Arbeitsübersetzung (maßgeblich ist der englische Text vom 20. September 2021)

Nicht klassifiziert

UMWELTDIREKTORAT
AUSSCHUSS FÜR CHEMIKALIEN UND BIOTECHNOLOGIE

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

OECD-SCHRIFTENREIHE ÜBER DIE GRUNDSÄTZE DER GUTEN LABORPRAXIS UND DIE ÜBERWACHUNG IHRER EINHALTUNG

Nummer 22

Advisory Document of the Working Party on Good Laboratory Practice
Beratungsdokument der Arbeitsgruppe Gute Laborpraxis

Integrität von GLP-Daten

OECD Environment, Health and Safety Publications
OECD-Veröffentlichungen zur Umweltsicherheit und –hygiene

Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring
Schriftenreihe über die Grundsätze der Guten Laborpraxis (GLP) und die Überwachung ihrer Einhaltung

Nr. 22

Advisory Document of the Working Party on Good Laboratory Practice

Beratungsdokument der Arbeitsgruppe für Gute Laborpraxis

Integrität von GLP-Daten

EBENFALLS IN DER OECD-SCHRIFTENREIHE ÜBER DIE GRUNDSÄTZE DER GUTEN LABORPRAXIS UND DIE ÜBERWACHUNG IHRER EINHALTUNG VERÖFFENTLICHT

- *No. 1, OECD Principles on Good Laboratory Practice (as revised in 1997)*
  Nr. 1, OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997)

- *No. 2, Revised Guides for Compliance Monitoring Procedures for Good Laboratory Practice (1995)*
  Nr. 2, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 3, Revised Guidance for the Conduct of Laboratory Inspections and Study Audits (1995)*
  Nr. 3, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 4, Quality Assurance and GLP (as revised in 1999)*
  Nr. 4, Qualitätssicherung und GLP (Neufassung aus 1999)

- *No. 5, Compliance of Laboratory Suppliers with GLP Principles (as revised in 1999)*
  Nr. 5, Einhaltung der GLP-Grundsätze durch Lieferanten (Neufassung aus 1999)

- *No. 6, The Application of the GLP Principles to Field Studies (as revised in 1999)*
  Nr. 6, Die Anwendung der GLP-Grundsätze auf Freilandprüfungen (Neufassung aus 1999)

- *No. 7, The Application of the GLP Principles to Short-term Studies (as revised in 1999)*
  Nr. 7, Die Anwendung der GLP-Grundsätze auf Kurzzeit-Prüfungen (Neufassung aus 1999)

- *No. 8, The Role and Responsibilities of the Study Director in GLP Studies (as revised in 1999)*
  Nr. 8, Rolle und Verantwortlichkeiten des Prüfleiters bei GLP-Prüfungen (Neufassung aus 1999)

- *No. 9, Guidance for the Preparation of GLP Inspection Reports (1995)*
  Nr. 9, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 10, The Application of the Principles of GLP to Computerised Systems (1995)*
  Nr. 10, Die Anwendung der GLP-Grundsätze auf computergestützte Systeme (1995)

- *No. 11, The Role and Responsibilities of the Sponsor in the Application of the principles of GLP (1998)*
  Nr. 11, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 12, Requesting and Carrying Out Inspections and Study Audits in Another Country (2000)*
  Nr. 12, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 13, The Application of the OECD Principles of GLP to the Organisation and Management of Multi-Site Studies (2002)*
  Nr. 13, Die Anwendung der OECD GLP-Grundsätze auf Organisation und Management von Multi-Site-Prüfungen (2002)

- *No. 14, The Application of the Principles of GLP to in vitro studies (2004)*
  Nr. 14, Die Anwendung der OECD GLP-Grundsätze auf in vitro Studien (2004)

- *No. 15, Establishment and Control of Archives that Operate in Compliance with the Principles of GLP (2007)*
  Nr. 15, Einrichtung und Betrieb von Archiven in Übereinstimmung mit den Grundsätzen der Guten Laborpraxis (2007)

- *No. 16, Guidance on the GLP Requirements for Peer Review of Histopathology (2014)*
  Nr. 16, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 17, Application of GLP Principles to Computerised Systems (2016)*
- *No. 17, Anwendung der GLP-Grundsätze auf Computergestützte Systeme (2016)*

- *No. 18, OECD Position Paper Regarding the Relationship between the OECD Principles of GLP and ISO/IEC 17025 (2016)*
  Nr. 18, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 19, The Management, Characterisation and Use of Test Items (2018)*
  Nr. 19, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 20, Guidance Document for Receiving Authorities on the Review of the GLP Status of Non-Clinical Safety Studies (2019)*
  Nr. 20, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 21, OECD Position Paper Regarding Possible Influence of Sponsors on Conclusions of GLP Studies (2020)*
  Nr. 21, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

Über die OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist eine internationale Organisation, in die Regierungsvertreter von 38 Industrieländern aus Nord- und Südamerika, Europa und der Region Asien und Pazifik sowie Vertretern der Europäischen Kommission zusammenkommen, um ihre Politik zu koordinieren und zu harmonisieren, 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 den 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, welches sich in Direktorate und Abteilungen untergliedert.

Die Abteilung Umweltsicherheit und Hygiene (EHS) veröffentlicht 11 unterschiedliche Reihen von kostenlos erhältlichen Dokumenten: **Testing and Assessment**; **Good Laboratory Practice and Compliance Monitoring**; **Pesticides**; **Biozides**; **Risk Management**; **Harmonisation of Regulatory Oversight in Biotechnolgy; Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Register; Emission Scenario Documents sowie Safety of Manufactured Nanomaterials.** Weitere Informationen über das Programm Umweltsicherheit und -hygiene und die EHS-Veröffentlichungen sind über die World Wide Web-Site der OECD (www.oecd.org/chemicalsafety/) verfügbar.

Die vorliegende Veröffentlichung wurde im Rahmen des Inter-Organization Programme for the Sound Management of Chemicals (IOMC) erstellt. Inhaltlich spiegelt die Veröffentlichung nicht unbedingt die Ansichten oder erklärten Strategien einzelner Teilnehmerorganisationen des IOMC wider.

Das Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) wurde 1995 gemäß den Empfehlungen der UN-Konferenz über Umwelt und Entwicklung aus dem Jahr 1992 eingerichtet, um die Zusammenarbeit zu stärken und die internationale Koordinierung im Bereich der Sicherheit von Chemikalien zu verbessern. Die Teilnehmerorganisationen sind FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, Weltbank und OECD. Ziel der IOMC ist es, die Koordinierung der von den Teilnehmerorganisationen gemeinsam oder einzeln verfolgten Politik und Aktivitäten zu fördern, um zu einem im Hinblick auf die menschliche Gesundheit und Umwelt sachgemäßen Umgang mit Chemikalien beizutragen.

VORWORT

Dieses Beratungsdokument wurde von der OECD-Arbeitsgruppe für Gute Laborpraxis (GLP) ausgearbeitet. Die Entwicklung des Dokuments wurde vom Vereinigten Königreich initiiert und geleitet und umfasste eine Redaktionsgruppe unter der Leitung von Stephen Vinter (UK) und Thomas Lucotte (France Medical Products). Der Redaktionsgruppe gehörten Vertreter aus Argentinien, Österreich (Medizinische Produkte), Belgien, Dänemark (Medizinische Produkte), Italien, Mexiko, den Niederlanden, den USA (EPA) und den USA (FDA) an. Das Verfahren umfasste eine öffentliche Kommentierungsphase sowie die Überprüfung und Billigung des Dokuments durch die Arbeitsgruppe für Gute Laborpraxis.

Dieses Dokument wird unter der Verantwortung des Chemicals and Biotechnology Committee (CBC) veröffentlicht, das am 8. September 2021 der Freigabe zugestimmt hat.

Inhaltsverzeichnis

1. Hintergrund

Eines der grundlegenden Ziele der Grundsätze der Guten Laborpraxis (GLP) ist die Sicherstellung der Qualität und Integrität der Prüfdaten im Zusammenhang mit nicht-klinischen Sicherheitsprüfungen.

Die Art und Weise, in der Prüfdaten zur Bewertung der Sicherheit von Mensch, Tier und Umwelt generiert, gehandhabt, berichtet, aufbewahrt und archiviert werden, hat sich im Einklang mit der Einführung und der fortlaufenden Entwicklung unterstützender Technologien weiterentwickelt. Dazu gehören die zunehmende Nutzung der elektronischen Datenerfassung, sowie die Integration und Automatisierung von Systemen und anderen Technologien. Die Systeme reichen von manuellen Verfahren mit Papieraufzeichnungen bis hin zum Einsatz komplexer computergestützter Systeme. Der Hauptzweck der Anforderungen der GLP-Grundsätze besteht jedoch weiterhin darin, dasselbe Vertrauen in die Qualität und Integrität der Daten zu haben sowie die Möglichkeit durchgeführte Tätigkeiten während der Durchführung von nicht-klinischen Sicherheitsprüfungen rekonstruieren zu können.

2. Einleitung

Für dieses Dokument gelten die folgenden übergreifenden Aspekte:

1. Dieses Dokument ist eine Leitlinie für Prüfeinrichtungen oder Prüfstandorte, die GLP-Prüfungen oder Phasen von GLP-Prüfungen durchführen.

   Für die Zwecke dieses Dokuments umfasst der Begriff "Prüfeinrichtung" Prüfstandorte; der Begriff "Prüfung" umfasst Phasen von Prüfungen; und der Begriff "Prüfleiter" wird erweitert, um gegebenenfalls die Aufgaben des örtlichen Versuchsleiters (Principal Investigator) abzudecken.

2. Die Leitlinie zielt darauf ab, einen risikobasierten Ansatz für die Verwaltung von Daten zu fördern, der das Datenrisiko, die Kritikalität und den Lebenszyklus einschließt. Die Benutzer dieses Dokuments müssen die Datenströme, für die sie verantwortlich sind oder an denen sie beteiligt sind (als Lebenszyklus) verstehen, um Daten zu identifizieren, die wahrscheinlich Auswirkungen auf die Einhaltung der GLP-Grundsätze haben. Dies wiederum wird die Identifikation und Umsetzung der wirksamsten und effizientesten risikobasierten Kontrollen unterstützen.

3. Datenintegrität beschreibt das Maß, in dem Daten vollständig, konsistent, korrekt sowie vertrauenswürdig sind und diese Datenmerkmale während des gesamten Datenlebenszyklus beibehalten werden. Daten sind auf sichere Weise zu sammeln und aufzubewahren, so dass sie zuschreibbar, lesbar, zeitnah aufgezeichnet und korrekt sind, egal ob es sich um Rohdaten oder eine überprüfte Kopie handelt.

4. Die Leitlinie nimmt Bezug auf das Akronym ALCOA (engl.: Attributable, Legible, Contemporaneous, Original and Accurate), welches zuschreibbar, lesbar, zeitnah, original und korrekt bedeutet. Die ALCOA-Eigenschaften werden historisch als die Dateneigenschaften angesehen, die für regulatorische Zwecke geeignet sind. In jüngerer Zeit wird dies durch ALCOA+ um die zusätzlichen Attribute vollständig (complete), konsistent (consistent), dauerhaft (enduring) und verfügbar (available) erweitert. Die Erwartungen an die Datenintegrität unterscheiden sich bei beiden

Begriffen nicht, da Data Governance-Maßnahmen sicherstellen müssen, dass die Daten während des gesamten Lebenszyklus vollständig, konsistent, dauerhaft und verfügbar sind.

5. Die Leitlinie befasst sich mit der Datenintegrität, nicht jedoch mit der Datenqualität, da die für die Integrität erforderlichen Maßnahmen die (wissenschaftliche) Qualität der Daten nicht gewährleisten können (siehe auch die Definitionen in den Abschnitten 3.4 und 3.5). Datenintegrität ermöglicht die Kontrolle über die Daten (d. h. ob diese vertrauenswürdig sind), während Datenqualität sich auf diejenigen Dateneigenschaften bezieht, die sicherstellen, dass die erzeugten Daten in Übereinstimmung mit den geltenden Vorgaben generiert werden und für ihren vorgesehenen Zweck verwendet werden können.
6. Diese Leitlinie ist gleichermaßen für die Kontrolle aller Datentypen und Formate anzuwenden. Einige Punkte zielen jedoch explizit nur auf elektronische Daten und elektronische Systeme ab.
7. Diese Leitlinie ist in Verbindung mit den OECD-Dokumenten Nr. 1 (*OECD-Grundsätze der Guten Laborpraxis*) (OECD, 1997 [1]), Nr. 15 (*Einrichtung und Betrieb von Archiven in Übereinstimmung mit den Grundsätzen der Guten Laborpraxis*) (OECD, 2007[2]), Nr. 16 *Guidance on the GLP Requirements for Peer Review of Histopathology*) (OECD, 2014 [3]) und Nr. 17 (*Anwendung der GLP-Grundsätze auf Computergestützte Systeme*) (OECD, 2016[4]) und geltenden nationalen Vorschriften zu lesen. Die GLP-Grundsätze für die Datenintegrität finden sich in den Abschnitten II, 1.1.2.b bis e, 1.1.2.l, 1.1.2.q, 1.2.2.f, 1.2.2.g, 1.2.2.i, 1.4.3, 2.1.1.c, 3.4, 7.1, 7.4.3, 8.2.6, 8.3.3., 8.3.4, 8.3.5, 10.1 des OECD-Dokuments Nr. 1. Sofern relevante ergänzende Informationen in diesem Dokument und anderen Dokumenten enthalten sind, wird im Text darauf verwiesen.

3. Definitionen und Begriffe

3.1. Daten

Bei Daten handelt es sich um quantitative oder qualitative Fakten, (Zahlen)werte und Statistiken, die zu Referenzzwecken oder zur Analyse erhoben werden. Diese umfassen alle Originalaufzeichnungen und überprüften Kopien von Originalaufzeichnungen, einschließlich Rohdaten und Metadaten und alle nachfolgenden Umwandlungen, die zum Zeitpunkt der GLP-Tätigkeit erzeugt oder aufgezeichnet wurden, und eine vollständige Rekonstruktion und Bewertung der GLP-Tätigkeit ermöglichen.

Daten können verschiedene Formate (z. B. analog, digital) und Strukturen, Layouts (z. B. auf Papier oder auf dem Bildschirm), Quellen (z. B. Chromatogramme, Text, Bild, Video usw.) und Medien haben, die zum Speichern oder Präsentieren verwendet werden (Papier, DVD, Fotofilm, Bandspeicher, elektronische Dateien usw.).

Daten können erfasst oder aufgezeichnet werden:

i. durch manuelle Aufzeichnung einer Beobachtung oder einer Tätigkeit auf Papier oder in einem elektronischen System;
ii. durch eine automatische Aufzeichnung, auf Papier (durch automatisches Drucken) oder in einem elektronischen System, unter Verwendung von Geräten, die von

einfachen Instrumenten bis hin zu hochkomplexen, konfigurierbaren computergestützten Systemen reichen;

iii. durch Verwendung eines Hybridsystems, bei welchem Kombinationen aus Papier (oder anderen nicht elektronischen Medien) und elektronischen Aufzeichnungen die Rohdaten bilden;

iv. auf anderen Trägern wie Fotografie, Bildgebungsverfahren und -technologien, Chromatografieplatten usw., die manuell oder automatisch oder mithilfe eines Hybridsystems erzeugt werden könnten.

Rohdaten

Die Grundsätze der GLP definieren Rohdaten als alle ursprünglichen Aufzeichnungen und Unterlagen der Prüfeinrichtung, oder deren überprüfte Kopien, die als Ergebnis der ursprünglichen Beobachtungen und Tätigkeiten in einer Prüfung anfallen und eine vollständige Rekonstruktion und Bewertung der GLP-Tätigkeiten ermöglichen. Zu den Rohdaten zählen beispielsweise Fotografien, Mikrofilm- oder Mikrofichekopien, computerlesbare Medien, diktierte Beobachtungen, aufgezeichnete Daten von automatisierten Geräten oder jegliche andere Daten auf Speichermedien, die anerkanntermaßen geeignet sind, Informationen über einen festgelegten Zeitraum sicher zu speichern.

Aufzeichnung

Eine Aufzeichnung ist eine Teilinformation (z. B. Daten). Der Begriff ursprüngliche Aufzeichnung wird verwendet, um die erste Informationsquelle oder Datenerfassung zu beschreiben. Ursprüngliche Aufzeichnungen sind in der Regel Rohdaten. Wenn eine ursprüngliche Aufzeichnung der Definition von Rohdaten entspricht, aber nicht als solche betrachtet wird, so ist dies zu begründen.

Überprüfte Kopie

Eine überprüfte (verifizierte) Kopie ist ein wahrheitsgetreues Abbild des Originals zum Zeitpunkt der Erstellung der Kopie. Eine überprüfte Kopie kann in einem anderen Format oder Dokumenttyp als das Original gespeichert/aufbewahrt werden.

Überprüfte Kopien können erstellt werden, um:

- ein Duplikat der Originale zu erstellen, um sie in verschiedene Ordner aufzunehmen (z. B. experimentelle Rohdaten, die in mehreren Prüfungen verwendet werden);
- die Aufbewahrungsdauer für einige Daten zu verlängern, deren ursprüngliches Format eine dauerhafte Erhaltung nicht zulässt (z. B. Thermodrucke);
- die Aufbewahrung der Daten zu ermöglichen, wenn das Original nicht aufbewahrt werden kann, ohne andere archivierte Materialien zu gefährden (z. B. mit Tierflüssigkeiten, Chemikalien usw. verunreinigte Papierrohdaten);
- Vereinfachung des Datenaustauschs;
- Unterstützung der Archivierungsverfahren.

Die gängigsten Verfahren, um überprüfte Kopien aus statischen Aufzeichnungen zu erstellen, sind:

- Fotokopie einer Papieraufzeichnung (Papier auf Papier);

- Scannen einer Papieraufzeichnung (Papier zu elektronisch);
- Bild einer Papieraufzeichnung (Papier zu Bild);
- Screenshot und Ausdruck einer elektronischen Aufzeichnung (elektronisch zu Papier).

Abgeleitete Daten

Abgeleitete Daten werden aus Rohdaten gewonnen und rekonstruiert (z. B. Endkonzentrationen werden durch eine Kalkulationstabelle berechnet, die sich auf Rohdaten eines Geräts stützt; Ergebnistabellen werden durch ein Labor-Informations- und Management-System (LIMS) zusammengefasst, usw.). Abgeleitete Daten werden durch Datenverarbeitung gewonnen.

Metadaten

Metadaten sind Daten, die Informationen zur Identifizierung, Beschreibung und Beziehungen von Daten bereitstellen. Metadaten verleihen Daten Bedeutung, bieten Kontext, definieren Struktur und ermöglichen systemübergreifende Abrufbarkeit sowie Verwendbarkeit, Authentizität und Überprüfbarkeit über einen längeren Zeitraum hinweg. Bei elektronischen Daten können Teile der Metadaten in Audit Trails erzeugt werden.

Metadaten bilden einen integralen Bestandteil der Daten. Ohne den Kontext, den Metadaten liefern, haben die Daten keine oder nur eine begrenzte Bedeutung. Unvollständige oder fehlende Metadaten verringern die Möglichkeit zur Dateninterpretation.

Audit Trail

Der Audit Trail ist eine Form von Metadaten, die Informationen zu Aktivitäten enthalten, die sich auf die Erstellung, Änderung oder Löschung von elektronischen Daten beziehen. Ein Audit Trail bietet eine automatisierte, sichere Möglichkeit, Lebenszyklusdetails wie Erstellung, Hinzufügung, Löschung oder Änderung von Informationen in einer elektronischen Aufzeichnung zu erfassen, ohne die ursprüngliche Aufzeichnung zu verschleiern oder zu überschreiben. Ein Audit Trail erleichtert die Rekonstruktion der Historie solcher Ereignisse im Zusammenhang mit der Aufzeichnung, einschließlich der Frage im Zusammenhang mit der Aktivität, „Wer hat was, wann und warum gemacht?“.

3.2. Datenstruktur

Daten können unterschiedliche Strukturen haben.

Statisches Format

Ein statisches Aufzeichnungsformat, wie eine Papier- oder elektronische Aufzeichnung, ist ein starres Format und lässt keine Interaktion zwischen dem Benutzer und dem Aufzeichnungsinhalt zu. Beispielsweise sind alle Papieraufzeichnungen statische Aufzeichnungen. Elektronische Aufzeichnungen, die keine Verknüpfung zu anderen Aufzeichnungen enthalten, die eine Interaktion ermöglichen, sind ebenfalls statische Aufzeichnungen. Ein Ausdruck einer einfachen elektronischen Waage, auf der keine elektronischen Daten gespeichert sind, ist ein Beispiel für eine statische Aufzeichnung aus einem elektronischen System.

Dynamisches Format

Aufzeichnungen in einem dynamischen Zustand sind meist elektronische Aufzeichnungen, die eine interaktive Beziehung zwischen dem Benutzer und dem Aufzeichnungsinhalt ermöglichen. Beispiele für ein dynamisches Format sind Chromatografie Daten, die als elektronische Aufzeichnungen gespeichert werden, um es dem Benutzer zu ermöglichen, auf die Basislinie zu zoomen, die Integration klarer darzustellen oder über elektronische Verknüpfungen direkten Zugriff auf die Analysensequenz, die Ergebnistabelle, die Audit Trails und die Erfassungs- und Integrationsmethoden zu haben. Elektronisch signierte Aufzeichnungen sind ebenfalls dynamische Aufzeichnungen, da sie eine Verknüpfung zur Authentifizierung der Signatur enthalten.

Dateistruktur

Die Art und Weise, in der die meisten elektronischen Daten innerhalb der GLP-Umgebung strukturiert sind, hängt davon ab, wofür die Daten verwendet werden. Dem Endnutzer wird dies fast immer durch die verfügbare Software / das computergestützte System vorgegeben.

Flat files

Ein flat file besteht aus einer einzigen Datentabelle, hat keine interne Hierarchie und ermöglicht dem Benutzer, Datenattribute anzugeben, d. h. die Datenstruktur ist in sich eigenständig und begrenzt.

Flat files sind vergleichbar mit Akten in einem Schrank, eine Sammlung einzelner Aufzeichnungen, die jeweils eigenständige Daten enthalten. Das bekannteste flat file ist eine CSV- oder XLS-Datei oder ein reines Microsoft Word™-Textdokument.

Relationale Datenbanken

Relationale Datenbanken sind eine Sammlung von Tabellen, die mithilfe eines gemeinsamen Datenelements, z. B. einer Prüfungsnummer, miteinander verknüpft sind, und können so eingerichtet werden, dass bestimmte Informationen für *Ad-hoc*-Abfragen hervorgehoben werden. Eine relationale Datenbank ist ein skalierbares und abfragefreundliches Werkzeug, mit dem eine Vielzahl von Datentypen erfasst werden kann. Relationale Datenbanken werden normalerweise nicht zum direkten Aufzeichnen von Rohdaten verwendet.

Relationale Datenbanken speichern verschiedene Komponenten der zugehörigen Daten und Metadaten an verschiedenen Orten. Jeder einzelne Eintrag entsteht, und kann wieder abgerufen werden, indem die Daten und Metadaten mit einem Tool zur Datenbank-Berichterstattung zusammengestellt werden.

Elektronische Aufzeichnungen in einem Datenbankformat ermöglichen dem Benutzer beispielsweise die Rückverfolgung, Trendermittlung und Abfrage von Daten.

3.3. Elektronische Signatur

Eine elektronische Signatur ist eine Signatur in digitaler Form, die die handschriftliche („nasse“) Unterschrift repräsentiert.

Es gibt verschiedene Arten von Systemen, von einfachen Systemen (z. B. interne Benutzeridentifikation mit Passwort) bis hin zu komplexen Signatursystemen (z. B. mit einem externen, zertifizierten elektronischen Signaturdienst, der Zeitstempel und

verschlüsselte Informationen hinter der Signatur liefert). Um rechtlich als elektronische Signatur zu gelten, sind nationale Vorschriften zu beachten.

3.4. Datenintegrität

Datenintegrität ist das Maß, in dem Daten vollständig, konsistent, korrekt, vertrauenswürdig und zuverlässig sind und diese Merkmale der Daten während des gesamten Datenlebenszyklus beibehalten werden. Die Gewährleistung der Datenintegrität erfordert geeignete Qualitäts- und Risikomanagementsysteme, einschließlich der Einhaltung fundierter wissenschaftlicher Grundsätze, guter Dokumentationspraktiken und der Schulung des Personals.

3.5. Datenqualität

Die Datenqualität ist die Zusicherung, dass die erzeugten Daten gemäß den geltenden Vorgaben erzeugt wurden und für den beabsichtigten Zweck geeignet sind. Die Datenqualität wird durch ein geeignetes Prüfungsdesign, das die untersuchten experimentellen Fragestellungen und Hypothesen genau und wissenschaftlich untersucht, sowie durch die Verfügbarkeit angemessener Ressourcen sichergestellt. Die Datenqualität beeinflusst den Wert und die allgemeine Akzeptanz der Daten in Bezug auf die Entscheidungsfindung oder die Weiterverwendung.

3.6. Datenlebenszyklus

Der Datenlebenszyklus umfasst alle Phasen der Datenlebensdauer von der Generierung und Aufzeichnung über die Verarbeitung (einschließlich Analyse, Umwandlung oder Migration), Nutzung, Datenaufbewahrung, Archivierung, Wiederauffindbarkeit und Vernichtung.

- Datenfreigabe: Die Datenfreigabe ist die Autorisierung der Daten nach der Erhebung, Verarbeitung oder Überprüfung, um zu dokumentieren, dass die Daten für den vorgesehenen Zweck geeignet sind.
- Abschrift (engl.: „transcriptions“): Bei der Abschrift werden die Daten manuell von einer Quelle in einen anderen aufgezeichneten Datensatz kopiert.

  Eine Abschrift kann auftreten, wenn:

  - dieselben Informationen in verschiedenen Systemen oder Dokumenten erfasst werden (z. B. wird das Eingangsdatum des Prüfgegenstands in mehreren Aufzeichnungen wie Logbüchern oder Formularen erfasst);
  - die Daten zur Berechnung in ein computergestütztes System eingegeben werden. Die Abschrift manueller Aufzeichnungen in ein elektronisches System ist ein Beispiel für ein hybrides System.
- Datenverarbeitung: Bei der Datenverarbeitung handelt es sich um eine Abfolge von Arbeitsschritten, die mit Daten durchgeführt werden, um abgeleitete Daten durch Extraktion darzustellen, zu berechnen und/oder abgeleitete Daten in einem vorgegebenen Format zu erhalten. Beispiele hierfür sind Berechnungen in einer Kalkulationstabelle, statistische Analyse einzelner Prüfsystemdaten zur Darstellung von Trends oder die Umwandlung eines elektronischen Rohsignals in

ein Chromatogramm und anschließendes Berechnen eines numerischen Ergebnisses.

- Datenmigration: Bei der Datenmigration handelt es sich um das Verfahren der Übertragung elektronischer Daten zwischen verschiedenen Datenspeichertypen, computergestützten Systemen oder einfach den Übergang von einem Format in ein anderes. Dies kann eine Änderung des Datenformats umfassen, jedoch nicht des Inhalts oder der Bedeutung, um die Daten auf einem alternativen computergestützten System nutzbar oder sichtbar zu machen.
- Computergestützte Systemtransaktion: Eine computergestützte Systemtransaktion ist ein einzelner Vorgang oder eine Folge von Vorgängen, die als eine einzige logische Arbeitseinheit ausgeführt werden. Die Vorgänge, die eine Transaktion darstellen, müssen erst dann als dauerhafte Aufzeichnung auf einem langlebigen Datenträger gespeichert werden, wenn der Benutzer die Transaktion durch eine bewusste Handlung (z. B. Drücken einer Speichertaste, siehe auch "Datenfreigabe") bestätigt oder wenn das System die Speicherung der Daten erzwingt.
- Datenaufbewahrung: Unter Datenaufbewahrung versteht man die Speicherung bzw. Aufbewahrung von Daten, die zum Zwecke der Archivierung (geschützte Daten zur Langzeitaufbewahrung/-speicherung) oder der Datensicherung (elektronische Daten oder für den Zweck der Wiederherstellung nach Systemausfällen) dienen kann.
- Datensicherung (Backup): Eine Datensicherung ist eine Kopie der aktuellen Daten, Metadaten und Systemkonfigurationseinstellungen, die zum Zwecke der Wiederherstellung einschließlich der Wiederherstellung nach Systemausfällen (Desaster Recovery) aufbewahrt wird.

  Die Datensicherung ermöglicht Vorkehrungen für die Wiederherstellung von Dateien oder Software, für die Wiederaufnahme der Verarbeitung oder für die Verwendung alternativer Computerausrüstung nach einem Systemfehler oder -ausfall.
- Archiv: Als Archiv wird ein Bereich oder eine Einrichtung (z. B. Schrank, Raum, Gebäude oder computergestütztes System) bezeichnet, der bzw. die zur sicheren Aufbewahrung und Erhaltung von Aufzeichnungen und Materialien bestimmt ist.

3.7. Data Governance

Data Governance ist die Summe aller Vorkehrungen, die sicherstellen, dass Daten (unabhängig vom Format, in dem sie erfasst, generiert, aufgezeichnet, verarbeitet, aufbewahrt, archiviert und verwendet werden) während ihres gesamten Lebenszyklus zuschreibbar, lesbar, zeitnah, im Original (oder in geprüfter Kopie), korrekt, vollständig, konsistent, langlebig und verfügbar (ALCOA+) sind.

Diese Vorkehrungen können aus einem einzelnen unabhängigen System oder aus einer Kombination von Systemen innerhalb einer Prüfeinrichtung bestehen.

4. GLP-Verantwortlichkeiten für Daten, von der Generierung bis zur Archivierung

Prüfendes Personal

Das gesamte prüfende Personal (Prüfpersonal) ist verantwortlich für die unverzügliche und genaue Erfassung von Rohdaten in Übereinstimmung mit den Grundsätzen der GLP.

Prüfleiter

Der Prüfleiter hat sicherzustellen, dass:

- alle gewonnenen Rohdaten lückenlos festgehalten und aufgezeichnet werden;
- die im Verlauf einer Prüfung verwendeten computergestützten Systeme validiert sind, einschließlich der Anforderungen an die Datenintegrität, und
- nach Abschluss (einschließlich Abbruch) der Prüfung Prüfplan, Abschlussbericht, Rohdaten und weiteres damit zusammenhängendes Material archiviert werden, sodass alle Materialien, einschließlich der Daten, die für die Rekonstruktion der Prüfung benötigt werden, verfügbar bleiben.

Archivverantwortlicher

Der Archivverantwortliche ist die Einzelperson, die für die Verwaltung, den Betrieb und die Verfahren zur Archivierung in Übereinstimmung mit den GLP Grundsätzen verantwortlich ist, einschließlich der physischen und elektronischen Archivierung von Daten.

Leitung der Prüfeinrichtung

Die Leitung der Prüfeinrichtung (LPE) ist für die Organisation und den Betrieb der Einrichtung verantwortlich, in der Daten generiert werden. Die LPE hat:

- sicherzustellen, dass eine ausreichende Anzahl qualifizierten Personals, geeignete Räumlichkeiten, Ausrüstungen und Materialien vorhanden sind, um die rechtzeitige und korrekte Durchführung der Prüfung zu gewährleisten, einschließlich der Ressourcen zur Gewährleistung der Data Governance;
- sicherzustellen, dass Aufzeichnungen über Aus-, Fort- und Weiterbildung sowie praktische Erfahrung und die Aufgabenbeschreibungen für alle wissenschaftlichen und technischen Mitarbeiter geführt werden;
- sicherzustellen, dass die Mitarbeiter mit den Aufgaben, die sie ausführen sollen, vertraut sind. Falls erforderlich, ist eine Einführung in diese Aufgaben vorzusehen, einschließlich der Aufgaben zur Datenintegrität;
- sicherzustellen, dass angemessene und dem Stand der Technik entsprechende Standardarbeitsanweisungen (SOPs) erstellt und befolgt werden, und hat sämtliche ursprünglichen SOPs sowie deren überarbeitete Versionen zu genehmigen, einschließlich derjenigen, die sich auf das Data Governance-System beziehen;
- sicherzustellen, dass eine verantwortliche Person für die Führung von Archiven, einschließlich der Archivierung von Daten, Papier und elektronischen Dokumenten, bestimmt wird;
- Verfahren einzuführen, die sicherstellen, dass computergestützte Systeme für ihre vorgesehene Anwendung geeignet sind und in Übereinstimmung mit den GLP-

Grundsätzen validiert, betrieben und gewartet werden, einschließlich der Funktionalitäten im Zusammenhang mit der Datenintegrität;

- Systeme umzusetzen, die den aktuellen regulatorischen Anforderungen entsprechen, und
- sicherzustellen, dass Restrisiken im Zusammenhang mit der Datenintegrität ermittelt und gemindert werden.

Qualitätssicherungspersonal

Das Qualitätssicherungspersonal hat Inspektionen durchzuführen, um festzustellen, ob alle Prüfungen unter Einhaltung der GLP-Grundsätzen durchgeführt werden. Dies kann die Datenerhebung, Datenerfassungssysteme sowie umgesetzte Maßnahmen zur Data Governance und zugehörige SOPs umfassen und ist in das QS-Programm der Prüfeinrichtung aufzunehmen.

5. Grundlegende Maßnahmen zur Gewährleistung der Datenintegrität

1. Die LPE hat sicherzustellen, dass die in der Prüfeinrichtung implementierten Systeme Daten erzeugen, die in allen ihren Formen, d. h. auf Papier und elektronisch zuschreibbar, lesbar, zeitnah, original, korrekt, vollständig, konsistent, langlebig und verfügbar sind (ALCOA+). Der Prüfleiter hat sich zu vergewissern, dass die in der Prüfung eingesetzten Systeme für die Integrität von Prüfdaten geeignet sind.
2. Von der LPE wird die Umsetzung eines vollständig dokumentierten und von begründeten Erläuterungen flankierten Systems erwartet, welches einen akzeptablen Kontrollzustand auf der Grundlage des Datenintegritätsrisikos ermöglicht. Ein geeigneter Ansatz besteht beispielsweise darin, eine Risikobewertung für die Datenintegrität durchzuführen, bei der die Verfahren, die Daten erzeugen, verarbeiten und/oder speichern, abgebildet und jedes der Formate und ihre Kontrollen identifiziert sowie die Datenkritikalität, inhärente Risiken und geeignete Risikominderungsmaßnahmen dokumentiert werden. Andere dokumentierte Ansätze zur Identifizierung und Kontrolle von Risiken für die Datenintegrität können akzeptabel sein.
3. Die innerhalb der Prüfeinrichtung getroffenen organisatorischen und personellen Vorkehrungen sowie Systeme und Einrichtungen sind so zu konzipieren, umzusetzen und gegebenenfalls anzupassen, dass sie ein geeignetes Arbeitsumfeld unterstützen, d. h. ein geeignetes Umfeld für das Funktionieren wirksamer Kontrollen der Datenintegrität ermöglichen.
4. Data Governance muss während des gesamten Datenlebenszyklus angewendet werden, um die Datenintegrität zu gewährleisten. Die Data Governance hat sich mit dem Dateneigentum und der -verantwortlichkeit zu befassen sowie die Konzeption, den Betrieb und die Überwachung von Verfahren/Systemen zu berücksichtigen, um die Anforderungen an die Datenintegrität, einschließlich der Kontrolle über alle Datenänderungen, zu erfüllen. Die Data Governance-Systeme haben auch zu gewährleisten, dass die Daten leicht verfügbar und zugänglich sind. Elektronische Daten haben in einer für den Menschen lesbaren Form vorzuliegen.

5. Im Rahmen der Data Governance müssen Risikomanagementtechniken verwendet werden, um Risiken für Datenintegritätsfehler in den Systemen der Prüfeinrichtung zu erkennen, sowie das potenzielle Risiko für die Datenintegrität zu minimieren und Restrisiken zu identifizieren. Ansätze für die Verwaltung von Data Governance (z. B. SOPs) sind stets von der LPE zu genehmigen. Die Wirksamkeit des Data Governance-Ansatzes ist regelmäßig, wie von der LPE festgelegt, zu überwachen und zu bewerten.
6. Von der LPE wird erwartet, dass angemessene Ressourcen und die Durchführung von Schulungen sichergestellt werden. Die Data Governance-Systeme müssen auch Personalschulungen mit dem Schwerpunkt auf Datenintegritätskonzepten beinhalten, und ein Arbeitsumfeld schaffen, das Transparenz ermöglicht und aktiv die Meldung von Fehlern, Versäumnissen und abweichenden Ergebnissen fördert.
7. Die Risiken für Daten spiegeln sich in ihrem Potenzial wider, entweder unbeabsichtigt oder absichtlich gelöscht, ergänzt, verändert oder ausgeschlossen zu werden, ohne dass eine Autorisierung hierfür vorliegt oder ohne die Möglichkeit, solche Tätigkeiten und Ereignisse erkennen zu können. Die Risiken für Daten können durch komplexe, inkonsistente oder fehlende Verfahren, deren Ergebnisse offen oder subjektiv sind, erhöht werden. Einfache, klar definierte Arbeitsabläufe, die konsequent durchgeführt werden und ein klares Ziel verfolgen, sind einzuführen, um solche Risiken zu mindern.
8. Eine Risikobewertung der Datenintegrität (oder ein gleichwertiges Verfahren) hat alle Faktoren zu berücksichtigen, die zur Durchführung eines Verfahrens oder einer Tätigkeit erforderlich sind. Die LPE hat Personal für die Durchführung der Risikobewertung zu benennen, und es wird empfohlen, dass diese von einem multidisziplinären Team durchgeführt wird, das Fachexperten mit Kenntnissen über das Verfahren, Prüfleiter, Spezialisten für Informationstechnologie (IT), Qualitätssicherung und alle anderen relevanten Funktionen einschließen kann. Es wird erwartet, dass nicht nur das System isoliert betrachtet wird, sondern auch alle unterstützenden Tätigkeiten und Funktionen einbezogen werden, wie Vorschriften, Verfahren, Schnittstellen zu anderen Systemen, menschliches Eingreifen, Schulungen und Qualitätssysteme. Automatisierung oder die Verwendung eines validierten Systems kann das Risiko für die Datenintegrität verringern, aber nicht beseitigen. Durch menschliches Eingreifen in das System, insbesondere bei der Beeinflussung der Art und Weise, wie oder welche Daten aufgezeichnet oder berichtet werden, kann ein erhöhtes Risiko durch unzureichende organisatorische Kontrollen oder unzureichende Datenüberprüfung entstehen, bedingt durch ein übermäßiges Vertrauen in den validierten Zustand des Systems.
9. Hat die Risikobewertung der Datenintegrität (oder ein gleichwertiges Verfahren) Bereiche mit Handlungsbedarf aufgezeigt, so hat das benannte Team (gemäß Ziffer 8.) die Priorisierung der Maßnahmen, einschließlich der Akzeptanz eines angemessenen Restrisikos, zu dokumentieren und der LPE zur Genehmigung vorzulegen. Die Risikobewertung ist regelmäßig zu überprüfen, um die durchgeführten Maßnahmen und mögliche Änderungen der Verfahren zu berücksichtigen. In Situationen, in denen nur langfristig umzusetzende Korrekturmaßnahmen identifiziert wurden, sind risikomindernde kurzfristige Maßnahmen zu ermitteln, zu dokumentieren, der LPE zur Genehmigung zu übermitteln und umzusetzen, um ein akzeptables Maß an Kontrolle der Data Governance zu gewährleisten, bis eine dauerhaftere Lösung umgesetzt ist.

10. Für Regulatorische Entscheidungen müssen die Prüfdaten maßgeblich und zuverlässig sein. Die Datenkritikalität kann bestimmt werden, indem berücksichtigt wird, wie sich die Daten auf die Zielsetzung, die Validität und die Einhaltung der GLP-Grundsätze einer Prüfung auswirken.
11. Der Aufwand und die Ressourcen zur Gewährleistung der Datenintegrität müssen in einem angemessenen Verhältnis zum Risiko und zu den Auswirkungen eines Datenintegritätsverlustes stehen.
12. Prüfeinrichtungen müssen sich darüber im Klaren sein, dass geeignete Kontrollen der Datenintegrität sowohl für computergestützte Systeme als auch für manuelle Systeme auf Papierbasis erforderlich sind, auch wenn die Kontrollen möglicherweise nicht dieselben sind. Hybridsysteme können verwendet werden, wenn ihre Fähigkeit, die Datenintegrität zu gewährleisten, nachgewiesen ist (siehe auch Abschnitt 7.3 "Überprüfung von Daten aus Hybridsystemen").

6. Anforderungen an die Datenintegrität während des gesamten Datenlebenszyklus

6.1. Allgemeine Anforderungen an Daten

Prüfeinrichtungen müssen über ein angemessenes Verfahrensverständnis und technische Kenntnisse der für die Datenaufzeichnung verwendeten Systeme verfügen, einschließlich deren Fähigkeiten, Einschränkungen und Schwachstellen.

Die Bereitstellung eines Arbeitsumfelds, welches die Durchführung von Aufgaben und die Aufzeichnung von Daten wie erforderlich ermöglicht, ist unerlässlich. Dazu gehören beispielsweise angemessene räumliche Gegebenheiten, ausreichend Zeit für die Aufgabenerfüllung und ordnungsgemäß funktionierende Geräte.

Die folgenden Anforderungen gelten für alle Daten.

Die Daten müssen:

A (attributable) - der Person zuschreibbar sein, die die Daten erstellt/ verändert/überprüft hat

L (legible) - lesbar

C (contemporaneous) - zeitnah

O (original) - Original (oder überprüfte Kopie davon)

A (accurate) - korrekt

sein.

Maßnahmen zur Data Governance müssen auch sicherstellen, dass die Daten während des gesamten Lebenszyklus vollständig, konsistent, langlebig und verfügbar sind (ALCOA+), wobei:

Vollständig (complete) - die Daten müssen vollständig sein / ein vollständiger Datensatz

Konsistent (consistent)	- die Daten müssen in sich konsistent und frei von Selbstwidersprüchen sein
Dauerhaft (enduring)	- langlebig, über den gesamten Datenlebenszyklus hinweg
Verfügbar (available)	- ohne weiteres verfügbar

Generierte Daten müssen dem Zeitpunkt der Erfassung und der für die Dateneingabe verantwortlichen Person zuschreibbar sein (Metadaten).

Die Konzeption computergestützter Systeme hat stets die vollständige Aufbewahrung von Audit Trails vorzusehen, um alle Datenänderungen anzuzeigen, ohne dass die ursprünglichen Aufzeichnungen unkenntlich gemacht werden. Es muss möglich sein, alle Datenänderungen der Person, die diese Änderungen vorgenommen hat, einschließlich dem Zeitpunkt, an dem sie vorgenommen wurden, zuzuordnen z. B. durch Verwendung eines Audit Trails oder gleichwertiger Mechanismen oder durch Zeitpunkt und Datum zugeordnete (elektronische) Signaturen. Die Änderungen sind zu begründen.

6.2. Erzeugung, Erfassung oder Aufzeichnung von Rohdaten

Die während der Prüfungsdurchführung anfallenden Rohdaten sind unmittelbar, unverzüglich, leserlich und genau aufzuzeichnen. Sämtliche Rohdaten sind abzuzeichnen und zu datieren, entweder elektronisch oder auf Papier oder auf anderen Medien. Wenn Rohdaten durch direkte Computereingabe erzeugt werden (z. B. durch Eingabe eines Wertes), sind die Rohdaten durch die Identität der für die Aufzeichnung verantwortlichen Person und durch den Zeitpunkt der Eingabe zu kennzeichnen.

Werden die ursprünglich erfassten elektronischen Daten nicht als Rohdaten betrachtet, so muss dies begründet und dokumentiert werden.

Manuelle Aufzeichnung

Manuell aufgezeichnete Daten erfordern möglicherweise eine unabhängige Überprüfung auf der Grundlage einer Risikobewertung für die Datenintegrität oder anderer Anforderungen. Beispiele hierfür können die zeitgleiche (oder zeitnahe) Überprüfung der Dateneingabe durch eine zweite Person oder ein Abgleich verwandter Informationsquellen (z. B. Gerätelogbücher, Prüfsystemdaten usw.) oder eine Datenüberprüfung sein. Das Kontrollniveau hat dem festgestellten Fehlerrisiko bei der manuellen Aufzeichnung zu entsprechen.

Beobachtungen, deren manuelle Dokumentation vorgesehen ist, sind vom entsprechend geschulten Beobachter (i. d. R. prüfendes Personal) unverzüglich und simultan aufzuzeichnen. Bestehen außergewöhnliche Erfordernisse, manuelle Beobachtungen zu bestätigen (z. B. aufgrund der hohen Kritikalität hinsichtlich der Validität der Prüfung), dann können zusätzliche Aktivitäten in Betracht gezogen werden, um die Integrität der Daten zu belegen (z. B. Bildaufzeichnung oder Anwesenheit eines Zeugen zur Bestätigung der Beobachtung). Über die vom Beobachter und gegebenenfalls von einem Zeugen durchgeführten zusätzlichen Tätigkeiten sind Aufzeichnungen als zusätzliche Daten mit den vom Beobachter aufgezeichneten Rohdaten zu führen.

In begründeten Fällen kann beispielsweise der Einsatz von Protokollanten in Betracht gezogen werden, die im Auftrag des Anderen simultan die Aufzeichnungen vornehmen, beispielsweise:

- Der Vorgang der gleichzeitigen Aufzeichnung beeinträchtigt die durchzuführende Tätigkeit (z. B. Dokumentation der Prüfgegenstandsvorbereitung unter sterilen Bedingungen durch das prüfende Personal).
- Untersuchungen der Prüfsysteme während einer kritischen Phase.

Aufzeichnungen durch die zweite Person haben zeitgleich mit der ausgeführten Aufgabe zu erfolgen. In den Aufzeichnungen sind sowohl das prüfende Personal, das die Aufgabe ausführt, als auch die Person, die die Aufzeichnungen dazu anfertigt, anzugeben. Das ausführende prüfende Personal hat die Aufzeichnung nach Möglichkeit gegenzuzeichnen, um die Tatsache, dass es die Tätigkeit ausgeführt hat, zu formalisieren (nicht die Akzeptanz der aufgezeichneten Daten). Das Verfahren zur Vervollständigung der Dokumentation bei der Verwendung eines Protokollanten muss in einer SOP beschrieben werden, in der auch die Tätigkeiten anzugeben sind, auf die das Verfahren angewendet wird

Der Zugriff auf die aktuelle Version der Vorlagen oder Formulare, die zur Aufzeichnung der Rohdaten verwendet werden, muss an den Orten gegeben sein, an denen Tätigkeiten stattfinden, damit die Daten umgehend aufgezeichnet werden können. Die Anzahl der verwendeten Vorlagen (oder Formulare) ist gegen die Anzahl ausgegebenen Kopien (dieser Vorlagen/Formulare) zu kontrollieren, um Vervielfältigungen zu verhindern und die Identifizierung von Datenintegritätsproblemen zu unterstützen, wie etwa die Erkennung einer Neuerstellung oder Abschrift eines Datensatzes. Wenn Vorlagen oder Formulare zum Aufzeichnen von Daten durch Drucken verfügbar sind, ist die Anzahl der Ausdrucke zu kontrollieren.

Das erforderliche Maß an Kontrolle ist durch eine Risikobewertung zu ermitteln. Bei Fehlen einer vollständigen Kontrolle und eines Abgleichs ist durch eine Risikobewertung begründet darzulegen, warum einige Situationen von dieser Anforderung ausgenommen sind.

Die Verwendung von Blanko-Papierformularen für die Aufzeichnung von Rohdaten muss begrenzt und kontrolliert werden, hat aber auch zur Verfügung zu stehen, um die zeitgleiche Aufzeichnung unerwarteter Ereignisse zu ermöglichen. Der Mengenabgleich zwischen den ausgegebenen und ausgefüllten (Blanko-)Formularen ist für alle verwendeten Formulare durchzuführen. Die Verwendung von paginierten Büchern kann eine geeignete Lösung sein, so dass das Entfernen von Seiten erkannt werden kann. Das erforderliche Maß an Kontrolle ist durch eine Risikoanalyse zu ermitteln, und das Fehlen einer vollständigen Kontrolle und eines Abgleichs ist zu begründen.

Gleichwohl hat das zur Kontrolle des Formularzugriffs eingerichtete System die einfache Verfügbarkeit des richtigen Dokuments zu ermöglichen, um die mögliche Verwendung unsachgemäßer Aufzeichnungen auf nicht genehmigten Formularen und jede nachfolgende Abschrift zu vermeiden.

Als direkte Computereingabe erzeugte Daten müssen dem Zeitpunkt der Dateneingabe und der/den für die direkte Dateneingabe verantwortliche(n) Person(en) zuschreibbar sein.

Bei elektronischen Daten dürfen die Zugriffsmöglichkeiten auf die Anwendungen nicht die zeitnahe Aufzeichnung der Daten behindern. Benutzerzugriffsrechte müssen unbefugte Dateneingaben verhindern.

Automatische Aufzeichnung

Externe Geräte oder Systemschnittstellen, die manuelle Dateneingaben und die menschliche Interaktion mit dem computergestützten System ersetzen, wie Barcodescanner, ID-Kartenleser oder Drucker, können verwendet werden, wenn sie validiert sind.

Die Risiken im Zusammenhang mit der Datenintegrität können davon abhängen, inwieweit Geräte oder computergestützte Systeme, die Daten automatisch erfassen, aufzeichnen oder generieren, konfiguriert und validiert werden können, sowie vom Potenzial der Manipulation oder des Datenverlustes innerhalb des Systems.

Hybridsysteme

Bei einfachen elektronischen Geräten, die keine elektronischen Daten speichern oder nur eine gedruckte Datenausgabe bieten (z. B. bestimmte Waagen oder pH-Meter), kann der Papierausdruck die Rohdaten darstellen.

Wenn elektronische Geräte zwar elektronische Daten speichern, aber nur ein bestimmtes Datenvolumen vorhalten, bevor diese wieder überschrieben werden, sind alle Anstrengungen zu unternehmen, um die Daten und Metadaten als elektronische Daten zu extrahieren und zu kontrollieren. Das Ausdrucken auf Papier, wenn es sofort unterschrieben und datiert wird, oder die Umwandlung in ein anderes Format ist akzeptabel, wenn dabei keine Informationen verloren gehen. Daten (einschließlich Metadaten) in ihrem Aufbewahrungsformat müssen vor der Löschung aus elektronischen Geräten überprüft werden.

Andere Medien

Daten können mittels Fotografie oder Bildgebungsverfahren und -technologien (oder anderer Medien) erfasst werden. Die Anforderungen an die Rückverfolgbarkeit der Aufzeichnung bleiben dieselben.

Aufzeichnung in flat files

Die meisten flat files erlauben keine Rückverfolgbarkeit der Identität der Person, die die Daten aufzeichnet, sowie des Datums und der Uhrzeit der Aufzeichnung. Einige flat files enthalten möglicherweise grundlegende Metadaten zur Dateierstellung sowie zum Datum der letzten Änderung, bieten jedoch keinen ausreichenden Audit-Trail. Flat files sind grundsätzlich nicht zur direkten Datenerfassung oder zur Speicherung von Rohdaten zu verwenden.

Wenn die Verwendung von flat files erforderlich ist und die Datenverwaltung nicht durch eine alternative Methode erreicht werden kann, so müssen Risikominderungsmaßnahmen festgelegt werden, die die Verwendung solcher Dateien berücksichtigen. Zu den möglichen Abhilfemaßnahmen gehören beispielsweise Verschlüsselung, Zugriffskontrollen auf den Dokumentenspeicherort oder technische Sicherheitsvorkehrungen, die Änderungen an der Datei außerhalb der ursprünglichen Software erkennen können.

6.3. Metadaten

Für die volle Aussagekraft von Rohdaten sind Metadaten erforderlich und müssen als Teil der Daten betrachtet werden (siehe auch Abschnitt 6.13 "Daten Audit-Trail").

Metadaten müssen zeitgleich mit den zugehörigen Daten erzeugt und gemeinsam mit ihnen aufbewahrt werden.

6.4. Elektronische Signatur

Eine elektronische Signatur muss der handschriftlichen Signatur des Unterzeichnenden gleichwertig sein und kann verwendet werden, um die Genehmigung, Autorisierung oder Überprüfung bestimmter Dateneinträge zu bestätigen.

Um die Datenintegrität zu gewährleisten, muss die Verwendung elektronischer Signaturen angemessen kontrolliert werden, wobei Folgendes zu berücksichtigen ist:

- die Zuschreibbarkeit der Unterschrift zu einer Person und zu dem Zweck, für den sie verwendet wird (z. B. Genehmigung, Überprüfung, Bestätigung);
- wie die Unterschrift im System aufgezeichnet wird, damit sie nicht verändert oder manipuliert werden kann, ohne dass die Unterschrift oder der Status des Eintrags ungültig gemacht wird;
- wie Uhrzeit und Datum der Unterschrift zusammen mit dem Namen des Eigentümers und der Bedeutung der Unterschrift aufgezeichnet werden;
- wie die Aufzeichnung der Signatur mit der Eintragung verknüpft wird und wie dies überprüft werden kann; und
- wie die Sicherheit der elektronischen Signatur gewährleistet wird, d. h. wie sichergestellt wird, dass diese nur vom Inhaber der Signatur angewendet werden kann.

Ein eingefügtes Bild einer Unterschrift oder eine Fußnote, aus der hervorgeht, dass das Dokument elektronisch unterzeichnet wurde (sofern dies nicht mit dem validierten Verfahren der elektronischen Signatur erfolgt ist), reichen nicht aus.

Wenn in Verbindung mit einer elektronischen Signaturfunktion eine herkömmliche Authentifizierung, bestehend aus einer Benutzer-ID und einem geheimen Passwort, durch eine biometrische Authentifizierung (z. B. Fingerabdruck, Hand-, Gesicht- oder Irisscanner) ersetzt wird, muss die umgesetzte Lösung gründlich validiert und dokumentiert werden.

(Siehe auch Abschnitt 3.9 des OECD-Dokuments Nr. 17 (OECD, *2016* [4]*))*

6.5. Erstellung überprüfter Kopien

Eine überprüfte (verifizierte) Kopie von Daten (unabhängig von der Art des verwendeten Mediums) muss nachweislich (d. h. mit datierter Signatur oder durch Generierung mittels eines validierten Verfahrens), dieselben Informationen wie das Original enthalten, einschließlich der Daten, die den Kontext, den Inhalt und die Struktur beschreiben. Original und überprüfte Kopien müssen die Integrität (Genauigkeit, Vollständigkeit, Inhalt und Bedeutung) der Daten wahren.

Die Überprüfung, dass es sich um eine Kopie vom Original handelt, muss der Person zugeordnet werden können, die diese durchführt. Das Datum (und die Uhrzeit, falls relevant) der Erstellung der überprüften Kopie müssen zusammen mit der betreffenden Kopie aufbewahrt werden.

Eine elektronische überprüfte Kopie der in Papierform aufgezeichneten Daten kann erstellt werden, sofern ein dokumentiertes Verfahren vorhanden ist, das sicherstellt, dass es sich bei dem Ergebnis um eine überprüfte Kopie handelt.

6.6. Berichtigung oder Änderung von Daten

Jede Änderung der Rohdaten muss so vorgenommen werden, dass der vorherige Eintrag nicht überschrieben wird, der Grund für die Änderung muss angeben werden und sie muss datiert und von der Person, die die Änderung vornimmt, signiert oder abgezeichnet werden.

Bei Daten, die als direkte Computereingabe generiert werden, muss das Design des computergestützten Systems stets die Aufbewahrung vollständiger Audit Trails vorsehen, um alle Datenänderungen aufzuzeigen, ohne dass der ursprüngliche Datensatz überschrieben wird. Es muss möglich sein, alle Datenänderungen den Personen zuzuordnen, die diese Änderungen vorgenommen haben, beispielsweise durch Verwendung von mit Zeit und Datum versehenen (elektronischen) Signaturen (siehe auch Abschnitt 6.13 "Daten-Audit Trail"). Gründe für Änderungen sind anzugeben und aufzuzeichnen.

6.7. Abschrift

Abschriften (engl.: „transcriptions“) sind zu vermeiden, da sie das Risiko von Fehlern und Unstimmigkeiten erhöhen. Können Abschriften nicht vermieden werden, so sind diese von einer zweiten Person zu überprüfen oder durch ein validiertes System vorzunehmen. Die ursprünglichen Aufzeichnungen sind als Rohdaten zu betrachten und sind aufzubewahren.

6.8. Ungültigerklärung oder Ausschließen von Daten

Daten dürfen nur dann für ungültig erklärt oder ausgeschlossen werden, wenn durch fundierte wissenschaftliche oder technische Begründungen oder logisches Verständnis nachgewiesen werden kann, dass die Daten für das aufgezeichnete Ereignis nicht repräsentativ sind. Beispiele hierfür sind z. B. das Verwerfen von Analyseergebnissen aufgrund einer Gerätefehlfunktionen oder der Ausschluss einer klinischen Beobachtung, die an einem toten Tier durchgeführt wurde.

Untersuchungen zur Ermittlung der Ursache für die Erzeugung von ungültig zu erklärenden oder auszuschließenden Daten sind unerlässlich. In allen Fällen muss die Begründung der Ungültigerklärung oder des Ausschlusses dokumentiert und bei der Datenüberprüfung und -berichterstattung berücksichtigt werden. Für gängige Fälle (z. B. inkohärente Analyseergebnisse für eine einzelne Probe oder Nichterfüllung der Akzeptanzkriterien) sind die Regeln für den Ausschluss oder die Ungültigerklärung von Daten vorab im Prüfplan oder in Standardarbeitsanweisungen festzulegen. Alle Daten (selbst wenn sie für ungültig erklärt werden) müssen zusammen mit dem Datensatz aufbewahrt werden und in einem Format zur Überprüfung verfügbar sein, welches es ermöglicht, die Stichhaltigkeit der Entscheidung zur Ungültigerklärung oder zum Ausschluss der Daten zu bestätigen.

6.9. Datenverarbeitung

Benutzerdefinierte Parameter im Rahmen der Datenverarbeitungstätigkeiten müssen angemessen rückverfolgbar sein, einschließlich der Zuordnung zu der Person, die die Tätigkeit ausgeführt hat. Beispiele hierfür sind Berechnungen oder (mit entsprechenden Zugriffsberechtigungen) die Auswahl und Anwendung von Chromatografie-

Integrationsparametern oder die Auswahl von Gating-Parametern für die Analyse eines Durchflusszytometrie-Tests. Die Regeln für die Verarbeitung von Daten müssen klar definiert sein und durch SOPs geregelt werden.

Die Rohdaten und verfügbaren Audit Trails des Verfahrens müssen aufbewahrt werden. Die aufbewahrten Aufzeichnungen müssen eine Rekonstruktion aller Tätigkeiten zur Datenverarbeitung ermöglichen, unabhängig davon, ob das Ergebnis dieser Verarbeitung anschließend berichtet wird. Wurde die Datenverarbeitung mit schrittweiser Änderung der Verarbeitungsparameter wiederholt, so muss dies mit dokumentierter Begründung ersichtlich sein, um sicherzustellen, dass die Verarbeitungsparameter nicht manipuliert werden, um einen wünschenswerteren Endpunkt zu erreichen.

6.10. Datenmigration

Datenmigrationsverfahren müssen eine Begründung enthalten und solide konzipiert und validiert sein, um sicherzustellen, dass die Datenintegrität während des gesamten Datenlebenszyklus erhalten bleibt. Sorgfältige Überlegungen zum Verständnis des Datenformats und des Potenzials für Änderungen in jeder Phase der Datengenerierung, -migration und anschließenden -speicherung sind erforderlich. Maßnahmen, die sicherstellen und nachweisen, dass die Daten während der einzelnen Schritte nicht verändert werden, müssen vorhanden sein.

Die Herausforderungen der Datenmigration werden häufig unterschätzt, insbesondere was die Aufrechterhaltung der vollen Bedeutung und Integrität der Aufzeichnungen, einschließlich der zugehörigen Metadaten, betrifft.

Im Falle einer Migration von einem Beteiligten (dem "Absender") zu einem anderen (dem "Empfänger") sind die Daten und die zugehörigen Metadaten, Datum/Uhrzeit der Migration, erwartetes Format und Spezifikation in Form eines Transferprotokolls oder einer Vereinbarung, das bzw. die zur Migration der Daten verwendet wird, vor der Migration festzulegen. Es müssen Kommunikations- und Koordinierungsmechanismen zwischen dem Absender und dem Empfänger vorhanden sein, die sicherstellen, dass die empfangenen Daten dieselben Attribute aufweisen wie die gesendeten Daten.

(Siehe auch Abschnitt 2.8 des OECD-Dokuments Nr. 17 (OECD, *2016* [4]*))*

6.11. Relationale Datenbanken

Zum Abrufen von Informationen aus einer relationalen Datenbank ist ein Datenbank-Berichterstellungswerkzeug oder die ursprüngliche Anwendung erforderlich, die den Datensatz erstellt hat.

Änderungen an Daten dürfen nicht direkt in den Datenbankfeldern vorgenommen werden, sondern müssen über das Softwarepaket erfolgen, mit dem sie ursprünglich erfasst wurden, so dass entsprechende Audit Trail-Einträge und Kontrollen bestehen bleiben. Wenn dennoch eine Datenänderung durch einen Systemadministrator direkt in der Datenbank erforderlich ist, muss dies begründet, kontrolliert, dokumentiert, vom Prüfleiter genehmigt und das Verfahren in einer Standardarbeitsanweisung beschrieben werden.

Die Zugriffsrechte für die Datenbankeingabe oder -änderung müssen kontrolliert sein und mit den Anforderungen für den Zugriff von Nutzern des computergestützten Systems/Systemadministratorenrollen übereinstimmen (siehe auch Abschnitt 8.2 "Zugriff auf computergestützte Systeme und Benutzerrollen").

6.12. Transaktionen im computergestützten System

Eine Transaktion in einem computergestützten System, bei der ein Parameter innerhalb einer bestimmten Grenze, eines bestimmten Bereichs oder einer bestimmten Verteilung liegen muss, um die Qualität der Daten sicherzustellen, ist als kritisch zu betrachten. Computersysteme müssen so konzipiert sein, dass die Ausführung solcher Transaktionen zeitgleich aufgezeichnet wird. Werden Transaktionssysteme verwendet, so sind Kombinationen mehrerer Einzelvorgänge zu einer kombinierten einzigen Transaktion zu vermeiden (z. B. Mehrfacheingabe von Daten vor dem Speichern), und die Zeitintervalle vor dem Speichern von Daten sind zu minimieren. Systeme müssen so konzipiert sein, dass sie das Speichern von Daten im Langzeitspeicher vorschreiben, bevor Benutzer Änderungen veranlassen können. Ausnahmen von diesen Anforderungen müssen begründet werden.

Die LPE muss bei der Entwicklung des Systems (z. B. über die Spezifikation der Benutzeranforderungen) definieren, welche kritischen Transaktionen mit diesem System verbunden sind, basierend auf der Funktionalität und dem mit dem System verbundenen Risikograd. Kritische Transaktionen müssen mit Verfahrenskontrollen dokumentiert werden, die das Systemdesign (Prävention) berücksichtigen, zusammen mit Überwachungs- und Überprüfungsverfahren. Die Überwachung der Tätigkeiten muss auf Fehler aufmerksam machen, die nicht durch das Verfahrensdesign abgedeckt sind. Die Überwachungstätigkeiten im Zusammenhang mit kritischen Transaktionen sind als Teil des Qualitätssicherungsprogramms zu betrachten.

6.13. Daten Audit Trail

Werden computergestützte Systeme verwendet, um Daten elektronisch zu erfassen, verarbeiten, ändern, berichten, speichern oder archivieren, so muss die Systemkonzeption stets die Aufbewahrung von Audit Trails vorsehen, um alle Änderungen oder Löschungen der Daten unter Beibehaltung früherer Daten aufzuzeigen. Es muss möglich sein, alle Daten und Datenänderungen den Personen zuzuordnen, die diese Änderungen vorgenommen haben, und die Änderungen müssen datiert und mit einem Zeitstempel versehen sein (Zeit und gegebenenfalls auch Zeitzone). Der Grund für die Änderung muss ebenfalls aufgezeichnet werden. Der Audit Trail muss jene Elemente umfassen, die für die vollständige Rekonstruktion des Verfahrens oder der Tätigkeit relevant sind.

Audit Trails müssen während GLP-Tätigkeiten immer eingeschaltet sein. Mitarbeiter mit einem unmittelbaren Interesse an den Daten (Prüfleiter, Leiter analytischer Abteilungen, prüfendes Personal usw.) dürfen nicht in der Lage sein, die Funktion des Audit Trails zu ändern oder abzuschalten. Ändert ein Systemadministrator die Funktion des Audit Trails oder schaltet diesen aus, so muss der Audit Trail dies automatisch erfassen. Dasselbe gilt, wenn die Funktion des Audit Trails wieder eingeschaltet wird.

Wenn keine entsprechenden Audit Trail Funktionen vorhanden sind oder die Systeme die Erwartungen an Audit Trails und individuelle Benutzerkonten (z. B. bei Altsystemen) nicht erfüllen, so müssen nachweisliche Maßnahmen zur Behebung dieser Mängel ergriffen werden. Dies muss entweder durch eine Add-on-Software erfolgen, die diese zusätzlichen Funktionen bereitstellt, oder durch ein Upgrade auf ein kompatibles System. Abhilfemaßnahmen müssen identifiziert und zeitnah umgesetzt werden.

Verfügt ein System nicht über Audit Trail-Fähigkeiten und kann bei der Überprüfung verfügbarer Systeme keine Alternativen und technische Anpassungen oder Ergänzungen

des bestehenden Systems festgestellt werden (d. h. eine Behebung ist nicht möglich), so muss dies durch den Nachweis gerechtfertigt werden, dass (bereits) eine konforme Lösung erarbeitet wird und welche Risikominderungsmaßnahmen, z. B. in Form einer alternativen Kontrollebene, vorübergehend die weitere Verwendung unterstützen. Alternative Kontrollebenen lassen sich beispielsweise durch die Verwendung manueller Logbücher oder die Festlegung streng beschränkter Zugangsrechte zum System erreichen. Das Ausdrucken der Daten kann ebenfalls in Betracht bezogen werden, wenn die Integrität der Daten, einschließlich der Metadaten, gewährleistet ist. Alternative Kontrollmaßnahmen müssen sich als wirksam erweisen, risikobasiert sein, in einer SOP definiert und regelmäßig zur Neubewertung überprüft werden.

Einige GLP-Überwachungsbehörden akzeptieren möglicherweise keine Systeme ohne Audit Trail-Funktionen, einschließlich der Systeme mit alternativen Kontrollmaßnahmen. *(Siehe auch Abschnitt 3.4 des OECD-Dokuments Nr. 17 (OECD, 2016 [4]))*

6.14. Datenaufbewahrung

Die Daten, die für die vollständige Rekonstruktion von Prüfungen erforderlich sind, müssen gesammelt und aufbewahrt werden. Die Daten müssen, wo anwendbar, zusammen mit den zugehörigen Metadaten aufbewahrt werden. Abgeleitete Daten müssen zusammen mit ihren Rohdaten aufbewahrt werden, wenn dies für die Rekonstruktion der Prüfung erforderlich ist.

Regelungen zur Aufbewahrung von Daten und Dokumenten müssen den Schutz der Aufzeichnungen vor beabsichtigter oder unbeabsichtigter Veränderung oder Verlust gewährleisten. Es müssen verlässliche Kontrollen vorhanden sein, um die Datenintegrität der Aufzeichnungen während des gesamten Aufbewahrungszeitraums sicherzustellen.

Die gewählte Methode zur Aufbewahrung muss sicherstellen, dass Daten von angemessener Korrektheit, Vollständigkeit, Inhalt und Bedeutung gesammelt und für den vorgesehenen Zweck aufbewahrt werden.

Aufbewahrung dynamischer Daten

Informationen, die in einem dynamischen Zustand erfasst werden, müssen in diesem Zustand verfügbar bleiben. Videoaufzeichnungen, die zum Nachweis einer Tätigkeit verwendet werden, können beispielsweise nicht auf ein einzelnes statisches Bild oder eine Reihe von Einzelbildern reduziert werden.

Computergestützte Systeme, die dynamische Aufzeichnungen erzeugen, müssen es ermöglichen, den dynamischen Charakter der Daten beizubehalten.

Es kann eine Herausforderung sein, dynamische Aufzeichnungen auf Papier zu drucken, ohne die interaktive Beziehung zwischen dem Benutzer und dem Inhalt der Aufzeichnung zu verlieren.

Ausdrucke müssen sämtliche zugehörigen verfügbaren Metadaten enthalten und den Verweis zu den Rohdaten beibehalten. Werden beispielsweise die zugehörigen Metadaten auf einer anderen Seite als die Rohdaten gedruckt, ist die Integrität des Verweises nicht gewährleistet und die Beziehung zu den Rohdaten fragwürdig.

Wenn elektronische Rohdaten nicht ohne Informationsverlust (z. B. zugehörige Metadaten) in überprüfte Kopien (z. B. in Ausdrucke auf Papier oder PDF) umgewandelt werden können, so müssen sie im Originalzustand verfügbar bleiben.

Kann das computergestützte System nicht aufrechterhalten werden, z. B. wenn es nicht mehr unterstützt wird, dann müssen die Aufzeichnungen gemäß einer dokumentierten Archivierungsstrategie archiviert werden, bevor das computergestützte System außer Betrieb genommen wird. Es ist denkbar, dass einige (dynamisch) elektronisch generierte Daten in einem angemessenen (statischen) Papier- oder elektronischen Format aufbewahrt werden, wenn begründet werden kann, dass eine statische Aufzeichnung die Integrität der Rohdaten bewahrt. Das Datenaufbewahrungsverfahren muss jedoch nachweislich überprüfte Kopien aller Rohdaten, Metadaten, relevanten Audit Trails und Ergebnisdateien, jegliche variablen Software-/Systemkonfigurationseinstellungen, die für die einzelnen Aufzeichnungen spezifisch sind, und alle Datenverarbeitungszyklen (einschließlich Methoden und Audit Trails) umfassen, die für die Rekonstruktion eines bestimmten Rohdatensatzes erforderlich sind.

Wenn der Ausdruck auf Papier als Lösung gewählt wird, bedarf es eines validierten Prozesses, um sicherzustellen, dass die gedruckten Aufzeichnungen eine genaue Darstellung des Datensatzes sind.

Sämtliche Informationen sind aufzubewahren. Jeder Informationsverlust muss festgestellt und das Risiko für die Integrität des Datensatzes bewertet und dokumentiert werden.

Aufbewahrung der elektronischen Signatur

Ein elektronisch signiertes Dokument ist in der Regel eine dynamische Aufzeichnung. Wird ein Dokument elektronisch signiert, so müssen die mit der Signatur verbundenen Metadaten (d. h. der gedruckte Name des Unterzeichners, die Bedeutung der Signatur sowie Datum und Uhrzeit der Signatur) elektronisch aufbewahrt werden. Ein elektronisch unterzeichnetes Dokument ist nur dann gültig, wenn es elektronisch aufbewahrt wird, es sei denn, der Ausdruck auf Papier oder die PDF-Kopie behält die gesamte Rückverfolgbarkeit zur Identität des Unterzeichners, Datum und Uhrzeit und Bedeutung der Unterschrift bei.

Aufbewahrung elektronischer Kommunikation

Elektronische Kommunikation ist ein weiteres Beispiel für Aufzeichnungen in einem dynamischen Zustand.

Werden Daten durch elektronische Kommunikationsmethoden wie E-Mail und elektronischen Nachrichtenaustausch unterstützt (z. B. zur Ermöglichung der Überprüfung der GLP-Tätigkeiten und -Zuständigkeiten), müssen Verfahren zur Sicherstellung der Aufbewahrung und der Zusammenstellung elektronischer Kommunikation festgelegt werden (einschließlich der Gewährleistung der Vollständigkeit der Aufzeichnungen und der Integrität). Diese Mechanismen müssen so konzipiert sein, dass die Zuordenbarkeit und Integrität der betreffenden elektronischen Mitteilungen gewahrt bleibt, z. B. indem sichergestellt wird, dass Absender und Empfänger zusammen mit den entsprechenden Daten und Uhrzeiten bestimmt werden können. Alle Anhänge müssen mit der entsprechenden Nachricht verbunden bleiben, und die Nachrichtenketten müssen erhalten bleiben.

Wenn möglich, müssen diese in ihrem ursprünglichen Format beibehalten werden. Wenn dies nicht möglich ist, muss die LPE Verfahren für eine originalgetreue Abschrift und Überprüfung in einem aufbewahrungsfähigen Format umsetzen.

Der Ausdruck der elektronischen Kommunikation auf Papier oder die Migration in einer flachen PDF-Datei kann die erforderliche Integrität nicht gewährleisten.

Aufbewahrung überprüfter Kopien

Überprüfte Kopien von dynamischen elektronischen Aufzeichnungen (die durch Migration generiert werden) sind in dynamischem Zustand aufzubewahren, sodass die überprüfte Kopie die für die Sicherstellung der vollständigen Bedeutung der Daten erforderlichen Metadaten (z. B. Datumsformate, Kontext, Layout, elektronische Signaturen und Autorisierungen) enthält, und ihre Historie, einschließlich der Erstellung der überprüften Kopie, rekonstruiert werden kann.

Überprüfte Kopien können anstelle des Originals aufbewahrt werden, sofern ein dokumentiertes System zur Überprüfung und Aufzeichnung der Integrität der Kopie vorhanden ist. Es müssen jegliche Risiken im Zusammenhang mit der Vernichtung der ursprünglichen Aufzeichnungen berücksichtigt werden. Es ist zu beachten, dass einige Bewertungsbehörden die Aufbewahrung der Originale fordern.

Aufbewahrung von Daten aus Hybridsystemen

Wo die Nutzung von Hybridsystemen erforderlich ist, muss klar dokumentiert werden, was den gesamten Datensatz ausmacht, und in SOPs festgelegt werden, welche Aufzeichnungen aufzubewahren sind.

Aufbewahrung von Daten auf anderen Medien

Werden Daten mittels Fotografien oder bildgebender Verfahren und Technologien (oder anderer Medien) erfasst, müssen die Anforderungen an die Speicherung dieser Formate während des gesamten Lebenszyklus denselben Erwägungen wie bei allen anderen Daten folgen, wobei etwaige zusätzliche Kontrollen, die für dieses Format erforderlich sind, zu berücksichtigen sind. Wenn das ursprüngliche Format aufgrund von Qualitätseinbußen (z. B. durch Zersetzung/Degradation/Zerfall/Alterung) nicht beibehalten werden kann, können alternative Mechanismen für die Aufzeichnung einschließlich der Überprüfung der Zuverlässigkeit des Verfahrens (z. B. Fotografie oder Digitalisierung) und die anschließende Speicherung in Betracht gezogen werden, wobei die Gründe für die Auswahl zu dokumentieren sind.

6.15. Datensicherung

Es müssen Mechanismen zur Sicherstellung der erfolgreichen Durchführung von Datensicherungen (Back-up) etabliert werden. Die verwendeten Systeme müssen validiert sein, und jede Datensicherung ist zu überprüfen, um sicherzustellen, dass sie ordnungsgemäß funktioniert hat, indem z. B. bestätigt wird, dass die Datengröße und andere kopierte Eigenschaften mit denen der ursprünglichen Aufzeichnung übereinstimmen.

Sicherungs- und Wiederherstellungsverfahren für elektronische Daten müssen gegebenenfalls getestet werden. Dies ist z. B. dann der Fall, wenn sich entweder das Verfahren oder die bei der Sicherung oder Wiederherstellung verwendeten Werkzeuge oder Anwendungen ändern. Darüber hinaus muss die Langlebigkeit einiger elektronischer Medien, die zur Datensicherung verwendet werden (wie CDs, DVDs usw.), regelmäßig überprüft werden.

Die Sicherungsverfahren sind in SOPs zu beschreiben und die Datensicherungs-Tätigkeiten müssen dokumentiert werden.

Sicherungen für Wiederherstellungszwecke ersetzen nicht die Notwendigkeit der Archivierung von Daten und Metadaten zum Zwecke der Rekonstruktion der Prüfungstätigkeiten.

6.16. Archivierung

Daten müssen unter der Kontrolle des Archivverantwortlichen sicher archiviert werden. Dies kann gegebenenfalls auch an einem geeigneten elektronischen Speicherort erfolgen, unabhängig davon, ob dieser im Originalsystem oder in einem anderen System verortet ist und angemessenen Kontrollen unterliegt, oder als eigenständiges elektronisches Archiv betrieben wird.

Alle (physischen und elektronischen) Archivstandorte, die mit den archivierten Daten in Verbindung stehen, müssen identifiziert und dokumentiert werden.

Die GLP-Grundsätze für die Archivierung müssen gleichbleibend auf elektronische und nicht elektronische Daten angewendet werden. Daher ist es wichtig, dass elektronische Daten mit dem gleichen Maß an Zugangskontrollen und Indexierungsanforderungen aufbewahrt werden wie nicht elektronische Daten.

Archivierte Aufzeichnungen können das Originaldokument und/oder eine überprüfte Kopie sein (siehe auch Abschnitt 6.14 "Aufbewahrung überprüfter Kopien") und müssen so geschützt werden, dass sie nicht unbemerkt verändert oder gelöscht werden können.

Die Archivierungsvorkehrungen müssen so gestaltet sein, dass sie während der gesamten erforderlichen Aufbewahrungsdauer den Abruf und die Lesbarkeit von Daten und Metadaten ermöglichen.

Wenn Altsysteme nicht mehr unterstützt werden können, muss die Bedeutung der Daten berücksichtigt werden und, falls erforderlich, muss die Software für die Zwecke der Datenzugänglichkeit weiter aufrechterhalten werden. Dies kann durch Aufrechterhalten von Software in einer virtuellen Umgebung erreicht werden. Wenn dies nicht möglich ist, müssen die Daten vor der Archivierung auf kontrollierte, getestete und überprüfte Weise in ein System migriert werden, auf das weiterhin zugegriffen werden kann. Die Migration zu einem alternativen Dateiformat, das die Eigenschaft überprüfter Kopien der Daten beibehält, kann mit zunehmendem Alter der Altsystemdaten erforderlich sein.

Ist eine Migration mit voller Funktion der ursprünglichen Aufzeichnungen technisch nicht möglich, müsste die Auswahl aus den verfügbaren Optionen auf dem Risiko und der Bedeutung der Daten im Zeitverlauf basieren. Das Dateiformat für die Migration muss unter Berücksichtigung des Risikos zwischen langfristiger Zugänglichkeit und der Möglichkeit einer eingeschränkten dynamischen Datenfunktionalität (z. B. Datenabfrage, Trendentwicklung, Wiederverarbeitung usw.) ausgewählt werden. Es wird anerkannt, dass die Notwendigkeit, die Zugänglichkeit aufrechtzuerhalten, die Migration zu einem Dateiformat erfordern kann, das den Verlust einiger Attribute und/oder dynamischer Datenfunktionen bedeutet. Die LPE ist dafür verantwortlich, die Auswirkungen solcher Verluste zu bewerten und die Verbindung zwischen dem lesbaren Audit Trail oder den elektronischen Signaturen und den geprüften Daten auf einem akzeptablen Niveau zu halten.

(Siehe auch Abschnitt 3.11 des OECD-Dokuments Nr. 17 (OECD, 2016 [4]))

7. Datenüberprüfung

7.1. Allgemeine Erwägungen

Die Datenüberprüfung umfasst die angemessenen Überprüfungen kritischer Daten zur Qualitätskontrolle, die von Prüfleitern oder anderem Personal durchgeführt werden kann.

Die Ziele der Datenüberprüfung sind:

- Feststellung jeglicher Löschung, Ergänzung, Änderung oder Ausschluss von Daten;
- Überprüfung durch die Prüfleitung, ob alle erzeugten Rohdaten vollständig dokumentiert und aufgezeichnet sind, und
- die Bewertung der Effizienz von Data Governance-Maßnahmen durch Überprüfung eines vollständigen Datensatzes, der durch Verfahren im Rahmen des gesamten Datenlebenszyklus generiert wird.

Um effektiv zu sein, müssen der Grad und der Umfang der Datenüberprüfung durch eine Risikobewertung festgelegt werden. Die als kritisch identifizierten Daten müssen über die kritischen Phasen ihres Datenlebenszyklus überprüft werden. Die Datenüberprüfung muss auch eine Überprüfung relevanter Metadaten, einschließlich Audit Trails oder Elemente davon, umfassen.

Die Datenüberprüfung ist zu dokumentieren. Die Aufzeichnung der Überprüfung muss alle bei der Überprüfung festgestellten Abweichungen von den GLP-Grundsätzen, Prüfplänen oder SOPs, das Datum der Überprüfung sowie die Unterschriften der Prüfer enthalten.

Das Verfahren der Datenüberprüfung ist in einer SOP zu beschreiben. Ein Verfahren muss auch die Maßnahmen beschreiben, die zu ergreifen sind, wenn bei der Datenüberprüfung Abweichungen festgestellt werden. Dieses Verfahren muss Datenkorrekturen oder Klarstellungen ermöglichen, bei denen die ursprünglichen Aufzeichnungen weiter sichtbar sind und Korrekturen über einen Audit Trail nachverfolgt werden können.

Viele Softwarepakete ermöglichen die Konfiguration benutzerdefinierter Berichte zur Unterstützung der Datenüberprüfung. Änderungen an der Berichtskonfiguration müssen kontrolliert werden, um unbefugte Änderungen zu verhindern. Das System muss validiert sein und gegebenenfalls die Berichtsergebnisse überprüft werden.

Hinweis: Die von der Qualitätssicherung durchgeführte Datenprüfung soll die Aussage untermauern, dass die berichteten Ergebnisse die Rohdaten der Prüfungen genau und vollständig widerspiegeln. Dies kann auch bei der Prüfung von Governance-Verfahren für die Datenintegrität wirksam sein. Der Umfang der Überprüfung muss sich nach der Kritikalität der Daten richten.

7.2. Überprüfung des Audit Trails

Es ist nicht erforderlich, dass die Prüfung des Audit Trails jede Systemaktivität umfasst.

Die relevanten Daten unter allen in den Audit Trails gespeicherten Daten müssen identifiziert werden, um eine solide Datenüberprüfung/Verifizierung zu ermöglichen. Die Überprüfung muss nach einem dokumentierten, risikobasierten Verfahren durchgeführt werden, bei dem die Kritikalität der zu überprüfenden Daten und der im Rahmen des Datenflusses ermittelten Transaktionen ermittelt werden. Die Überprüfung kann durch direkten Zugriff auf den System Audit Trail oder durch Verwendung von entsprechend gestalteten und validierten Systemberichten erfolgen.

Die routinemäßige Datenüberprüfung muss eine dokumentierte Prüfung des Audit Trails umfassen, deren Ausgestaltung durch die Risikobewertung festgelegt wird. Bei der Konzeption eines Systems zur Überprüfung von Audit Trails kann dies auf Tätigkeiten mit GLP-Relevanz beschränkt sein (z. B. im Zusammenhang mit der Erstellung, Verarbeitung, Einhaltung von Verfahren, Änderung und Löschung usw.). Audit Trails können mittels Auflistung relevanter Informationen (Checkliste) oder durch einen "Ausnahmeberichtsverfahren" überprüft werden. Ein Ausnahmebericht ist ein validiertes Suchwerkzeug, das vorab festgelegte "ungewöhnliche" Daten oder Handlungen identifiziert und dokumentiert, die eine weitere Überprüfung durch den Datenprüfer erfordern.

Die mit der Überprüfung betrauten Personen müssen über angemessene Kenntnisse und Systemzugriffsrechte verfügen, um relevante Audit Trails, Rohdaten und Metadaten zu überprüfen.

7.3. Überprüfung von Daten aus Hybridsystemen

Bei Hybridsystemen ist voraussichtlich eine verstärkte Datenüberprüfung erforderlich, da diese anfälliger für nicht zuordenbare Datenänderungen sind. Alle Aufzeichnungen aus Hybridsystemen, die als ein Datensatz definiert sind, müssen von einer qualifizierten Person überprüft werden. Das Kontrolllevel muss an die im Hybridsystem verwendeten Verfahren angepasst werden. Die Überprüfung von Daten aus Hybridsystemen muss eindeutig definiert und beschrieben werden, damit die tatsächlich überprüften Datenquellen ermittelt werden können.

8. Datenzugriff

8.1. Allgemeine Erwägungen

Zugriffsrechte auf Daten und Aufzeichnungen müssen immer auf der Grundlage der Risikobewertung jeder Phase des Datenlebenszyklus erstellt werden.

Zugriffsberechtigungen müssen so festgelegt werden, dass das Personal seinen GLP-Aufgaben nachkommen kann.

Der Zugriff auf Aufzeichnungen muss für das Personal, welches Tätigkeiten bei der Datenüberprüfung durchführt, gewährt werden.

Erforderliche Zugriffsmöglichkeiten (einschließlich zu Aufzeichnungen, Audit Trails und Systemfunktionalität), Berechtigungen und Schulungen müssen zur Unterstützung der Qualitätssicherung zur Verfügung stehen, damit überprüft werden kann, ob alle Prüfungen in Übereinstimmung mit den GLP-Grundsätzen durchgeführt werden.

8.2. Zugriff auf computergestützte Systeme und Benutzerrollen

Benutzerzugriff

Zugriffskontrollen müssen vollumfänglich genutzt werden, um sicherzustellen, dass Mitarbeiter nur Zugriff auf Funktionen haben, die für ihre Tätigkeiten und ihre Funktion bei Prüfungen angemessen sind, und dass Handlungen einer bestimmten Person zugeordnet werden können. Die LPE muss in der Lage sein, die den einzelnen Mitarbeitern gewährten

Zugriffsebenen nachzuweisen und sicherzustellen, dass historische Informationen über die Zugriffsebene der Benutzer verfügbar sind. Wenn das System diese Daten nicht erfasst, muss hierzu ein Papierdokument verfügbar sein. Die Kontrollen müssen sowohl auf Betriebssystem- als auch auf Anwendungsebene erfolgen. Eine individuelle Anmeldung auf Betriebssystemebene ist möglicherweise nicht erforderlich, wenn andere geeignete Kontrollen vorhanden sind, um die Datenintegrität sicherzustellen (z. B. kann eine individuelle Anmeldung auf Anwendungsebene ausreichen, wenn eine Änderung von Daten außerhalb der Anwendung nicht möglich ist).

Bei Systemen, die GLP-Daten erzeugen, ändern oder speichern, dürfen keine gemeinsamen Logins oder generische Benutzerzugriffe verwendet werden. Unterstützt das computergestützte Systemdesign den individuellen Benutzerzugriff, so muss diese Funktion verwendet werden. Dies kann den Erwerb zusätzlicher Lizenzen erfordern.

Systeme, die nicht vollumfänglich für GLP-Zwecke verwendet werden, aber über GLP-relevante Elemente verfügen, wie freigegebene Lieferanten, Bestandsstatus, Standort und Transaktionshistorien, erfordern eine angemessene Bewertung.

Es wird anerkannt, dass einige computergestützte Systeme nur eine einzige Benutzerkennung oder eine begrenzte Anzahl von Benutzerkennungen unterstützen. Steht kein geeignetes alternatives computergestütztes System zur Verfügung, so kann eine gleichwertige Kontrolle durch Software von Drittanbietern oder durch ein papiergestütztes Verfahren zur Gewährleistung der Rückverfolgbarkeit (mit Versionskontrolle) erfolgen. Die Eignung alternativer Systeme muss begründet und dokumentiert werden.

Systemadministratorzugriff

Der Systemadministratorzugriff muss auf eine möglichst geringe Anzahl von Personen beschränkt werden, und die Größe und Art der Prüfeinrichtung berücksichtigen. Das allgemeine Systemadministratorkonto darf nicht für den Routineeinsatz verfügbar sein. Mitarbeiter mit Systemadministratorrechten müssen sich mit benutzerspezifischen Anmeldeinformationen anmelden, die es ermöglichen, Ereignisse in Audit Trails einer bestimmten Person zuzuordnen. Damit soll verhindert werden, dass Nutzer mit einem potenziellen Interessenskonflikt Administrationszugriff erhalten, und unbefugte Änderungen vorgenommen werden, die der Person nicht zugeordnet werden können.

Systemadministratorrechte (welche Tätigkeiten wie Datenlöschung, Datenbankänderung oder Systemkonfigurationsänderungen erlauben) dürfen nicht Personen zugewiesen werden, die ein direktes Interesse an den Daten haben (Datengenerierung, -änderung, -löschung, -überprüfung oder -freigabe). Änderungen an Prüfungsdaten durch einen Systemadministrator dürfen nur nach vorheriger Genehmigung durch den Prüfleiter vorgenommen werden.

Kann kein unabhängiger Systemadministrator zugewiesen werden (z. B. in kleinen Prüfeinrichtungen), kann ein ähnliches Maß an Kontrolle durch Verwendung zweier Benutzerkonten mit unterschiedlichen Rollenberechtigungen erreicht werden, wobei alle Änderungen, die unter dem Zugriff des Systemadministrators durchgeführt werden, einer angemessenen Überprüfung und Genehmigung unterliegen.

Das Personal muss sich über ein Benutzerkonto mit den entsprechenden Zugriffsrechten für die jeweilige Aufgabe anmelden, z. B. darf sich ein Labortechniker, der Daten überprüft, nicht als Systemadministrator anmelden, wenn für diese Aufgabe eine angemessenere Zugriffsberechtigung besteht. Die Eignung solcher Regelungen muss regelmäßig überprüft werden.

(Siehe auch Abschnitte 1.3.1 und 3.7 des OECD-Dokuments Nr. 17 (OECD, 2016 [4])*)*

Referenzen

OECD (1997), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 1: OECD Principles on Good Laboratory Practice (as revised in 1997) [1]

OECD (2007), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 15: Advisory Document of the Working Group on Good Laboratory Practice : Establishment and Control of Archives that Operate in Compliance with the Principles of GLP. [2]

OECD (2014), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 16: Advisory Document of the Working Group on Good Laboratory Practice : Guidance on the GLP Requirements for Peer Review of Histopathology. [3]

OECD (2016), OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 17: Advisory Document of the Working Party on Good Laboratory Practice : Application of GLP Principles to Computerised Systems. [4]