate
Environmental Health and Safety Division

2 rue André-Pascal
75775 Paris Cedex 16
France

Fax: (33-1) 45 24 16 75

E-mail: ehscont@oecd.org

VORWORT

Im Rahmen des dritten OECD Consensus Workshop über Gute Laborpraxis vom 05. bis 08. Oktober 1992 in Interlaken, Schweiz, diskutierte eine Expertengruppe über die Anwendung der GLP-Grundsätze auf Computergestützte Systeme. Den Vorsitz dieser Arbeitsgruppe führte Dr. Theo Helder von der niederländischen GLP-Überwachungsbehörde. Der Berichterstatter war Herr Bryan Doherty (Vorsitzender des Computing Committee of the British Association for Research Quality Assurance). Die Teilnehmer der Arbeitsgruppe kamen sowohl von nationalen GLP-Überwachungsbehörden als auch von Prüfeinrichtungen aus folgenden Staaten: Österreich, Belgien, Dänemark, Finnland, Frankreich, Deutschland, Japan, Niederlande, Schweiz, Großbritannien und USA. Diese Arbeitsgruppe konnte sich in der zur Verfügung stehenden Zeit nicht auf ausformulierte Leitlinien einigen. Es wurde lediglich ein Papier mit dem Titel "Concepts relating to Computerised Systems in a GLP Environment" erstellt, welches die allgemeinen Grundsätze ausführte und die sich daraus ergebenden Probleme beschrieb. Dieses Papier wurde den Mitgliedstaaten zur Kommentierung übersandt.

Aufgrund der eingegangenen Kommentare entschied der GLP-Panel auf seiner fünften Sitzung im März 1993, daß eine weitere Aufbereitung notwendig sei, und berief eine zweite Expertenrunde ein. Unter dem Vorsitz von Dr. Helder und mit dem Berichterstatter Herrn Doherty fand ein Treffen der Gruppe vom 14. bis 16. Dezember 1994 in Paris statt. Vertreter sowohl von Behörden als auch von der Industie aus Kanada, Dänemark, Frankreich, Deutschland, Japan, Niederlande, Schweden, Großbritannien und USA nahmen teil.

Auf der Basis des "Interlaken-Papiers", der eingegangenen Kommentare aus den Mitgliedstaaten sowie eines von einer gemeinsamen Arbeitsgruppe, bestehend aus Vertretern von Regierung und Industrie aus Großbritannien, erarbeiteten Papiers wurde ein Entwurf eines Konsensdokumentes entwickelt. Das Dokument wurde anschließend überarbeitet, leicht modifiziert und vom OECD Panel on GLP sowie von der Arbeitsgruppe Chemikalien und dem Management Komitee des Sonderprogramms für die Kontrolle von Chemikalien befürwortet. Der Umweltpolitische Ausschuß empfahl sodann, dieses Dokument unter der Verantwortung des Generalsekretärs herauszugeben.

GLP - KONSENSDOKUMENT

DIE ANWENDUNG DER GLP-GRUNDSÄTZE AUF COMPUTERGESTÜTZTE SYSTEME

Im Laufe der letzten Jahre hat die Verwendung computergestützter Systeme durch 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, -verarbeitung, 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 dabei 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 der 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-Grundsätze. 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, 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 direkter 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. Sie 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 deshalb 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 Betriebes 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- oder 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, -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 vornahmen. 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. 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 und 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- und 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 Routinen, die die Anwendungen bereitstellen oder durch eine Kombinationen 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 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 zu Rohdaten und muß deshalb wie 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. 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 Orientierunghilfe für die Minimaldokumentation zu 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/des Datenbankdesigns, die in Zusammenhang mit der Anwendung stehen.

- 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, wie für 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 gespeicherten 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 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.

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

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

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

der Systemressourcen, der Rechenzeit, die Ein-/Ausgabesteuerung und die Datenverwaltung zur Verfügung stellen.

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