GERMAN QUALITY MANAGEMENT ASSOCIATION E.V.

Elektronische Archivierung im GxP-regulierten Umfeld

1. Ausgabe (September 2021)

Elektronische Archivierung im GxP-regulierten Umfeld

Version 1

Herausgegeben von der
German Quality Management Association e.V. (GQMA)

Version: **1**

Datum: **28.08.2021**

Verfasser: **in alphabetischer Reihenfolge**

Dr. Benjamin M. **Bader**	Z.A.S. Zentral Archiv Service GmbH
Dr. Susanne **Becker**	medac GmbH
Eva Maria **Grüner**	AbbVie Deutschland GmbH & Co.KG
Holger **Koschel**	Janssen Vaccines, a pharmaceutical company of Johnson & Johnson
Dr. Norbert **Lüthe**	Fraunhofer-Gesellschaft (ITEM)
Jürgen **Neuss**	Bayer AG
Dr. Simon **Pflug**	Bayer AG
Adele **Plaggenborg**	medac GmbH
Bettina **Quernheim**	Sanofi-Aventis Deutschland GmbH

Zusammenfassung

Stetig wachsende Datenmengen, zunehmende regulatorische Anforderungen sowie die Notwendigkeit, zulassungsrelevante Daten jederzeit global nutzen zu können, erfordern zukunftsorientierte Ansätze zur Archivierung von Daten unter GxP-Bedingungen. Es fehlen derzeit spezifische Gesetze und Guidelines zum elektronischen Archivieren im GxP-regulierten Umfeld, wie sie für die physische Archivierung existieren.

Das vorliegende Praxishandbuch wurde, auf Anregung des GQMA-Vorstands, durch eine GQMA Arbeitsgruppe von GxP-Expertinnen und -Experten aus den Bereichen Archivierung, Qualitätsmanagement, Audit und IT aus der GxP-regulierten Anwendersicht erarbeitet. Es stellt bewusst keine vollständige Anleitung zur Konzeption eines elektronischen Archivs dar. Vielmehr ist es eine Momentaufnahme und soll das interessierte Publikum mit den Mindestanforderungen an die elektronische Archivierung unter GxP-Bedingungen vertraut machen. Mit dem Hinweis auf die vielfältigen Literatur- und Regelwerksquellen, soll die Zielgruppe in die Lage versetzt werden, eine für den eigenen Bedarf passende Archivierungsstrategie zu entwickeln. Durch die zu erwartenden Veränderungen im technischen und regulatorischen Bereich muss diese Strategie an zukünftige Weiterentwicklungen angepasst werden.

Aufgrund der besseren Lesbarkeit haben sich die Autoren und Autorinnen dazu entschieden, Begriffe nicht in geschlechtsneutraler Form zu verwenden.

Inhalt

1. Einleitung

Im GxP-Umfeld werden immer mehr Daten[1] elektronisch generiert, weiterverarbeitet und für die Zulassung von Pharmazeutika oder Pflanzenschutzmitteln genutzt. Durch die Weiterentwicklung von Gesetzen und Verordnungen gibt es eine Reihe neuer Vorschriften, welche erfordern, diese elektronischen Daten auch in das Archivierungskonzept einzubeziehen. Eine weitere Entwicklung ist auch das steigende Interesse seitens der Regulierungsbehörden an der Bereitstellung elektronischer Daten. Auch die Unternehmen sehen vermehrt Bedarf die steigenden Datenmengen elektronisch vorzuhalten, um sie strategisch nutzen zu können.

Das erfordert die Betrachtung einer Vielzahl von Aspekten, die bei der Konzeption und Implementierung eines elektronischen Archivs beachtet werden müssen. Das vorliegende Handbuch gibt einen Überblick über den derzeitigen Stand der regulatorischen Anforderungen und daraus resultierende Empfehlungen und Interpretationen. Die nachfolgenden Kapitel enthalten Erläuterungen und Literaturquellen, die dem Leser helfen sollen, sich mit dem Thema elektronische Archivierung vertraut zu machen und eine für sein Umfeld passende Archivierungslösung zu entwickeln.

Elektronische Daten sind nur dann vertrauenswürdig, wenn ihre Authentizität, Integrität, Identität und Lesbarkeit langfristig, d. h. für die Dauer der erforderlichen Aufbewahrungsfrist, gewährleistet ist. Eine zentrale Anforderung an elektronische Archivierung betrifft die Integrität der archivierten Daten. Gewährleisten lässt sich diese durch die geeignete Kombination von:

- Hardware (z. B. durch unveränderbare und fälschungssichere Datenträger)
- Software (z. B. durch Verschlüsselung, Sicherung, Sperren, Versionierung)
- Organisatorische Maßnahmen (z. B. Nutzerrechtekonzepte, periodische Audit Trail Reviews, regelmäßige Prüfung der Tauglichkeit des Archivierungskonzeptes)

[1] Eine in formalisierter Weise rückinterpretierbare Repräsentation von Information, die zur Kommunikation, Interpretation oder Verarbeitung geeignet ist. Beispiele für Daten beinhalten eine Bitsequenz, eine Zahlentabelle, die Buchstaben auf einer Seite, die Tonaufnahmen einer sprechenden Person oder eine Mondgesteinsprobe. (Quelle: Nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland (Hrsg.): Referenzmodell für ein Offenes Archiv-Informations-System - Deutsche Übersetzung 2.0 (nestor-materialien 16), S. 9)

Eine einfache Ablage in einem Dateisystem (z.B. geschützter Fileshare) ohne zusätzliche Maßnahmen erfüllt die Anforderungen zur Unveränderbarkeit elektronischer Daten in der Regel nicht. Ein klassisches Backup ist kein Archivierungsverfahren und dient lediglich der kurzfristigen Datensicherung.

Wichtig ist, den gesamten Archivierungsprozess in den Fokus der Betrachtung zu rücken, nicht nur den Speichervorgang.

2. Regulatorischer Rahmen

Die aktuellen GxP Regularien setzen unter anderem folgende, für die elektronische Archivierung relevanten Anforderungen fest, um die Lesbarkeit von Daten über den Archivierungszeitraum sicherzustellen:

- Erstellung von Verfahrensanweisungen (SOPs) für die Nutzung und Administration des elektronischen Archivs
- Benutzerberechtigungskonzept (Definition von Rollen)
- Vollständigkeit und Integrität der Daten bei der Überführung ins Archiv
- Datenverwaltung inklusive Metadaten (Prozess- und Systemmetadaten)
- Schutz der Daten gegen Veränderung / Alterung (Langzeitstabilität)
- Festlegung der Aufbewahrungsfrist (mindestens die gesetzliche Aufbewahrungsfrist)
- Entscheidungsprozess über die endgültige Löschung der Daten nach Ablauf der Aufbewahrungsfrist
- Maßnahmen gegen einen Totalverlust

Wechsel des Eigentümers der Daten (Verkauf/Schließung) oder eines von einem externen Dienstleister betriebenen Archivs sind gesondert zu betrachten.

Eine Zusammenstellung von Anforderungen aus einschlägigen Regularien und sonstiger Veröffentlichungen, getrennt nach GxP-Bereichen, befindet sich in Kapitel 7 dieses Dokuments. Die dortige Aufstellung erhebt keinen Anspruch auf Vollständigkeit.

3. Rollen und Verantwortlichkeiten

Die Gesamtverantwortung für die Konzeption, den Betrieb und die Nutzung des Archivs trägt die Leitung der Prüfeinrichtung (GLP), der Sponsor klinischer Studien (GCP) oder die Leitung der Herstellung (GMP). Detaillierte Angaben zu den Verantwortlichkeiten und den einzelnen Rollen/-bezeichnungen sind mit Verweis auf die entsprechenden Regularien im Kapitel 7 ausführlich beschrieben.

Für den Betrieb und die Nutzung des Archivs sind abgestufte Berechtigungskonzepte und Vereinbarungen zu erstellen, aus denen Rollen und Verantwortlichkeiten des Archivars, der Qualitätssicherung, des IT-Supports, der Nutzer und eventuellen externen Dienstleistern hervorgehen. Außerdem sind Kommunikationswege/ Berichtswege zwischen den handelnden Personen/-gruppen festzulegen.

3.1 Konzeption

Zunächst sollte eine Analyse der zu archivierenden Daten durchgeführt werden. Ferner ist abzuklären, ob es sich um dynamische oder statische Daten handelt oder ob eine “online” oder “offline” Archivierung vorgesehen ist. Sollen die Daten betriebsintern archiviert werden oder ist die Vergabe an externe Dienstleister, ganz oder teilweise, vorgesehen? Welche Anforderungen aus Richtlinien und Gesetzen sind zu beachten?

3.2 Nutzerrollenkonzept innerhalb des Archivsystems

Unabhängig davon wo und durch wen das elektronische Archiv betrieben wird, sollte ein Nutzerkonzept erarbeitet werden. Hierzu gehört die Rolle des Archivars (Kapitel 7), genauso wie die Rollen weiterer Nutzer mit definierten Rechten. Nutzerrechte könnten hier beispielsweise auf der Ebene des Datentyps (record type) oder der Organisationseinheit vergeben werden.

3.3 Grundsätzliches zu vertraglichen Regelungen bei der Vergabe an Dienstleister

Mindestens folgende Punkte sollten bei einer vertraglichen Vereinbarung betrachtet werden (die Aufzählung erhebt keinen Anspruch auf Vollständigkeit)[2]:

- rechtliche Einflussfaktoren:
  - Mindestaufbewahrungsdauer
  - Berücksichtigung von Datenschutzbestimmungen
  - Auswertbarkeit oder Reproduzierbarkeit von Daten aus gesetzlichen Forderungen
- Verfügbarkeit:
  - Aufbewahrung und Zugriff der Daten über den geforderten Zeitraum
  - Ausfallsicherheit
  - Stabilität der Speichermedien und Informationserhalt der Daten
- Festlegung von Antwortzeiten/Reaktionszeiten
- Geschäftsaufgabe, Insolvenz
- Finanzielle Rahmenbedingungen:
  - einmalige Investitionen
  - laufende Kosten z. B. Personalkosten,
  - Lizenzgebühren
- Kommunikation:
  - zwischen Dateneigner, Archivar und (externen) IT-Serviceanbietern und /oder Archivdienstleistern
  - folgende Informationen sind auszutauschen und müssen eventuell ebenfalls archiviert werden:
    - Abweichungen und Zwischenfälle
    - Veränderungsmanagement (sowohl technisch als auch organisatorisch)
    - Kommunikationswege

[2] Siehe auch Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, IT Grundschutz Bausteine, OPS: Betrieb, OPS.1.2.2 Archivierung

3.4 Zusätzliche Vereinbarungen je nach Art der Archivierung

3.4.1 Archivierung innerhalb der eigenen Organisation

Bei einer betriebsinternen Datenarchivierung sind entsprechende Organisationsdiagramme, Berichtslinien und Vereinbarungen (wie z.B. firmeninterne Verträge oder Standardarbeitsanweisungen (SOPs)) zwischen den beteiligten Abteilungen schriftlich zu erstellen (siehe Kapitel 7). Dies können beispielsweise die Servicevereinbarungen und Kommunikationslinien mit der internen IT-Abteilung des Unternehmens sein, besonders dann, wenn diese nicht der direkten Organisation des Dateneigners zugeordnet ist. Die Aufnahme in das QS-Programm stellt die Durchführung regelmäßiger Audits in der Serviceabteilung sicher.

3.4.2 Archivierung unter Einbezug eines externen IT-Dienstleister

Wird zur Archivierung auf einen externen IT-Dienstleister zurückgegriffen, so hängt der Umfang der notwendigen vertraglichen Regelungen von dem in Anspruch genommenen Servicemodell ab. Je nach dem gewählten Modell sind unterschiedlich detaillierte schriftliche Vereinbarungen zu treffen. Dies sollte auf Basis einer Risikoanalyse und in Abhängigkeit vom Grad der externen Vergabe erfolgen.

Eine weitere Forderung ist, die Kompetenz und Zuverlässigkeit des Lieferanten zu überprüfen. Die Möglichkeit der Auditierung des Lieferanten durch den Auftraggeber, auch in Form eines vor-Ort Audits, sollte in einer vertraglichen Vereinbarung ebenfalls berücksichtigt werden. Für den GLP-Bereich beispielsweise ist die Schriftform zwischen Lieferanten und Prüfeinrichtung explizit gefordert. Dabei trifft der Begriff „Lieferant“ sowohl für interne IT-Abteilungen, externe Dienstleister als auch für Anbieter von Hosting – Diensten zu. Ebenfalls wird eine Vereinbarung gefordert, die eine eindeutige Formulierung zum Dateneigentum, sowie eine Regelung der Verantwortlichkeiten zwischen den Auftraggebern und dem Lieferanten beinhaltet (OECD 17 1.6, 34).[3]

[3] OECD Advisory Document Nr.17, Application of GLP Principles to Computerised Systems

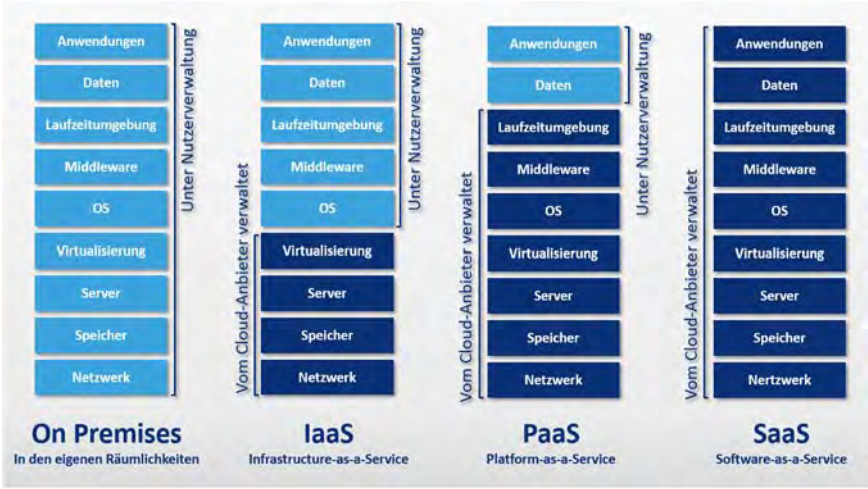

Abbildung 1: Gängige Servicemodelle[4]

3.4.3 Archivierung durch und in einem externen Auftragsarchiv

Die Nutzung externer Dienstleister für das Management des elektronischen Archivs erfolgt häufig unter dem Software as a Service (SaaS) Modell. Dies beinhaltet neben der Hardwareinfrastruktur auch die Software und Schnittstellen zur Datenübertragung, welche qualifiziert bzw. validiert werden und über das Change-Management im validierten Zustand gehalten werden sollten. Die dynamische Entwicklung von Hardware resultiert in immer kürzeren Intervallen von Hardware-Upgrade und Betriebssystem-Updates (siehe Kapitel 6 Erhaltungsstrategien). Dieses Life-Cycle Management von Hard- und Software hat direkten Einfluss auf den Validierungszustand des elektronischen Archivs. Die Re-validierung inkl. einer kontinuierlichen Änderungsdokumentation bei tiefgreifenden Änderungen ist dringend erforderlich. Die Definition von tiefgreifenden Änderungen ist individuell, systemabhängig und sollte vertraglich geregelt werden (Abbildung 1).

[4] Bildquelle: https://www.ionos.de/digitalguide/fileadmin/DigitalGuide/Screenshots/schematische-darstellung-der-cloud-service-modelle.png - Zugriff: 22.08.2021

Eine Risikoabschätzung aktiver Änderungen, aber auch unvorhergesehener Ereignisse, muss in einem Service Level Agreement und Disaster Recovery Plan (siehe Kapitel 10 Disaster Recovery) fixiert werden, um im Falle eines Ausfallereignisses je nach Service Level einen geregelten Ablauf der Wiederherstellung und Bereitstellung zu gewährleisten. Diese Service Level Agreements können weitere Themen beinhalten, sofern diese nicht bereits im Vertrag fixiert wurden, wie z.B.:

- Redundante Speicherung und Ort der Speicherung
- Dokumentation tiefgreifender Änderungen: z.B. Umzug vom Server, Updates von Betriebssystemen
- Zugriffswege: z.B. web-interface zum Lesen, bzw. File Transfer Protokolle zum Schreiben
- Datenpakete und -formate: z.B. einzelne Dateien, gepackte Transferorder, Standardformate
- Zugriffszeiten: z.B. regelmäßige und zeitliche definierte Datenübertragung ins Archiv
- Datenschutzregelung und Löschkonzepte (siehe Kapitel 9 Datenschutz)
- Verschlüsselung: z.B. Verschlüsselungsprogramm auf jedem Nutzerclient

4. Archivierungsprozess (allgemeine Bedingungen)

Die GxP-Regularien liefern Ansätze und Bedingungen hinsichtlich der elektronischen Archivierung. Für die Umsetzung eines elektronischen Archivierungsprozesses wird im Nachfolgenden ein Modell beschrieben (OAIS), wohlwissentlich, dass das OAIS-Referenzmodell kein „Leitfaden“ ist, der in einer 1:1 Umsetzung die Herausforderungen der elektronischen Archivierung überwindet. Es bildet jedoch ein „logisch-konzeptionelles Rahmenwerk zur Definition und Überprüfung von Archiven“,[5] und kann dazu dienen, ein „besseres Verständnis für die Aufgaben einer konkreten, strategischen Archivplanung zu gewinnen“[6] ohne Bestimmung definierter Hardware, Software, Architektur oder Sprache.

[5] Schneider, Holger: Digitale Amnesie: Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, 2012, S. 105

[6] Schneider, Holger: Digitale Amnesie: Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, 2012, S. 118

4.1 OAIS-Referenzmodell

Das OAIS ist ein ISO-Norm basiertes Referenzmodell,[7] welches weltweit bei der Konzeption von elektronischen Archiven als Standard für das Management und den Langzeiterhalt von Archivinformationen eine hohe Akzeptanz gefunden hat. Darin wird ein elektronisches Archiv definiert als „Organisation (bestehend aus Personen und technischen Systemen) die die Verantwortung für den Langzeiterhalt und die Langzeitverfügbarkeit von Information in digitaler Form sowie die Bereitstellung für eine bestimmte Zielgruppe übernommen hat."[8] Die Kernkomponenten dieses Modells bilden das Informations- und Funktionsmodell, welche im Folgenden beschrieben werden.

Im Informationsmodell wird dargestellt, welche Informationen die Archivdaten enthalten müssen. Dazu gehören neben den eigentlichen Inhaltsinformationen z. B. Informationen bezüglich der Zugriffsrechte oder der Herkunft. Diese Informationen werden in einem so genannten „Archival Information Package" (AIP) zusammengeführt. Das AIP bildet den Dreh- und Angelpunkt der Archivierungsprozesse, ist als selbsttragendes Objekt konzipiert und umfasst und speichert alle wesentlichen Informationen, die zur langfristigen, gesicherten Wiederherstellung und Nutzung erforderlich sind (Abbildung 2).

[7] Das Modell ist Bestandteil der ISO 14721 (ISO 14721:2012 Space data and information transfer systems — Open archival information system (OAIS) — Reference model) bzw. DIN 31644 (DIN 31644:2012-04 Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive

[8] Keitel, C., Schoger, A. (Hrsg.): Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644; Beuth Verl., 2013; S. 80

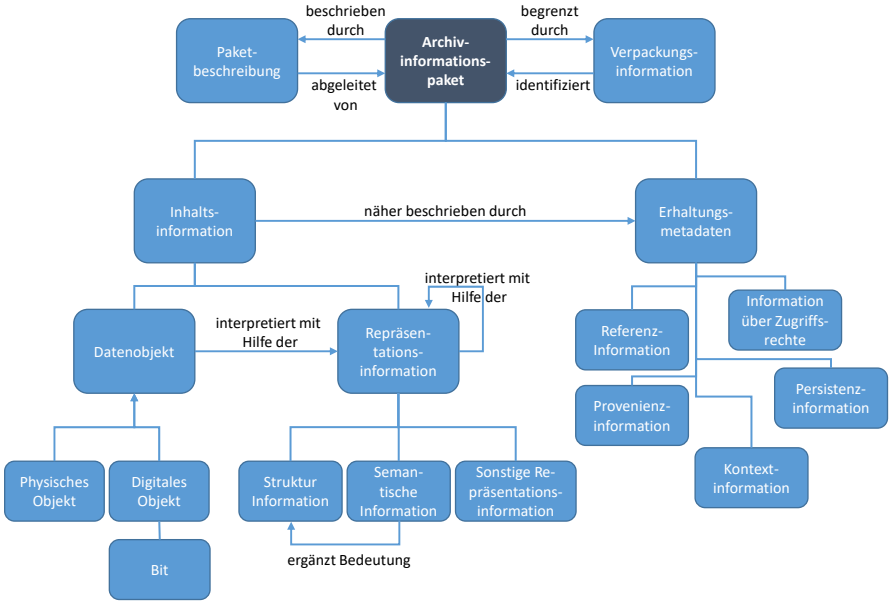

Abbildung 2: Detaillierte Ansicht eines Archivinformationspakets (AIP), adaptiert nach Nestor[9]

Im Funktionsmodell werden Prozesse und Arbeitsabläufe dargestellt, die für die Übernahme der Daten (SIP=Submission Information Package), dem Management der Daten im Archiv (AIP, Abbildung 2) sowie für den Zugriff auf die Daten (DIP=Dissemination Information Package) notwendig sind.

[9] nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland (Hrsg.): Referenzmodell für ein Offenes Archiv-Informations-System - Deutsche Übersetzung 2.0 (nestor-materialien 16), S. 69, Abb. 4-18

Das Funktionsmodell – Kern der OAIS-konformen Archivierung

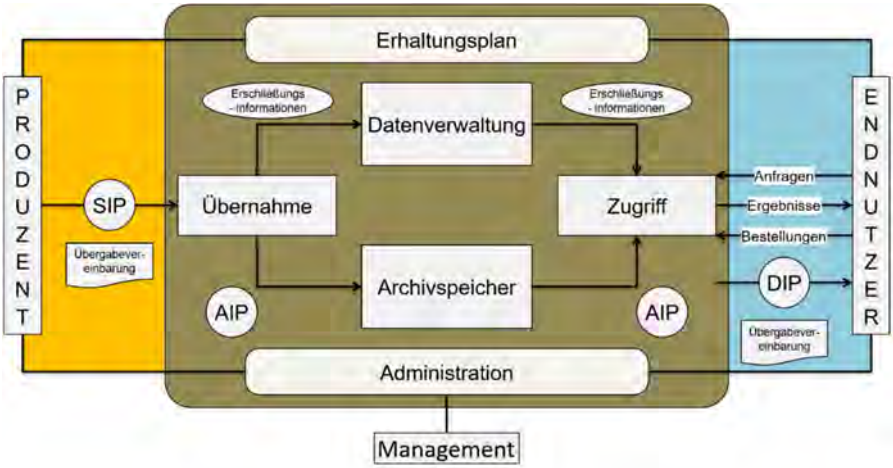

Abbildung 3: Funktionsmodell adaptiert nach OAIS Ref. Modell[10] Produzent: SIP=Submission Information Package (=zu archivierendes digitales Objekt); Management: AIP=Archival Information Package (=digitales Archivobjekt); Endnutzer: DIP=Dissemination Information Package (=Ausgabepaket des AIP)

[10] nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland (Hrsg.): Referenzmodell für ein Offenes Archiv-Informations-System - Deutsche Übersetzung 2.0 (nestor-materialien 16), S. 33, Abb. 4-1

Den sechs im Funktionsmodell dargestellten Archivfunktionen werden die folgenden Aufgaben zugewiesen. Eine konkretere Beschreibung der Funktionen/Aufgaben befindet sich in Kapitel 5 „Datenverwaltung“)

- **Übernahme**: Generierung der notwendigen Erschließungsmaßnahmen wie Indexierung, Definition der Zugriffsrechte etc.
- **Archivspeicher**: digitaler Speicher im engeren Sinne, also die unveränderliche Speicherung der Daten auf Festplatten, optischen Datenträgern, Magnetbändern o. ä.
- **Datenverwaltung**: u. a. Koordination der Erschließungsinformationen wie z. B. den Indexlisten, Bereitstellung von Recherchewerkzeugen, Management der Rechtevergabe und der Aufbewahrungsfristen
- **Zugriff** Zugang, der es externen Benutzer/innen ermöglicht, im elektronischen Archiv zu recherchieren. Die Übergabe an den Benutzer erfolgt in Form eines DIP=Kopie des AIP
- **Administration**: Systemverwaltung. Die zentrale Ablaufsteuerung kontrolliert kontinuierlich die Funktionalität des gesamten Archivsystems und steuert die Abläufe und Informationsflüsse zwischen den einzelnen Modulen. Koordination von Archiv/Nutzern und Hard- und Softwaresystem
- **Erhaltungsplanung**: Die Bestandserhaltung sorgt durch vorausschauende Planung, Wahl und Anwendung geeigneter Maßnahmen für die langfristige Verfügbarkeit digitaler Informationen unter Wahrung ihrer Integrität und Authentizität. Zu den Aufgaben gehört u. a. Empfehlungen für Migration/Emulation/Erhaltung der Originaltechnik zu erarbeiten (s. Kapitel 6 Erhaltungsstrategien).

4.1.1. Anwendung auf das regulierte / validierte Umfeld

Aus der Definition ergibt sich bereits das **Hauptziel eines OAIS**: Information für eine vorgesehene **Zielgruppe** zu erhalten. Das Archiv muss deshalb die Anforderungen seiner Zielgruppe kennen, um zu wissen, welches Minimum an Information gepflegt werden muss. Es entwickelt sich mit seiner Zielgruppe. Bei der Umsetzung im regulierten Bereich müssen beispielsweise Aufbewahrungsfristen festgelegt, sowie die Abgrenzung von „aufbewahrungspflichtig“ und „aufbewahrungswürdig“ beachtet werden, d. h. auch nach Ablauf der regulatorischen Aufbewahrungsfristen sind gegebenenfalls Entscheidungen zu treffen, ob Daten weiterhin „aufbewahrungswürdig“ sind oder überhaupt noch aufbewahrt werden dürfen (wie z. B. bei der Archivierung personenbezogener Daten, siehe Kapitel 9 Schutz personenbezogener Daten). Dementsprechend wurde im GAMP „Good Practice Guide: Electronic Data Archiving“ bereits 2007 auf das OAIS Modell hingewiesen[11]. Das OAIS Referenzmodel lässt sich generell auf online und offline-Archivlösungen anwenden. Insbesondere mit den neueren Veröffentlichungen eröffnet sich für Organisationen die Möglichkeit, eine online-Archivierung in Erwägung zu ziehen. Vor dem Hintergrund der technologischen Entwicklung kann der Begriff Archivsystem auch als sicherer, abgeschlossener Archivbereich innerhalb eines Produktivsystems interpretiert werden[12].

4.2. Datenformate

In Datenformaten werden die Struktur sowie die Darstellung von Daten festgelegt. Es wird definiert, wie die Daten bei der Speicherung und dem Wiederaufruf zu interpretieren sind. Der Begriff „Datenformat“ wird zum Teil synonym zum Begriff „Dateiformat“ verwendet. Dabei gilt jedoch: jedes Dateiformat ist ein Datenformat, aber nicht jedes Datenformat ist auch ein Dateiformat. Beispiel: ein Datenformat kann Daten beschreiben, die auf mehrere Dateien verteilt sind oder sich nur auf einzelne Dateien beziehen.

[11] GAMP Good Practice Guide: Electronic Data Archiving, International Society for Pharmaceutical Engineering (ISPE), 2007, S. 78 ff

[12] Guidelines for the Archiving of Electronic Raw Data in a GLP Environment/ AGIT: Swiss Working Group on Information Technology in a GLP Environment, 2018, Version 2.0, S. 6

4.2.1. Auswahlkriterien für Datenformate

Für die Archivierung elektronischer Daten, wie Dokumente und Aufzeichnungen müssen geeignete Datenformate gewählt werden. Idealerweise sollte bereits bei der Erstellung von Daten bzw. bei der Entscheidung, welche computergestützten Systeme ausgewählt werden, eine Abschätzung für die spätere Eignung hinsichtlich einer (Langzeit-) Archivierung erfolgen.[13]
Das Bundesamt für Sicherheit in der Informationstechnik führt für die Auswahl geeigneter Datenformate in ihrem Grundschutzkatalog[14] bzgl. der Archivierung von Dokumenten folgende allgemeine Kriterien auf:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- die Dokumentstruktur sollte eindeutig interpretiert werden können,
- der Dokumentinhalt sollte elektronisch weiterverarbeitet werden können,
- Beachtung gesetzlicher Vorschriften,
- die Grammatik und Semantik des Datenformates müssen ausführlich dokumentiert sein, so dass eine spätere Migration problemlos möglich ist,
- Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Die Beachtung dieser Kriterien erleichtert die exakte Interpretierbarkeit des Datenformats – und damit die Lesbarkeit der in den Dateien/Dokumenten erhaltenen Informationen – während der Aufbewahrungszeit. Bei der langfristigen Archivierung ist, neben dem Erhalt möglichst aller ursprünglichen Informationen (Merkmale wie Inhalt und Bedeutung), auch das Beibehalten in einer für Menschen lesbaren Form[15] von großer Bedeutung. Beide Aspekte sind gegeneinander abzuwägen und gelten sowohl für das Original als auch für eine originalgetreue Kopie („True Copy“).

Die Medicines and Healthcare products Regulatory Agency (MHRA) konstatiert dazu beispielsweise: „It is recognized that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality …“[16]. Ferner bietet es sich an, komplexe Daten in mehreren

[13] Guidelines for the Archiving of Electronic Raw Data in a GLP Environment/ AGIT: Swiss Working Group on Information Technology in a GLP Environment, 2018, Version 2.0 , S.3
[14] Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein OPS.1.2.2 Archivierung, S. 18f
[15] Guidelines for the Archiving of Electronic Raw Data in a GLP Environment/ AGIT: Swiss Working Group on Information Technology in a GLP Environment, 2018, Version 2.0., Kapitel 2 Introduction
[16] MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018, Kapitel 6.17.1

elektronischen Datenformaten parallel zu archivieren (im proprietären Ursprungsformat und in einem langzeitverfügbaren Format, z.B. als PDF/A). Dadurch kann einem unerwünschten Verlust von Information vorgebeugt werden. Es ist dann allerdings eine Festlegung nötig, bei welchen Daten (Original vs. True Copy) es sich um die Originaldaten handelt.

4.2.2. Standardisierte/Non-proprietäre Datenformate

Standardisierte bzw. non-proprietäre Datenformate sind weit verbreitet und stellen deshalb in der Regel keine besonderen Probleme bzgl. der Langzeitverfügbarkeit und –interpretierbarkeit von archivierten Daten dar. Es kann für alte Formate und besonders für die Zukunft dennoch die Notwendigkeit entstehen, die Verfügbarkeit und Interpretierbarkeit neu zu bewerten.

Es existieren zahlreiche Verzeichnisse, in denen einzelne, für die Archivierung geeignete Formate aufgeführt und bewertet werden und anhand derer eine Einschätzung bezüglich der Langzeitverfügbarkeit der Formate möglich ist.[17]

4.2.3. Proprietäre Datenformate

Viele Analysegeräte im GxP-Bereich sind an computergestützte Systeme angeschlossen, auf denen mit spezieller Software Rohdaten aufgezeichnet und in einem proprietären Format gespeichert werden. Dies kann für den Erhalt und die Reprozessierbarkeit der Daten über den gesamten Archivierungszeitraum problematisch sein, wenn das verwendete Datenformat oder die computergestützten Systeme veralten (siehe auch Kapitel 6 Erhaltungsstrategien). Es gibt Bestrebungen, auch von Herstellern computergestützter Systeme und Vertretern der pharmazeutischen Industrie, für diesen Bereich standardisierte Formate zu entwickeln.

[17] Koordinierungsstelle für die dauerhafte Archivierung elektronischer Unterlagen (KOST): Katalog archivischer Dateiformate (KaD) v5.0 Empfehlung der KOST; Bg/Km/Rc21.12.2016Forschungsdateninfo: Formate erhalten

4.2.4. Statische vs. dynamische Daten/Reprozessierbarkeit

Aus aktuellen GxP-Regularien (i. e. gesetzlich normierte GxP-Anforderungen), lässt sich nicht ableiten, dass archivierte Daten in reprozessierbarer Form aufzubewahren sind. Demnach wäre eine Archivierung von GxP-Daten in einem anderen Format als dem, in dem diese ursprünglich aufgezeichnet worden sind, zulässig. Eine Migration der Daten in ein speziell für die Archivierung elektronischer Aufzeichnungen geeignetes, idealerweise offengelegtes Datenformat, verspräche auch Vorteile hinsichtlich der Langzeitverfügbarkeit der enthaltenen Information. In einzelnen GxP-Leitlinien wird jedoch gefordert, die ursprüngliche Erstaufzeichnung der Daten im reprozessierbaren Originalformat („Originalaufzeichnungen“) aufzubewahren. Dies gelte insbesondere dann, wenn es sich dabei um sogenannte „dynamische Daten“ handelt.[18] Dynamische Daten werden definiert als Aufzeichnungen, die in einem Format vorliegen, welches eine interaktive Nutzung der Daten (z. B. für eine erneute Auswertung, Trendanalysen usw. [19]) ermöglicht.[20] Falls dynamischen Daten, z. B. für Archivierungszwecke, in eine statische Repräsentanz dieser Daten überführt werden, kann auch die Aufbewahrung der dynamischen Daten im ursprünglichen IT-System zusätzlich erforderlich oder ratsam sein.[21] Eine ausschließliche Archivierung ursprünglich

---

[18] Data Integrity and Compliance with CGMP Guidance for Industry, Food and Drug Administration (FDA), (Pharmaceutical Quality/Manufacturing Standards (CGMP)), December 2018, S. 13, Kapitel 10

[19] z. B. empfohlen im GMP-Bereich in: EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines: Volume 4 of "The rules governing medicinal products in the European Union" contains guidance for the interpretation of the principles and guidelines of good manufacturing practices for medicinal products for human and veterinary use laid down in Commission Directives 91/356/EEC, as amended by Directive 2003/94/EC, and 91/412/EEC respectively, Part I, Kapitel 6.9

[20] Vgl. z. B. die Definition „dynamischer Daten“ in: MHRA GXP Data Integrity Guidance and Definitions; Revision 1, Medicines and Healthcare Regulatory Agency (MHRA), o. O., March 2018, S. 12: “Records in dynamic format, such as electronic records, allow an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user or reviewer (with appropriate access permissions) to reprocess the data and expand the baseline to view the integration more clearly.”
Zu originalen Aufzeichnungen in Form „dynamischer“ vs. „statischer“ Information vgl. z. B. die Definition in: Draft PIC/S Guidance Good Practices for Data Management and Integrity in regulated GMP/GDP Environments (PI 041-1 (Draft 2)), Pharmaceutical Inspection Co-operation Scheme (PIC/S), 10 August 2016, S. 12: “The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.”

[21] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 5.3., S. 12

dynamischer Daten in statischer Form kann u. U. nicht ausreichend sein, um die regulatorische Anforderung der Aufbewahrung der Originaldaten oder verifizierter Kopien davon zu erfüllen.[22] Auch bei einer Außerbetriebnahme des ursprünglichen IT-Systems kann es notwendig sein, zur weiteren Aufbewahrung andernorts verifizierte Kopien der Originaldaten zu erstellen, bei denen das „dynamische Format" erhalten wird, sofern dies zum Verständnis dieser Daten und damit als Beitrag zum Erhalt der Datenintegrität erforderlich ist.[23] Die Archivierung von Daten in reprozessierbarer Form in Übereinstimmung mit den erwähnten Leitlinien kann auch als Beitrag zur gesetzlich geforderten „Herstellung oder Prüfung der Arzneimittel nach dem Stand von Wissenschaft und Technik" gewertet werden.[24]

Das Vorhalten von Daten in einem dynamischen, (re-)prozessierbaren Format erfordert geeignete Software und ggf. auch Hardware während der gesamten Aufbewahrungsdauer (siehe auch Kapitel 6 Erhaltungsstrategien). Dies stellt eine erhebliche Herausforderung für die Langzeitverfügbarkeit der Daten und eine dafür geeignete Archivierungsstrategie dar. Daher wird empfohlen, die Daten, die im dynamischen Originalformat aufbewahrt werden sollen, sowie den Zeitraum, für den dies sinnvoll und erforderlich ist, auf der Grundlage einer Risikoanalyse festzulegen. Grundlage hierfür sollte der konkrete Nutzen sein, den die Aufbewahrung von Daten im dynamischen Originalformat für die Patientensicherheit, Produktqualität und Nachvollziehbarkeit von GxP-Aktivitäten hat[25]. Siehe auch Kapitel 6.1.3.2 Emulation.

[22] Data Integrity and Compliance with Drug CGMP: Questions and Answers, Guidance for Industry, Food and Drug Administration, December 2018, S. 9, Abschnitt 10

[23] WHO Guidance on Good Data and Record Management Practices, World Health Organization (WHO Technical Report Series, No. 996), Annex 5, o. O., 2016, S. 206f

[24] §14, Absatz 6a Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz - AMG). Siehe auch: Terhechte, Arno et al: Datenintegrität: Static Data vs. Dynamic Data, In: Die Pharmazeutische Industrie (Pharmind), 79 (2017) 11, S. 1581

[25] Ausführlich diskutiert in: Terhechte, Arno et al: Datenintegrität: Static Data vs. Dynamic Data, In: Die Pharmazeutische Industrie (Pharmind), 79 (2017) 11, S. 1578-1582.

4.2.5. Archivierung von strukturierten Daten/ Datenbanken

Bei Datenbanken sind aufgrund ihrer Komplexität weitere Aspekte bezüglich der elektronischen Archivierung zu beachten:

Auf Grund der Vielzahl von Informationen in digitaler Form und deren ständig wachsender Zahl, werden diese Informationen in Datenbanken abgelegt. Datenbanken speichern und verwalten große Datenmengen strukturiert und stellen den Zugriff auf die darin befindlichen Informationen sicher.[26] Die Datenbank enthält zum einen die eigentlichen Daten und zum anderen noch Angaben über die logische Datenstruktur.

Eine der am häufigsten verwendeten Arten ist die relationale Datenbank, diese soll hier in ihrer Funktion beispielhaft betrachtet werden:

Bei relationalen Datenbanken werden die Informationen nicht alle in einem Datensatz gespeichert, sondern unter Umständen in einer Vielzahl (bis zu hunderten) verschiedener Tabellen, in denen einzelne Teile der Informationen enthalten sind. Eine Kombination aus Tabellenname, dem Primärschlüssel (der die eindeutige Identifikation von Zeilen darstellt) und einem Spaltennamen identifiziert die Einträge eindeutig. Diese können durch Fremdschlüssel, die auf andere Tabellen verweisen, mit weiteren Informationen verknüpft werden. Eine Abfrage stellt die Daten unterschiedlicher Tabellen, die über gemeinsame Attribute verknüpft sind, als Ergebnis dar. Dabei ist oft nicht zu erkennen, dass dieses Ergebnis der Abfrage konsolidierte Information aus verschiedenen Quellen darstellt. Die Information über die Datenbankstruktur wird ebenso in einer Tabelle gespeichert, wie die Daten selbst. Diese Struktur aller Tabellen einer Datenbank wird in einem sogenannten Katalog (ebenfalls eine Tabelle) zur Verfügung gestellt. Wichtig und daher unbedingt zu beachten ist: Änderungen an diesem Katalog haben eine Änderung der Datenbankstruktur zur Folge!

Diese Beziehungen machen deutlich, wie wichtig umfassende Überlegungen bei der Archivierung einer Datenbank sind, um zu vermeiden, dass Informationen verloren gehen bzw. nicht mehr auffindbar sind, weil die Informationen über die Beziehungen (Relation) nicht mehr zur Verfügung stehen. Die Archivierung von Datenbanken darf sich folglich nicht ausschließlich auf den Informationsanteil beschränken, sondern muss immer auch den Katalog enthalten, ohne den die

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, Edition 2021, APP.4.3 Relationale Datenbanksysteme

Gesamtheit der Informationen nicht zur Verfügung steht. Für nicht-relationale Datenbanken sind ggfs. andere Aspekte bzgl. Verknüpfung von Dateninhalten und Metadaten hinsichtlich der Archivierung zu beachten. Für alle zu archivierenden Datenbanken muss zudem eine Erhaltungsstrategie erarbeitet werden.[27] (Siehe auch Kapitel 6 Erhaltungsstrategie).

5. Datenverwaltung

Während auf der einen Seite viel Aufwand betrieben werden muss, die archivierten Daten im Sinne der Datenintegrität unveränderbar zu sichern, stellt das Datenmanagement gem. OAIS-Modell alle Funktionalitäten bereit, die für die Administration und die Wiederauffindbarkeit, also Recherche und Abruf, der gesicherten Daten und Metadaten erforderlich sind. Damit unterstützt das Datenmanagement in einer Querschnittsfunktion die Kernprozesse des elektronischen Archivs (Aufnahme, Speicherung, Nutzung, Erhaltung) und sichert die in den ALCOA+ Prinzipien geforderten Datenintegritätskriterien (Erhalt des Originals, Lesbarkeit und Auffindbarkeit).[28]

Zentral sind die Terminierung und Koordination der einzelnen Erhaltungsprozesse.

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium Edition 2021, APP.4.3 Relationale Datenbanken

[28] siehe auch WHO Guidance on good data and record management practices, Annex 5, S. 204

5.1. Administration

Für den Erhalt und dem Nachweis der Authentizität und Integrität sollte ein geeignetes Datenmanagement betrieben werden. Hier sind die Prozesse Aufnahme, Archivablage, Nutzung und Veränderung, Nutzerrecherche und die Löschung festzulegen.[29]

Folgende Aufgaben muss das Datenmanagement erfüllen.[30]

- Objektverwaltung: Die Beziehung unterschiedlicher Daten (entspricht Archivobjekte im OAIS-Modell) zueinander muss identifiziert werden
- Nutzerrechteverwaltung: Verwaltung der Nutzerrechte durch regelmäßige und dokumentierte Identifizierungsmaßnahmen
- Metadatenverwaltung: Formale, inhaltliche und strukturelle Beschreibung der Archivobjekte zur Auffindbarkeit und Nutzung (gemeint ist das OAIS Archival Information Package (AIP, siehe Kapitel 4.1 OAIS))
- Verwaltung technischer Metadaten des Archivsystems: technische Beschreibung der Archivobjekte um eine Interpretierbarkeit, die Sicherung der Integrität sowie die Planung und Durchführung von Langzeiterhaltungsmaßnahmen zu gewährleisten (gemeint ist das OAIS Submission Information Package (SIP, siehe Kapitel 4.1 OAIS))
- Verwaltung der Erhaltungsmaßnahmen
- Audit Trail Verwaltung: Die Dokumentation aller Veränderungen an den digitalen Objekten ist notwendig, um die Authentizität und Integrität der Daten nachzuweisen
- Löschkonzepte und rechtliche Vorgaben: Einhaltung von rechtlichen Vorgaben während der gesamten Aufbewahrungsfrist bedingt eine Bewertung und Festlegung auf Ebene der Objekttypen sowie unterschiedliche Löschkonzepte, basierend auf Gesetzen, Verordnungen, Verträgen und Vereinbarungen

[29] nestor-Kriterien, Kriterienkatalog, vertrauenswürdige digitale Langzeitarchive - Version 2, S. 32
[30] nestor-Kriterien, Kriterienkatalog, vertrauenswürdige digitale Langzeitarchive - Version 2, S. 33

5.2. Objektverwaltung

Das elektronische Archiv ermöglicht die Verknüpfung von Daten (Objekten und Dokumenten), um Beziehungen zu identifizieren. Die Verwaltung dieser Beziehung kann über die Vergabe von Metadaten und Markierungen (Engl. Tags) erfolgen, die entweder manuell oder automatisch zu einer Verknüpfung von Daten (Objekttypen: Text, Bild, Ton) sowie der assoziierten Datenformate im Archiv führen. Dies ermöglicht die Recherche und das Auffinden über das eingegebene Schlagwort oder den Objekttyp hinaus, da die Objekte über Querverweise dargestellt werden.

Ein weiterer Aspekt der Objektverwaltung bezieht sich auf Aufbewahrungsfristen und die ihnen zugrunde liegenden gesetzlichen Vorgaben (siehe Kapitel 8). Hier können Dokumententypen auf inhaltlicher Objektebene klassifiziert werden. Beispielsweise ergeben sich aus den Dokumentklassen “Personalunterlagen”, “klinische Studie”, “Zulassungsunterlagen” unterschiedliche Aufbewahrungsfristen. Es ist zu beachten, dass sich während der Archivierung die Aufbewahrungsfristen ändern können (insbesondere bei klinischen Studien nach Zulassungen und Ländern). (siehe Kapitel mit Tabelle Aufbewahrungsdauer, Kapitel 8).

5.3. Administration der Zugangsberechtigungen

Die Nutzer, Rollen und Verantwortlichkeiten sind in Kapitel 3 bereits beschrieben worden. Das beschriebene abgestufte Nutzerkonzept muss über die gesamte Aufbewahrungsfristen verwaltet werden und bedarf einer regelmäßigen Überprüfung und ggf. einer Aktualisierung. Der verantwortliche Archivar hat sicherzustellen, dass die Zugangsberechtigungen zum elektronischen Archiv regelmäßig abgefragt bzw. festgelegt werden, sowie dass Nutzerrechte rechtzeitig entzogen werden (z.B. bei Abteilungswechsel oder Verlassen der Firma).

Die Nutzerrechte als Solche können sich u. U. von einfachen Leserechten zu Schreibrechten einzelner Nutzer ändern (z.B. Metadatennacherfassung durch Nutzer). Hierzu sollte eine Option vorhanden sein, um zeitlich begrenzte, protokollierte Änderung der Nutzerrechte zu ermöglichen (z.B. Auditorenzugang, Zugang für Projektmitarbeiter).

Die Nutzerverwaltung bedingt eine eindeutige Identifizierung der Nutzer. Im ortsunabhängigen und internationalen Kontext einer elektronischen Archivnutzung sollten Mechanismen bereitgestellt werden, um die Überprüfung der Identität der Nutzer zu gewährleisten. Hier kann z.B. die Steuerung über die Active Directory und/oder eine elektronische Signatur (siehe Kapitel 6.2) verwendet werden. Eine Risikobewertung sollte festlegen, ob die Nutzerrechteveränderung dem Changemanagement-Prozess unterliegen muss.

5.4. Metadatenverwaltung

Metadaten, die während der Aufbewahrungsfristen entstehen, werden erhoben und gespeichert, um oben genannte administrative Aufgaben zu erfüllen. Diese können in einem Metadatenschema erfasst werden, welches sich nach strukturellen (Format, Beziehungen), beschreibenden (Schlagworte), technischen (Prüfsummen), administrativen (Rollen) und rechtlichen Verwendungszwecken (DSGVO) richtet.

Metadatenschemata sind im Hinblick auf die Nachhaltigkeit, Kooperationen und den Datenaustausch zwischen Produzenten bzw. Lieferanten, elektronischem Archiv und Nutzern sinnvoll.[31]

Die Verwaltung von Metadatenschemata beinhaltet die Pflege definierter Felder, in denen die jeweiligen Inhalte erfasst werden, um eine sowohl für Menschen als auch Maschinen interpretierbare Datenstruktur zu gewährleisten.

Dafür müssen Regeln für die Feldeingabe festgelegt werden (z.B. Nutzung von kontrolliertem Vokabular). Das Datum für z.B. “Ende Aufbewahrungsfrist” bzw. “Archivierung bis” muss änderbar sein.

5.5. Verwaltung technischer Metadaten des Archivsystems

Verschiedene Werkzeuge ermöglichen die automatische Generierung bzw. Extraktion von technischen Metadaten bei der Archivverwaltung (z.B. Zugriffsprotokolle). Diese sind im Zusammenhang mit der Verwaltung als SIP zu verstehen und nicht als AIP (Kapitel OAIS). Hier ist z.B. die automatische Generierung von Zeitstempeln oder Prüfsummen notwendig um die Integrität (siehe Kapitel 6.1.3) zu gewährleisten. Die Verwaltung kann z.B. in Datenbanken und/oder XML-Strukturen[32] erfolgen.

Die technischen Metadaten sind definiert, um Interpretierbarkeit, Sicherung der Integrität sowie Authentizität und die Steuerung der Langzeiterhaltungs-maßnahmen zu gewährleisten.

[31] nestor-Kriterien, Kriterienkatalog, vertrauenswürdige digitale Langzeitarchive - Version 2, S. 22
[32] nestor-Kriterien, Kriterienkatalog, vertrauenswürdige digitale Langzeitarchive - Version 2, S. 33

5.6. Administration der Erhaltungsmaßnahmen

Erhaltungsstrategien dienen insbesondere dem Erhalt des Originals und dessen Lesbarkeit (siehe Kapitel 6). Für die Strategien wie Migration, Emulation und Datenintegritätschecks sollte ein Verwaltungskonzept erarbeitet werden, aus dem hervorgeht

- in welchem zeitlichen Abstand
- für welche Dokumente und Objekte
- für Hardware und Software

diese Maßnahmen durchgeführt werden.

Die Migration von Inhalten zwischen Objektklassen (dynamisch vs. statisch) und Datenformaten (proprietär vs. öffentlich) birgt besondere Risiken (z.B. Metadatenverlust bei Migration), diese sollten im Konzept beachtet werden (Siehe Kapitel 4.2 Datenformate). Folgende Fragen stellen sich dem Archivar bei der Erstellung einer Datenmigrationsstrategie:

- wird das Original weiter archiviert, obwohl dieses in Zukunft nicht mehr lesbar sein könnte (z.B. Zugriff auf Originalerfassungssystem)
- werden technische Metadaten wie Hashsummen bei Migration erneuert?
- wie werden diese Maßnahmen dokumentiert und geprüft (Validierung)?

Die Emulation von Systemen ist durch beschleunigte technische Weiterentwicklungen von besonderer Bedeutung, da zum einen die Authentizität von digitalen Objekten und deren Inhalte sowie die Funktionalität erhalten bleiben (siehe Kapitel 6 Erhaltungsstrategien). Für die Verwaltung von Emulatoren zur Erhaltung sollten diese mit den stetig aktualisierten Hard- und Software-Systemen abgestimmt werden. Jedes Aufrechterhalten von Emulationen bedarf einer regelmäßigen Bewertung, ob künftige Alternativen (Metadatenextraktion) eine weitere Emulation notwendig machen und Objektinhalte und Funktionalitäten auf alternativem Wege erhalten werden können.

5.7. Löschkonzepte und Rechtliche Vorgaben

Aus den gesetzlichen Vorgaben zur Aufbewahrungsdauer im GxP Umfeld (siehe auch Kapitel 8) und den datenschutzrechtlichen Bestimmungen (siehe auch Kapitel 9) ergeben sich administrative Aufgaben:

- in Abhängigkeit von GCP oder GLP festlegen von Studientyp-abhängigen Löschregeln in Verbindung mit Nutzerregeln z.B. durch Einbinden Dritter (z.B. Prüfer)
- Festlegung, ab welchem Zeitpunkt laut aktueller Datenschutzgrundverordnung (DSGVO) personenbezogene Daten gelöscht oder unter Umständen anonymisiert werden müssen
- Die vorgeschlagene Datenlöschung signalisiert, ob es sich um eine Pflichtlöschung aufgrund gesetzlicher Vorgaben handelt oder sie durch den Ablauf einer Mindestaufbewahrungspflicht induziert wird
- Workflow zur Verlängerung der Archivierung (u.a. Legal Hold, Zulassung)
- Komplette Löschung inklusive Backups
- Löschung von Querverweisen zur Vermeidung von „toten Links“
- Löschung von assoziierten Daten (z.B. Audit Trail, Checksummen, technische Metadaten)

Automatische Workflows ermöglichen ein geringes Eingreifen durch den Archivar, bedürfen aber einer klaren Festlegung der Regeln zur Löschung in einem Löschkonzept (siehe auch 8.2). Sämtliche, auch automatische, Löschungen müssen im System Audit Trail protokolliert und begründet werden.

5.8. Recherche

Über die Recherchefunktion (Suche) wird die Nutz- und Wiederauffindbarkeit der archivierten Daten sichergestellt. Dies dient einerseits regulatorischen Erfordernissen (v.a. Wiederauffindbarkeit) andererseits können über diese Funktion die in den Archivdaten gespeicherten Informationen für unternehmerische Zwecke genutzt werden (Archiv als Informationsquelle via Verknüpfungen und Beziehungen).

Im Vergleich zur Papierarchivierung werden die Vorteile eines elektronischen Archivsystems im Hinblick auf die Recherche besonders deutlich:

- Archivdaten sind über jedes Zugangssystem abrufbar
- Schnellerer Zugriff
- Mehrfachzugriff auf ein Archivobjekt
- Die Originaldaten bleiben beim lesenden Zugriff unversehrt, da bei der Ausgabe über das Recherchesystem lediglich eine Kopie des Originals erzeugt wird, während das Original sicher und unveränderbar gespeichert ist (s. OAIS Modell, DIP).
- Durch den letztgenannten Punkt ist die in einigen Regularien streng geregelte Zugangsberechtigung u. U. nicht mehr von der Papierwelt auf die elektronische Welt zu übertragen.

Für die Gewährleistung der Auffindbarkeit und Nutzung der Archivdaten über einen langen Zeithorizont ist ein sinnvolles Konzept für die Vergabe und Pflege der semantischen Metadaten (Verschlagwortung, Klassifizierung) notwendig. Diese Metadaten müssen die in den Archivdaten enthaltenen Informationen/Inhalte repräsentieren, wobei deren Extraktion durch KI-basierte Verfahren unterstützt werden können (z. B. automatische Metadatenextraktion). Unter Umständen reicht die alleinige Option der Volltextrecherche für die Vollständigkeit und Konsistenz der Rechercheergebnisse nicht aus. Um zu große Treffermengen einzugrenzen und die Auflistung der Suchergebnisse zu reproduzieren, sollten alternative Suchoptionen definiert und bereitgestellt werden und die Suchparameter speicherbar sein.

Neben der Suche nach den Inhalten der archivierten Daten müssen über die Suchfunktionen des Datenmanagements auch alle weiteren Metadaten such- und wiederauffindbar sein. Dazu zählt beispielsweise die Suche nach den im Archivsystem verwendeten Datenformaten (z. B. für erforderliche Erhaltungsmaßnahmen, s. Kapitel 6 Erhaltungsstrategien) oder auch die Suche nach dem Ersteller der Daten.

6. Erhaltungsstrategien

6.1. Erhaltungsstrategie

6.1.1. Ziel der Erhaltungsstrategie

Die Gewährleistung des langfristigen Erhalts der Nutzbarkeit von elektronischen Daten gehört zu den Kernaufgaben der elektronischen Archivierung und stellt aufgrund des stetigen technologischen Fortschritts und der daraus resultierenden Veralterung (Obsoleszenz) von Hard- und Software eine Herausforderung dar. Ziel der Entwicklung einer Erhaltungsstrategie ist deshalb, das Risiko des Verlustes des Informations- und Beweiswertes der Daten zu minimieren. Für den GxP-regulierten Bereich ergibt sich die Forderung nach Etablierung einer Erhaltungsstrategie aus den ALCOA + Prinzipien zur Datenintegrität[33], insbesondere des Erhalts des Originals (bzw. der signifikanten Eigenschaften) und dessen Lesbarkeit.

Bezüglich des „Erhalts des Originals“ muss zwischen Originalinhalten und Originalformaten unterschieden werden. Für die Archivierung ist der Erhalt der Originalinhalte (d.h. der signifikanten Inhalte und deren Eigenschaften) relevant. Die signifikanten Eigenschaften sind je Datenquelle zu definieren. Das originale Format kann (z. B. direkt im Rahmen des Archivierungsprozesses) über einen validierten Prozess in für die Archivierung geeignete Formate migriert werden, um die signifikanten Eigenschaften zu erhalten.

6.1.2. Risiken

Elektronische Daten müssen durch ein Zusammenwirken von Hard- und Software interpretiert werden, damit eine mit den menschlichen Sinnen wahrnehmbare Repräsentation entsteht. Dies muss zumindest für die Dauer der vorgeschriebenen Aufbewahrungsfristen gewährleistet sein.

Durch die Weiterentwicklung von Hard- und Software und der damit einhergehenden Veralterung der zum Zeitpunkt der Archivierung bestehenden Systeme, entsteht das Risiko, dass die exakte Darstellung (Lesbarkeit) von elektronischen Daten nach Hard- und Softwareerneuerungen nicht mehr möglich ist.

[33] WHO Guidance on Good Data Record Management Practices, World Health Organization (WHO Technical Report Series No.996), Annex 5, 2016, S. 183

Ein weiteres Risiko für die Integrität der Daten besteht in der begrenzten Haltbarkeit der Speichermedien. Beispielsweise wird bei einigen optischen und statischen Datenträgern von einer Haltbarkeit zwischen 5 und 10 Jahren ausgegangen.[34]

6.1.3. Maßnahmen für den Erhalt

Um den Erhalt von elektronischen Daten sicherzustellen ist es erforderlich, ein ganzheitliches Konzept zur Speicherung und dauerhaften Lesbarkeit zu entwickeln. Technische Entwicklungen müssen beobachtet, Anforderungsänderungen berücksichtigt und ggf. angemessen umgesetzt werden, was durch entsprechende Infrastruktur, Prozesse und Ressourcen gewährleistet sein muss.

Alle Lösungsansätze erfordern den Erhalt der signifikanten Eigenschaften (AIP im OAIS Modell bzw. siehe Zitat WHO Annex 5[35]) eines Datensatzes. Sie können einzeln oder in Kombination genutzt werden. Im Rahmen einer GxP-konformen Archivierung sind sämtliche Maßnahmen und Verfahren zu dokumentieren und – wo erforderlich- vor Erstanwendung zu validieren. Siehe auch Administration der Erhaltungsmaßnahmen (Kapitel 6.1.3).

6.1.3.1. Migration

Im Rahmen der Migration werden digitale Daten transferiert und ggf. in ein anderes Datenformat umgewandelt. Unterschieden wird dabei zwischen einer Hardware- und Softwaremigration.[36] In jedem Fall sollte ein geeignetes Konzept zur Erfolgskontrolle erstellt werden, um zu prüfen, dass alle Daten vollständig und lesbar migriert wurden.

[34] Schneider, Holger, 2012:: Digitale Amnesie: Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, BOD, S. 10

[35] "When the original system is retired or decommissioned, migration of the data to other systems or other means of preserving the data should be used in a manner that preserves the context and meaning of the data, allowing the relevant steps to be reconstructed", WHO Technical Report Series No.996, 2016, Annex 5 "Guidance on good data and record management practices", S. 204,

[36] Schneider; Holger, 2012: Digitale Amnesie Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, BOD, S. 123 f

Hardwaremigration (Datenträger/Speichermedien):

- Auffrischung (Refreshment): Medien werden durch neue Medien gleichen Typs ersetzt.
- Ersetzen (Replication): Migration auf andere elektronische Medien. Hierbei ist zu berücksichtigen, dass das neue Medium im Allgemeinen nicht ohne Änderung der Speicherinfrastruktur einzusetzen ist.

Softwaremigration:

- **Datenformate:** hier werden Daten von einem Datenformat in ein aktuelleres, möglichst standardisiertes und offengelegtes Format transformiert. (s. Kapitel 4.2 Datenformate: Erhaltung während der Langzeitarchivierung / Archivierungskonzept)
- **Versionen:** neuere Versionen von Software müssen abwärts kompatibel bezüglich Lesbarkeit und zugrundeliegenden Algorithmen zur Datenprozessierung sein. Bevor eine Software nicht mehr verfügbar ist, müssen die mit Hilfe dieser Software archivierten Daten in ein neues System oder Datenformat migriert werden können. Dies kann u. U. auch das Datenbankmanagement des Archivs selbst betreffen.

Die Erhaltungsmaßnahmen sind der Datenkomplexität anzupassen und insbesondere bei hoher Datenkomplexität risikobasiert zu betrachten. Bei der Migration müssen Metadaten (siehe Kapitel 5.4 Metadatenverwaltung) ebenso migriert werden.

6.1.3.2. Emulation

Eine weitere Erhaltungsstrategie liegt in der Emulation, bei der Computer bzw. deren Betriebssysteme durch Zusatzprogramme (Emulatoren) dazu veranlasst werden, alte Anwendungsprogramme auszuführen, um so veraltete Datenformate zu interpretieren. Der Vorteil liegt in der Erhaltung der Originalform der Daten, wodurch die Authentizität erhalten bleibt. Bei einer sehr langen Vorhaltung von Daten besteht allerdings die Gefahr, dass auch die Emulation an Grenzen stößt. Bei jedem Generationswechsel ist auch wiederum ein Emulator zu entwickeln und zu dokumentieren. Der Aufwand ist recht hoch und für komplexe Objekte schwierig. Das Wissen bezüglich der Bedienung der Altsysteme muss zusätzlich weitergegeben werden (z.B. Benutzerhandbuch, Faktor Mensch, Passwörter) und die Emulation hinsichtlich des Sicherheitskonzepts im jeweils aktuellen Umfeld bewertet und eingebunden werden. Die zunehmende Verbreitung der Virtualisierung ermöglicht jedoch auch in zunehmendem Maße virtuelle Maschinen vollständig zu archivieren.

6.1.3.3. Überprüfung der Datenintegrität

Gemäß der britischen Gruppe Health Sciences Records and Archives Association (HSRAA, früher SAG)[37] sollte die Unversehrtheit der digitalen Dokumente auf der Bit-Ebene mittels periodischer Prüfung der Checksummen überprüft/nachgewiesen werden.

Die periodische Überprüfung kann in modernen Speichersystemen wie z. B. Object Storages automatisiert werden. Erasure Coding Verfahren (Vorwärtsfehlerkorrekturcode) unterstützen die automatische Fehlerkorrektur. Dazu werden Daten in einer zu definierenden Anzahl von Kopien an unterschiedlichen Orten gespeichert. Im Hintergrund werden Speichersegmente (Slices) kontinuierlich gescannt und Abweichungen vom ursprünglichen Eintrag korrigiert. Bei der Qualifizierung des Object Storages ist die Überprüfung und Fehlerkorrektur zu berücksichtigen (z.B. bewusste Entfernung einer Storage Unit und daraus resultierende automatische Korrektur (inkl. systeminterner Dokumentation)). Prozedurale Anforderungen z.B. bezüglich Vorhaltung der Logfiles, Anzahl der Datenkopien, akzeptable Abweichungsrate, sollten seitens IT-Infrastruktur im Rahmen eines risikobasierten Ansatzes definiert und dokumentiert werden.

6.2. Elektronische Signaturen

6.2.1. Rechtsgrundlagen

Laut der EU-weit gültigen „VERORDNUNG Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ (eIDAS-VO), werden elektronische Signaturen definiert als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet“.[38] Fälschlicherweise wird der Begriff „digitale Signatur“ häufig synonym zur elektronischen Signatur verwendet, bezeichnet jedoch eine spezielle und mit Hilfe kryptographischer Verfahren erstellte elektronische Signatur.

[37] Scientific Archivists Group, Stiles, T. et al, 2014: Good Clinical Practice: A Guide to Archiving of Electronic Records, S. 21

[38] VERORDNUNG Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Art. 3, Nr.10

Mit der eIDAS-VO besteht für die EU ein einheitlicher Rechtsrahmen für die gegenseitige Anerkennung von elektronischen Signaturen. Darüber hinaus müssen für die außereuropäische Anerkennung ggf. noch weitere Regularien beachtet werden ebenso wie die GxP-spezifischen Richtlinien (z. B. WHO - Annex 5, FDA 21 CFR Part 11; Guidance for Industry - Part 11, Electronic Records; Electronic Signatures — Scope and Application) zu berücksichtigen sind.

Die Verwendung von elektronischen Signaturen und Zeitstempeln ermöglicht, die Echtheit eines elektronischen Dokuments und der darin enthaltenen Informationen zu bestätigen, sowie deren nachträgliche Modifikationen bzw. unautorisierte Änderungen sichtbar zu machen. Ferner dient die elektronische Signatur dazu die unterzeichnende Person als Eigentümer der Unterschrift zu identifizieren. Damit bilden elektronische Signaturen und die dazugehörigen Zeitstempel einen wichtigen Bestandteil zur Sicherstellung der Integrität der in elektronischen Dokumenten gespeicherten Informationen.

6.2.2. Formen der elektronischen Signatur

Gemäß der eIDAS-VO werden folgende Formen elektronischer Signaturen unterschieden:

- einfache elektronische Signatur (eIDAS-VO, Art. 3 No. 10)
- fortgeschrittene elektronische Signatur (eIDAS-VO, Art. 3 No. 11)
- qualifizierte elektronische Signatur (eIDAS-VO, Art. 3 No. 11) hat gem. § 25 (2) eIDAS die gleiche Rechtswirkung wie die handschriftliche Unterschrift.

Alle Formen der elektronischen Signatur können gültig sein. Unterschiede bestehen jedoch in der Beweiskraft. Die letztgenannte Form der qualifizierten elektronischen Signatur besitzt die höchste Beweiskraft.[39]

[39] Zivilprozessordnung (ZPO): § 371a Beweiskraft elektronischer Dokumente

6.2.3. Archivierung elektronischer Signaturen

Werden im GxP-Prozess elektronische Signaturen genutzt, darf der Archivierungsprozess die Beweiskraft und Rechtsgültigkeit nicht beeinträchtigen.

Während der Aufbewahrungsfrist stellt die Beweiskrafterhaltung und die Bewahrung der Rechtsgültigkeit elektronischer Signaturen aus den folgenden Gründen eine Herausforderung dar:

- Die elektronische Signatur muss für die Dauer der Aufbewahrungsfrist mit dem signierten Dokument verknüpft bleiben. Beispielsweise ist im WHO Annex 5, „Guidance on Good Data and Record Management Practices" festgelegt, dass Informationen zu elektronischen Signaturen als Teil des elektronischen Originals aufbewahrt werden müssen. Sie müssen der Aufzeichnung/dem Dokument eindeutig zuzuordnen sein und, unabhängig vom für die Archivierung verwendeten System, während der gesamten Aufbewahrungsfrist lesbar sein.[40]
- Kryptographische Algorithmen können veralten. „Hierdurch besteht gemäß IT Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) die Gefahr, dass im Falle der Kompromittierung von Kryptoverfahren oder Kryptoschlüsseln verschlüsselte Daten unbefugt entschlüsselt werden können, von Unbefugten Dokumente mit einer technisch gültigen Signatur versehen werden können, so dass dann authentische, signierte Dokumente nicht mehr von gefälschten unterschieden werden können."[41] Die europäische SOG-IS (Senior Official Group Information Information Systems Security) Expertengruppe prognostiziert in einem Algorithmenkatalog die Gültigkeitsdauer der Verschlüsselungsalgorithmen.
- Im Falle einer Migration oder Transformation von Dokumenten/Aufzeichnungen (s. auch Kapitel 4.2 Datenformate), können elektronische Signaturen ihre Gültigkeit verlieren und müssten in diesem Fall erneuert werden.[42]

[40] WHO Guidance on Good Data and Record Management Practices, World Health Organization (WHO Technical Report Series, No. 996) Annex 5, 2016, S. 192f

[41] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, 15. Ergänzungslieferung 2016, Kapitel G 4.47 Veralten von Kryptoverfahren, S. 1009

[42] Bundesministerium für Wirtschaft und Technologie: Handlungsleitfaden zur Aufbewahrung elektronisch signierter Dokumente, Dokumentation Nr. 564, Stand August 2007, S. 22

6.2.4. Maßnahmen für den Erhalt der Beweiskraft archivierter elektronischer Signaturen

Generell sollte risikobasiert für jeden Dokumententyp festgelegt und dokumentiert werden, welche Form der elektronischen Signatur erforderlich ist.[43]

- Die Funktion(en) der elektronischen Signatur innerhalb eines GxP relevanten computerisierten Systems müssen in der entsprechenden Nutzeranforderung (User Requirements Specification) adressiert sowie validiert werden.
- Bei der Nutzung digitaler, d. h. mit kryptographischen Mitteln erstellter Signaturen, sollten möglichst standardisierte Signaturformate (z. B. „e-Signature baseline profiles“ der EU[44] verwendet werden. Dadurch kann die langfristige Lesbarkeit und damit die Beweiskraft am ehesten gewährleistet werden und eine aufwändige Migration mit Nachsignaturverfahren ist unwahrscheinlicher.[45]
- Archivierung der Metadaten, die für die Verifizierung elektronisch signierter Dokumente erforderlich sind, um Echtheit und Gültigkeit einer Signatur nachträglich überprüfen zu können wie z. B. qualifizierte Zeitstempel gemäß eIDAS VO[46].

[43] Elektronische Signaturen: Empfehlung der Fachgruppe Informationstechnologie der Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik e. V. (APV) sowie der Expertengruppe Elektronische Signatur; Stand: 01.12.2010; Version 2.0, S. 21f

[44] s. eSignature standards: website https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature zuletzt aufgerufen am 22.08.2021

[45] BSI Technische Richtlinie 03125, Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-M2: Krypto-Modul, Bundesamt für Sicherheit in der Informationstechnik (BSI) Version 1.2.1. 15.03.2018

[46] Qualifizierte Zeitstempel werden nicht von einem lokalen Computer, sondern von einem gemäß eIDAS VO qualifizierten Trustcenter erzeugt. Bestätigt wird damit, dass digitale Daten und Dokumente zu der bestätigten Zeit so und nicht anders vorgelegen haben. S. auch eIDAS VO Rechtswirkung elektronischer Zeitstempel in Artikel 41, Abs. 2: „Für qualifizierte elektronische Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, *sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten*.“

6.2.5. Nachsignatur oder andere Maßnahmen der Beweissicherung

Eine digitale Unterschrift basiert auf asymmetrischer Verschlüsselung. Die zur Verschlüsselung genutzten Algorithmen haben eine begrenzte Gültigkeit[47]. Das im BSI-Grundschutzkatalog beschriebene Konzept sieht deshalb vor, rechtzeitig vor Ablauf der Gültigkeit eine Nachsignatur mit gültigem, neuerem Algorithmus durchzuführen und einen neuen qualifizierten Zeitstempel einzuholen, um den Beweiserhalt zu gewährleisten. Mit diesem als Nachsignatur (manchmal auch Übersignatur) bezeichneten Verfahren ist nicht gemeint, dass der ursprüngliche Unterzeichner das Dokument erneut unterschreiben muss. Dieser hat per Unterschrift den Inhalt freigegeben/bestätigt und Verantwortung übernommen. Die Nachsignatur hat jedoch den Zweck zu bestätigen, dass die Daten/Dokumente seit der Unterzeichnung nicht verfälscht, manipuliert oder modifiziert wurden. Erfolgt eine Nachsignatur nicht rechtzeitig (*vor* Ablauf der Gültigkeit des genutzten Algorithmus), kann u. U. die Integrität der ursprünglichen Signatur und in letzter Konsequenz der Beweiswert gem. § 371 a Zivilprozessordnung (ZPO) nachträglich in Frage gestellt werden. „Das ist ein entscheidender Unterschied zur manuellen Unterschrift auf Papier."[48]

Nach Risikobetrachtung gibt es auch die Möglichkeit, auf die Nachsignatur zu verzichten, da mit der Übergabe an das elektronische Archiv der Prozess für das jeweilige digital signierte Dokument abgeschlossen ist. In diesem Fall muss gewährleistet werden, dass der Archivierungsprozess sicher genug ist, eine Manipulation zu verhindern.[49]

Mit dem Konzept der Blockchain befindet sich derzeit ein weiteres Verfahren für den Erhalt des Beweiswertes von Dokumenten in der Entwicklung, für deren Anwendbarkeit es aber für diesen Bereich derzeit noch keine Standards zu geben scheint.[50]

---

[47] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, 15. Ergänzungslieferung 2016, Kapitel G 4.47 Veralten von Kryptoverfahren, S. 1009, s. a. Bundesamt für Sicherheit in der Informationstechnologie: OPS.1.2.2. Archivierung, 2.5: Unzureichende Erneuerung von kryptographischen Verfahren bei der Archivierung, Stand: Februar 2021

[48] Appel, B.: Archivierung elektronischer Daten im GxP Umfeld, Teil 3: Umsetzung der Archivierung elektronischer Daten – Ein Konzeptionspapier der Fachgruppe Informationstechnologie der APV, In: Pharmazeutische Industrie, 73, Nr. 7 (2011), S. 1212

[49] Appel, B.: Archivierung elektronischer Daten im GxP Umfeld, Teil 3: Umsetzung der Archivierung elektronischer Daten –Ein Konzeptionspapier der Fachgruppe Informationstechnologie der APV, In: Pharmazeutische Industrie, 73, Nr. 7 (2011), S. 1213

[50] Kusber, T. et al.: Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation. In: H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg): Open Identity Summit 2020, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, S. 49 ff

7. Identifizierung der zu archivierenden Daten und Verantwortlichkeiten

In den folgenden Unterkapiteln wird gemäß den geltenden regulatorischen Anforderungen pro GxP-Bereich sowie für die regulatorischen Anforderungen für Medizinprodukte beschrieben, welche Aufzeichnungen in Form welcher Daten bzw. Datenrepräsentationen zu archivieren sind und die Inhaber welcher Funktionen für die Identifizierung und Festlegung dieser Daten und deren Archivierung verantwortlich sind.

7.1. Gute Laborpraxis (GLP)

Nach Abschluss (oder Abbruch) einer GLP-Prüfung sind Prüfplan, Abschlussbericht[51], Rohdaten und weiteres damit zusammenhängende Material zu archivieren[52]. Zu den Rohdaten einer GLP-Prüfung zählen „alle ursprünglichen Aufzeichnungen und Unterlagen der Prüfeinrichtung oder deren überprüfte Kopien, die als Ergebnis der ursprünglichen Beobachtungen oder Tätigkeiten bei einer Prüfung anfallen“[53] und für die Rekonstruktion und Evaluierung des Berichts zu dieser Prüfung erforderlich sind.[54] Elektronische Rohdaten umfassen nicht nur die während der Prüfung aufgezeichneten eigentlichen Datenwerte, sondern auch die dazugehörenden Metadaten. Dazu zählen inhaltliche Metadaten (z. B. Prüfungsnummer, Zeitstempel, Identifizierungsnummern usw.) und technische Metadaten (z. B. Datenschlüssel, Feldbeschreibungen, Informationen über Datenverknüpfungen)[55] sowie elektronische Signaturen. Mit Hilfe der Metadaten können die Datenwerte zugeordnet, interpretiert und verstanden werden[56]. Die zu archivierenden Rohdaten sind jeweils spezifisch für die verwendeten computer-

[51] Im Fall des Abbruchs der Prüfung, sofern gefordert.

[52] OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), Paris 1999, Kapitel 10.1

[53] OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), Paris 1999, Kapitel 2.3 (7.)

[54] Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A – General, Part 58 (21 CFR 58): Good Laboratory Practice for Nonclinical Laboratory Studies, Definitions (k)

[55] Guidelines for the Archiving of Electronic Raw Data in a GLP Environment, Swiss Working Group on Information Technology (ArbeitsGruppe InformationsTechnologie, AGIT), o. O., Release Date: 31.01.2018, Version 2.0, Kapitel 4.2

[56] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung; 17), 22. Apr. 2016, Kapitel 3.3., Absatz 79

gestützten Systeme festzulegen.[57] Ebenfalls zu archivieren sind die Daten der Audit Trails der computergestützten Systeme, mit denen die Rohdaten aufgezeichnet und verarbeitet wurden, wobei die Zuordnung der Audit Trail-Daten zu den relevanten Rohdaten erhalten bleiben muss.[58] Zur Sicherstellung der Erhaltung von Inhalt und Bedeutung der Rohdaten während der gesamten Aufbewahrungsdauer sind demzufolge Rohdaten, Metadaten, Audit Trail-Daten und elektronische Signaturen als „Informationspaket" zu identifizieren und zu archivieren.[59] Außerdem sind zu archivieren:

- Erläuternde Informationen (z. B. Wartungsprotokolle, Aufzeichnungen über Kalibrierungen und Konfigurationen usw.), die benötigt werden, um die Validität von Rohdaten zu verifizieren oder um die gesamte Prüfung oder Teile davon zu rekonstruieren.[60]
- Weitere Informationen für die Interpretation und Evaluierung der Daten, die nicht in den Bericht Eingang gefunden haben, wozu u.a. auch Korrespondenz gehören kann.[61]
- Von spezifischen GLP-Prüfungen unabhängige Dokumentation, die notwendig ist, um die Übereinstimmung der Prüfeinrichtung mit den GLP-Grundsätzen nachzuweisen.[62]

---

[57] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung ; 17), Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Paris 22. Apr. 2016, Kapitel 3.2, Absatz 76 a)

[58] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung ; 17), 22. Apr. 2016, Kapitel 2.8., Absatz 69

[59] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung; 17 22. Apr. 2016, Kapitel 3.11., Absatz 114

[60] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung; 17), 22. Apr. 2016, Kapitel 3.2., Absatz 75

[61] Code of Federal Regulations, Title 40 - Protection of Environment, Environmental Protection Agency, Vol. 24, Part 160 Good Laboratory Practice Standards (40 CFR 160), Subpart J—Records and Reports § 160.190

[62] OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), Paris 1999, Kapitel 10.1 a)-g)

Die Daten können entweder im Original oder in Form überprüfter Kopien archiviert werden.[63] Entscheidend ist die Aufbewahrung der Daten in einer von Menschen lesbaren Form[64] sowie die Sicherstellung der kontinuierlichen Lesbarkeit, weshalb eine Migration in ein anderes Datenformat bzw. die Aufbewahrung der Daten in einem anderen System oder Speichermedien erforderlich werden kann.[65]

Die Leitung der Prüfeinrichtung hat als Dateneigner sicherzustellen, dass die zu archivierenden elektronischen Aufzeichnungen festgelegt werden und dass eine verantwortliche Person für die Führung der Archive bestimmt wird.[66] Verantwortlich für die Übergabe der Aufzeichnungen einer Prüfung zur Archivierung ist der Prüfleiter.[67] Es kann erforderlich sein, eine Frist festzulegen, innerhalb derer die Archivierung spätestens zu erfolgen hat, wie z. B. die von der FDA vorgeschlagene Zeitspanne von 2 Wochen.[68]

[63] Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A – General, Part 58 (21 CFR 58): Good Laboratory Practice for Nonclinical Laboratory Studies, §58.195

[64] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung; 17), 22. Apr. 2016, Kapitel 3.3., Absatz 79

[65] Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung; 17), 22. Apr. 2016, Kapitel 3.11., Absatz 114

[66] OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), 1999, Kapitel 1.1., Absatz 2. l)

[67] OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), 1999, Kapitel 1.2, Absatz 2 i)

[68] 21 CFR Parts 16 and 58 Good Laboratory Practice for Nonclinical Laboratory Studies; Proposed Rule: "In §58.33(b)(14), we propose adding a timeframe for archiving of no later than 2 weeks after the study completion date. We think that timely archiving of raw data, documents, protocols, specimens, and final reports will help prevent their loss or destruction. [...]. We propose the 2-week timeframe to allow flexibility for archiving material without jeopardizing study material integrity."

7.2. Gute klinische Praxis (GCP)

Zu archivieren ist der Master File über die klinische Prüfung (Trial Master File, TMF) bestehend aus den „wesentlichen Dokumenten" für die Durchführung einer klinischen Studie[69] sowie weiterer Dokumentation, die zum Nachweis der Übereinstimmung mit GCP-Anforderungen erforderlich ist, wozu auch nicht-studienbezogene Dokumentation zählt (z.B. SOPs, Validierungsdokumentation computergestützter Systeme). Die im TMF enthaltenen wesentlichen Dokumente und Daten sollen es ermöglichen, die Durchführung der Studie gemäß Studienprotokoll sowie die Qualität der dabei gewonnenen Daten zu prüfen und zu bewerten.[70] Der TMF ist aufgeteilt in einen TMF des Sponsors der klinischen Studie und in einen TMF des Prüfers (Investigator), auch genannt Investigator Site File (ISF) oder Site Master File (SMF). Der ISF/SMF beinhaltet u.a. auch personenbezogene Daten (Informed Consent Forms etc.), die unabhängig vom Sponsor archiviert werden müssen, da dieser kein Zugriffsrecht darauf haben darf. Die Verantwortung für die Archivierung ist demzufolge aufgeteilt zwischen Sponsor und Prüfer, wobei der Sponsor auch dafür zu sorgen hat, dass der Prüfer die Archivierung des ISF/SMF sicherstellt. Lediglich in wenigen Ausnahmefällen ist eine Archivierung des TMF ausschließlich durch den Prüfer zulässig.[71] Falls der Prüfer zur Erfüllung dieser Anforderung nicht in der Lage ist, sollte der Sponsor unter Beachtung des Schutzes der enthaltenen personenbezogenen Daten auch für die Archivierung des ISF/SMF Sorge tragen.[72]

Der Sponsor hat in seiner Organisation Personen zu benennen, die für die Archive zuständig sind.[73] Auch wenn die Führung des TMF während der laufenden Studie an Dienstleister (Auftragsforschungsinstitute, CROs) und ebenso die Archivierung an externe Dienstleister ausgelagert werden kann, liegt die Gesamtverantwortung für die Qualität, Integrität, Vertraulichkeit und die Verfügbarkeit der zum Sponsor-TMF

---

[69] Vgl. die Liste der „Essential Documents" in Guideline for good clinical practice EG(R2) Step 5, Kapitel 8

[70] Guideline of the content, management and archiving of the clinical trial maser file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 1

[71] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 3.1.

[72] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 6.4.

[73] Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG, Artikel 58; vgl. auch: Richtlinie 2005/28/EG der Kommission vom 8. April 2005 zur Festlegung von Grundsätzen und ausführlichen Leitlinien der guten klinischen Praxis für zur Anwendung beim Menschen bestimmte Prüfpräparate sowie von Anforderungen für die Erteilung einer Genehmigung zur Herstellung oder Einfuhr solcher Produkte, Artikel 19

zählenden Dokumente und Daten in jedem Fall beim Sponsor als Dateneigner.[74] Der Inhalt des TMF muss während der gesamten Aufbewahrungsfrist „vollständig erhalten und lesbar" bleiben.[75] Unter dieser Voraussetzung ist eine Migration in ein anderes Datenformat und auf andere Speichermedien (z. B. Digitalisierung von Papierdokumenten, mit dem Ziel, einen vollständigen e-TMF zu erzeugen) grundsätzlich zulässig. Digitalisierte Papierdokumente, welche anstelle des Originals Teil eines e-TMFs werden sollen, sollten dabei als verifizierte Kopien („certified copies") erstellt werden. Eine Vernichtung von Papier-Originalen darf dabei nicht ohne eine vorherige risikobasierte Qualitätskontrolle der Digitalisate und Genehmigung durch den Sponsor erfolgen.[76] Außerdem wird es innerhalb eines TMF Dokumente geben, die aus Gründen der Rechtssicherheit auch nicht durch eine verifizierte Kopie substituiert werden können (z. B. Verträge). Die Erstellung von Kopien solcher Dokumente und der Umgang damit bei gleichzeitiger Aufbewahrung der Originale ist in einer Verfahrensbeschreibung festzulegen.[77]
Ebenfalls aufzubewahren sind die für eine Rekonstruktion und Prüfung einer klinischen Studie erforderlichen „Source Documents" (Quelldaten z. B. die Patientenakten der Studienteilnehmer), welche „Source Data" (Laborbefunde usw.) enthalten, wofür der Prüfer bzw. beteiligte Labore etc. verantwortlich sind. Source Documents können entweder als Original oder in Form überprüfter Kopien aufbewahrt werden,[78] wobei allerdings für Patientenakten die Aufbewahrung im Originalformat empfohlen wird.[79] Dabei ist zu berücksichtigen, dass die Aufbewahrungsfristen für Quelldaten von denen für Studien-TMFs abweichen können (siehe Tabelle in Kapitel 8.1).

---

[74] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 6.1

[75] Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG, Artikel 58

[76] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 5.1.

[77] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 5.2.

[78] Reflection paper on GCP compliance in relation to trial master files (paper and/or electronic) for management, audit and inspection of clinical trials, Draft (EMA/INS/GCP/636736/2012), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 15 June 2015, Kapitel 8.1., Zeilen 427-433

[79] Reflection paper on GCP compliance in relation to trial master files (paper and/or electronic) for management, audit and inspection of clinical trials, Draft (EMA/INS/GCP/636736/2012), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 15 June 2015, Kapitel 8.1, Zeilen 427-429

7.3. Gute Herstellungspraxis (GMP)

Der pharmazeutische Unternehmer gemäß § 4 Abs. 18 des Arzneimittelgesetzes hat alle Aufzeichnungen über den Erwerb, die Herstellung einschließlich der Freigabe, die Prüfung, Lagerung, die Einfuhr oder die Ausfuhr und das Inverkehrbringen aufzubewahren.[80] Dies schließt die Aufbewahrung von Rohdaten jeglicher Form mit ein, die zuvor festzulegen sind.[81] Ebenfalls aufzubewahren sind Dokumente, die für das Qualitätsmanagementsystem notwendig sind (Site Master File, SOPs etc.). Die Aufbewahrung kann im Original oder als überprüfte Kopie erfolgen.[82] Die Zugriffsberechtigung zu den Aufzeichnungen ist auf dazu befugte Personen einzuschränken.[83] Weitere Anforderungen an die Verantwortlichkeiten für die Archivierung sind aus GMP-Regularien nicht zu entnehmen. Als Dateneigner ist der pharmazeutische Unternehmer anzusehen.

7.4. Gute Pharmakovigilanz-Praxis (GVP)

Der Zulassungsinhaber hat ein Records Management-System zu führen, welches sicherstellt, dass alle Dokumente im Zusammenhang mit Pharmakovigilanz-Aktivitäten aufbewahrt und verfügbar gehalten werden.[84] Die Aufbewahrung kann in elektronischer Form erfolgen, wobei auch eine Digitalisierung von Papierdokumenten zulässig ist, sofern die Vollständigkeit und Lesbarkeit gewährleistet wird.[85]

---

[80] Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) § 20, Abs. (1)

[81] EudraLex - The Rules Governing Medicinal Products in the European Union, Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation

[82] Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter C – Drugs: General, Part 211 (21 CRF 211): Current Good Manufacturing Practice for Finished Pharmaceuticals, Subpart J – Records and Reports, Section 211.180 (d)

[83] Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) § 20, Abs. (1)

[84] Guideline on good pharmacovigilance practices (GVP) Module I – Pharmacovigilance systems and their quality systems, European Medicines Agency (EMA) (EMA/541760/2011), 22 Jun. 2012, S. 9. Dazu auch: Durchführungsverordnung (EU) Nr. 520/2012 der Kommission vom 19. Juni 2012 über die Durchführung der in der Verordnung (EG) Nr. 726/2004 des Europäischen Parlaments und des Rates und der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vorgesehenen Pharmakovigilanz-Aktivitäten, Artikel 12, Satz 2

[85] Guideline on good pharmacovigilance practices (GVP) Module I – Pharmacovigilance systems and their quality systems, European Medicines Agency (EMA) (EMA/541760/2011), 22 Jun. 2012, S. 18

7.5. Medizinprodukte

Zwischen den regulatorischen Anforderungen für Medizinprodukte und GCP-Anforderungen gibt es Berührungspunkte, wenn eine Kombination aus einem Arzneimittel oder Wirkstoff und einem Medizinprodukt vorliegt.[86] Sowohl laut bisheriger Medizinprodukterichtlinie[87] als auch gemäß der 2017 in Kraft getretenen Medizinprodukteverordnung[88] ist der Hersteller des Medizinprodukts dafür verantwortlich, den zuständigen Behörden die geforderte Dokumentation während festgelegter Mindestzeiträume zur Verfügung zu halten. Falls der Hersteller keine eingetragene Niederlassung in einem EU-Mitgliedstaat hat, muss dessen Bevollmächtigter die Dokumentation im Namen des Herstellers den Behörden zur Verfügung halten.[89] Zu den aufzubewahrenden Unterlagen zählen die technische Dokumentation zur Baumusterprüfung und zur EU-Konformitätserklärung inklusive eventueller Nachträge und Ergänzungen, die Konformitätserklärung selbst sowie die Dokumentation über das Qualitätsmanagementsystem des Herstellers. Gemäß FDA-Anforderungen ist Dokumentation aufzubewahren, die unter „Device Master Record“, „Device History Record“, „Quality System Record“ und „Complaint Files“ zusammengefasst werden.[90]

---

[86] Siehe auch Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, Satz 10: „Produkte, die eine Kombination aus einem Arzneimittel oder Wirkstoff und einem Medizinprodukt sind, werden entweder von dieser Verordnung oder von der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates erfasst.“

[87] Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte.

[88] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.

[89] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, Anhang IX, Kapitel III, Abschnitt 7. Hinweis: Die Medizinprodukterichtlinie 93/42/EWG wird durch die am 25. Mai 2017 in Kraft getretene neue Verordnung über Medizinprodukte (EU) 2017/745 (auch bezeichnet als „Medical Device Regulation“ (MDR) mit einer Übergangfrist ersetzt.

[90] Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter H - Medical Devices, Part 820 Quality System Regulation (21 CFR 820)

8. Die Aufbewahrungsdauer GxP-relevanter Dokumentation

Die gesetzlich bzw. regulatorisch festgelegte Aufbewahrungsdauer GxP-relevanter Dokumentation ist grundsätzlich befristet. Zur Erfüllung dieser Anforderungen sind die Daten u. U. für sehr lange Zeiträume aufzubewahren, wobei der Erhalt von Integrität, Verfügbarkeit, Lesbarkeit und Interpretierbarkeit stets sicherzustellen ist. In neuerer archivfachlicher Literatur wird im Zusammenhang mit der Aufbewahrung elektronischer Aufzeichnungen oft der Begriff (digitale) „Langzeitarchivierung" verwendet, ein Begriff, der mitunter auch in Dokumente des GxP-Umfelds vordringt.[91] „Langzeit" ist jedoch nicht definiert, hat keinen Bezug zu einer bestimmten (Mindest-) Aufbewahrungsdauer, sondern „ist die Umschreibung eines nicht näher fixierten Zeitraumes, währenddessen wesentliche, nicht vorhersehbare technologische […] Veränderungen eintreten; Veränderungen, die sowohl die Gestalt als auch die Nutzungssituation digitaler Ressourcen in rasanten Entwicklungszyklen vollständig umwälzen können […] und die verantwortliche Entwicklung von Strategien, die den beständigen, vom Informationsmarkt verursachten Wandel bewältigen können", erfordern.[92] Insofern kann die GxP-konforme Archivierung digitaler Daten durchaus als Langzeitarchivierung bezeichnet werden.

Die folgende Tabelle listet eine Auswahl von Aufbewahrungszeiten für GxP-relevante Aufzeichnungen und Daten sowie für Dokumentation zu Medizinprodukten zusammen mit ihren regulatorischen Grundlagen auf. Der Schwerpunkt liegt dabei auf Regularien, die in der Europäischen Union in Kraft sind. Berücksichtigt wurden jeweils die längsten Aufbewahrungszeiten, die für einen Sponsor von nicht-klinischen bzw. klinischen Studien, einen pharmazeutischen Unternehmer oder Zulassungsinhaber mit Sitz in Deutschland sowie für einen Hersteller von Medizinprodukten gelten. Bei der Ermittlung relevanter Aufbewahrungsfristen sind ggf. weitergehende nationale regulatorische Anforderungen in den Ländern zu berücksichtigen, in denen eine Marktzulassung für ein Produkt besteht oder angestrebt wird. Darüber hinaus empfiehlt es sich, über regulatorisch festgelegte Fristen hinaus aufzubewahren, sofern dies im Unternehmensinteresse geboten erscheint.[93]

---

[91] Vgl. Guidelines for the Archiving of Electronic Raw Data in a GLP Environment, Swiss Working Group on Information Technology (ArbeitsGruppe InformationsTechnologie, AGIT), o. O., Release Date: 31.01.2018, Version 2.0.

[92] nestor Handbuch : eine kleine Enzyklopädie der digitalen Langzeitarchivierung, Version 2.3, 2010, S. 17f

[93] Vgl. z. B. §84 Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz - AMG) zur Gefährdungshaftung.

8.1. Aufbewahrungsfristen

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
GLP		
Gesetz zum Schutz vor gefährlichen Stoffen (Chemikaliengesetz – ChemG), Anhang 1 zu § 19a Absatz 1, Grundsätze der Guten Laborpraxis (GLP), Absatz 10.2	Daten und Aufzeichnungen zu GLP-Prüfungen und prüfungsunabhängige Dokumentation.	Mindestens 15 Jahre
GCP		
§ 13, Abs. (10), Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen (GCP-Verordnung – GCP-V)	Die wesentlichen Unterlagen der klinischen Prüfung einschließlich der Prüfbögen. Andere Vorschriften zur Aufbewahrung von medizinischen Unterlagen bleiben unberührt.	Mindestens 10 Jahre
Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel, Anhang I, Modul 5, Abschnitt 5.2 c)[94]	Die wesentlichen Unterlagen für die klinische Prüfung (einschließlich der Prüfbögen)	- Mindestens 15 Jahre nach Abschluss oder Abbruch der Prüfung, - oder mindestens zwei Jahre nach Erteilung der letzten Zulassung in der Europäischen Gemeinschaft, bis keine Zulassungsanträge in der Europäischen Gemeinschaft mehr anhängig sind oder in Aussicht stehen, - oder mindestens zwei Jahre nach dem formellen Abbruch der klinischen Entwicklung des Prüfpräparats.

[94] In 5.2 c) wird außerdem auf die Richtlinie 2001/20/EG verwiesen: „Bei innerhalb der Europäischen Gemeinschaft durchgeführten Prüfungen muss der Zulassungsinhaber zudem zusätzliche Vorkehrungen treffen, damit die Dokumentation gemäß der Richtlinie 2001/20/EG aufbewahrt wird und ausführliche Leitlinien umgesetzt werden“. In Richtlinie 2001/20/EG des Europäischen Parlaments und des Rates vom 4. April 2001 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Anwendung der guten klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Humanarzneimitteln, ist jedoch keine Aufbewahrungsdauer festgelegt.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
	Die medizinische Akte des Prüfungsteilnehmers	Sollte gemäß den geltenden Rechtsvorschriften und in Übereinstimmung mit der in der Klinik, in der Einrichtung oder der privat üblichen Höchstaufbewahrungsdauer aufbewahrt werden. Die Unterlagen können jedoch noch länger aufbewahrt werden, falls geltende gesetzliche Bestimmungen oder eine Vereinbarung mit dem Sponsor dies verlangen. Der Sponsor ist dafür zuständig, das Krankenhaus, die Einrichtung oder die Praxis zu informieren, wenn diese Unterlagen nicht länger aufbewahrt zu werden brauchen.
	Alle Versuchsunterlagen […]. Dazu gehören der Prüfplan mit der Begründung, Zielsetzung, statistischen Konzeption und Methodik der Prüfung sowie die Bedingungen, unter denen sie durchgeführt und geleitet wird, und ausführliche Angaben zum Prüfpräparat, dem Referenzarzneimittel und oder dem Placebo, die verwendet werden, die Standardarbeitsanweisungen (SOP), alle schriftlichen Stellungnahmen zum Prüfplan und zu den Verfahren, die Prüferinformation, die Prüfbögen für jede Versuchsperson, der Abschlussbericht, und gegebenenfalls die Auditbescheinigung(en).	Solange wie das Arzneimittel zugelassen ist.
	Abschlussbericht (einer klinischen Prüfung/Studie)	Weitere fünf Jahre, nachdem keine Zulassung für das Arzneimittel mehr besteht.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Richtlinie 2003/63/EG der Kommission vom 25. Juni 2003 zur Änderung der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel, Modul 5, Kapitel 5.1, Absatz c)	TMF, welcher eine Zulassung unterstützt.	Mindestens 15 Jahre nach Abschluss oder Abbruch der Prüfung, oder mindestens zwei Jahre nach Erteilung der letzten Zulassung in der Europäischen Gemeinschaft, bis keine Zulassungsanträge in der Europäischen Gemeinschaft mehr anhängig sind oder in Aussicht stehen, oder mindestens zwei Jahre nach dem formellen Abbruch der klinischen Entwicklung des Prüfpräparats.
	Prüfplan mit der Begründung, Zielsetzung, statistischen Konzeption und Methodik der Prüfung sowie die Bedingungen, unter denen sie durchgeführt und geleitet wird, und ausführliche Angaben zum Prüfpräparat, dem Referenzarzneimittel und oder dem Placebo, die verwendet werden, die Standardarbeitsanweisungen (SOP), alle schriftlichen Stellungnahmen zum Prüfplan und zu den Verfahren, die Prüferinformation, die Prüfbögen für jede Versuchsperson, der Abschlussbericht, und gegebenenfalls die Auditbescheinigung(en).	Solange, wie das Arzneimittel zugelassen ist.
	Abschlussberichte klinischer Studien.	Fünf Jahre nach Ende der Zulassung des Arzneimittels.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Richtlinie 2005/28/EG der Kommission vom 8. April 2005 zur Festlegung von Grundsätzen und ausführlichen Leitlinien der guten klinischen Praxis für zur Anwendung beim Menschen bestimmte Prüfpräparate sowie von Anforderungen für die Erteilung einer Genehmigung zur Herstellung oder Einfuhr solcher Produkte, Artikel 17; in Verbindung mit: Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 6.3.	TMF von Studien, die noch unter der Richtlinie 2001/20/EG durchgeführt wurden[95].	Mindestens fünf Jahre nach Abschluss der Studie
Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG, Artikel 58[96]	TMF (Sponsor und Prüfer)	Soweit in anderen Rechtsvorschriften der Union nicht ein längerer Zeitraum vorgeschrieben ist […] mindestens 25 Jahre
	Patientenakten der Studienteilnehmer	Gemäß nationalem Recht

[95] Richtlinie 2001/20/EG des Europäischen Parlaments und des Rates vom 4. April 2001 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Anwendung der guten klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Humanarzneimitteln.

[96] Die Verordnung (EU) Nr. 536/2014 ist seit 16. Juni 2014 in Kraft. Die Verordnung wird jedoch gemäß Artikel 99 in Verbindung mit Artikel 82 Absatz 3 erst gültig, wenn die in Artikel 82 beschriebene Funktionsfähigkeit des EU-Portals und der EU-Datenbank gewährleistet ist. Dies wird nicht vor 2022 erwartet.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018, Kapitel 6.3 In Verbindung mit: Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates vom 31. März 2004 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Spende, Beschaffung, Testung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen, Artikel 8 und Richtlinie 2006/86/EG der Kommission vom 24. Oktober 2006 zur Umsetzung der Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Rückverfolgbarkeit, der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen sowie bestimmter technischer Anforderungen an die Kodierung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen, Artikel 9	Dokumentation zur Rückverfolgbarkeit von Arzneimitteln für neuartige Therapien (Advanced Therapy Investigational Medicinal Product – ATIMP) im TMF des Sponsors und des Prüfers sowie in den Patientenakten der Studienteilnehmer.	30 Jahre nach dem Verfall des Produkts oder länger, falls notwendig gemäß Genehmigung der klinischen Studie (clinical trial authorisation – CTA).

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
GMP		
§ 20, Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) vom 3. November 2006 (BGBl. I S. 2523), zuletzt geändert durch Artikel 48 des Gesetzes vom 29. März 2017 (BGBl. I S. 626)	Alle Aufzeichnungen über den Erwerb, die Herstellung einschließlich der Freigabe, die Prüfung, Lagerung, das Verbringen in den oder aus dem Geltungsbereich des Arzneimittelgesetzes, die Einfuhr oder die Ausfuhr, das Inverkehrbringen einschließlich der Auslieferung sowie Aufzeichnungen über die Tierhaltung und Aufzeichnungen der oder des Stufenplanbeauftragten oder der nach § 19 Abs. 7 Satz 1 entsprechend beauftragten Person.	Mindestens bis ein Jahr nach Ablauf des Verfalldatums, jedoch nicht weniger als fünf Jahre. (§20, Abs. 1 AMWHV)
		Mindestens fünf Jahre nach Abschluss oder Abbruch der letzten klinischen Prüfung, bei der die betreffende Charge zur Anwendung kam. (§ 20, Abs. 4 AMWHV)
	Aufzeichnungen im Zusammenhang mit Blutzubereitungen, Sera aus menschlichem Blut und gentechnisch hergestellten Plasmaproteinen.	30 Jahre. (§ 20, Abs. 2 AMWHV)
	Aufzeichnungen mit den Angaben nach Anhang VI Teil A der Richtlinie 2006/86/EG[97] bei hämatopoetischen Stammzellen oder Stammzellzubereitungen aus dem peripheren Blut oder aus dem Nabelschnurblut.	Mindestens 30 Jahre. (§ 20, Abs. (5) AMWHV)
Richtlinie 2002/98/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Gewinnung, Testung, Verarbeitung, Lagerung und Verteilung von menschlichem Blut und Blutbestandteilen und zur Änderung der Richtlinie 2001/83/EG	Aufzeichnungen über die Informationen gemäß Richtlinie 2002/98/EG Anhänge II und IV und Artikel 29 Buchstabe b), c) und d).	15 Jahre

[97] Richtlinie 2006/86/EG der Kommission vom 24. Oktober 2006 zur Umsetzung der Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Rückverfolgbarkeit, der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen sowie bestimmter technischer Anforderungen an die Kodierung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Richtlinie 2003/94/EG der Kommission vom 8. Oktober 2003 zur Festlegung der Grundsätze und Leitlinien der Guten Herstellungspraxis für Humanarzneimittel und für zur Anwendung beim Menschen bestimmte Prüfpräparate, Artikel 9, Absatz 1	Chargenbezogene Unterlagen in Bezug auf Arzneimittel.	Mindestens ein Jahr über das Verfallsdatum der entsprechenden Chargen oder mindestens fünf Jahre über die Ausstellung der Bescheinigung gemäß Artikel 51 Absatz 3 der Richtlinie 2001/83/EG hinaus, wobei der längere Zeitraum gilt.
	Chargenbezogene Unterlagen in Bezug auf Prüfpräparate.	Mindestens fünf Jahre nach Abschluss oder formellem Abbruch der letzten klinischen Prüfung, bei der die betreffende Charge zur Anwendung kam.
	Die für die Genehmigung für das Inverkehrbringen erforderlichen Unterlagen.	Entsprechend Anhang I der Richtlinie 2001/83/EG, sofern dies für eine spätere Genehmigung für das Inverkehrbringen erforderlich ist.[98]

[98] Siehe Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel, Anhang I, Modul 5, Abschnitt 5.2 c)

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates vom 31. März 2004 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Spende, Beschaffung, Testung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen, Artikel 8, Absatz 4, In Verbindung mit: Richtlinie 2006/86/EG der Kommission vom 24. Oktober 2006 zur Umsetzung der Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Rückverfolgbarkeit, der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen sowie bestimmter technischer Anforderungen an die Kodierung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen, Artikel 9, Absatz 2.	Daten bei „Gewebebanken und für die Verwendung beim Menschen verantwortliche Einrichtungen“ zur Identifizierung von eingegangenen und verteilten Geweben und Zellen und zur Sicherstellung von deren Rückverfolgbarkeit. Laut Richtlinie 2004/23/EG kann die Aufbewahrung der Daten auch in elektronischer Form erfolgen.	30 Jahre.
Richtlinie (EU) 2017/1572 der Kommission vom 15. September 2017 zur Ergänzung der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates hinsichtlich der Grundsätze und Leitlinien der Guten Herstellungspraxis für Humanarzneimittel, Artikel 9, Absatz 1	Chargenbezogene Unterlagen.	Mindestens ein Jahr über das Verfallsdatum der entsprechenden Chargen oder mindestens fünf Jahre über die Ausstellung der Bescheinigung gemäß Artikel 51 Absatz 3 der Richtlinie 2001/83/EG hinaus, wobei der längere Zeitraum gilt.
EudraLex – The Rules Governing Medicinal Products in the European Union, Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Part I, Chapter 4: Documentation, Section 4.12	Critical documentation, including raw data (for example relating to validation or stability), which supports information in the Marketing Authorisation.	Whilst the authorization remains in force.
	Process validation data: accompanying raw data.	For a period at least as long as the records for all batches whose release has been supported on the basis of that validation exercise.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
GVP		
Durchführungsverordnung (EU) Nr. 520/2012 der Kommission vom 19. Juni 2012 über die Durchführung der in der Verordnung (EG) Nr. 726/2004 des Europäischen Parlaments und des Rates und der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vorgesehenen Pharmakovigilanz-Aktivitäten, Artikel 12, Satz 2	Die in Artikel 2 der Durchführungsverordnung (EU) Nr. 520/2012 mindestens geforderten Elemente der Pharmakovigilanzsystem-Stammdokumentation (pharmacovigilance system master file (PSMF))	Mindestens fünf Jahre nach der formellen Einstellung des in der Pharmakovigilanzsystem-Stammdokumentation beschriebenen Systems.
	Pharmakovigilanz-Daten und -Unterlagen für die einzelnen zugelassenen Arzneimittel.	So lange […], wie das Produkt zugelassen ist, sowie mindestens 10 Jahre nach Ablauf der Zulassung. Die Unterlagen müssen jedoch länger aufbewahrt werden, sofern die EU-Rechtsvorschriften oder einzelstaatliches Recht dies vorschreiben.[99]

[99] Vgl. z. B. §84 Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz - AMG) zur Gefährdungshaftung.

Regulatorische Grundlage	GxP-Dokumentation	Aufbewahrungsdauer
Medizinprodukte		
Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates	Technische Dokumentation, die EU-Konformitätserklärung sowie gegebenenfalls eine Kopie von gemäß Artikel 56 ausgestellten einschlägigen Bescheinigungen (i. e. die Konformitäts-bescheinigungen) einschließlich etwaiger Änderungen und Nachträge; die Dokumentation über das Qualitätsmanagement-system des Herstellers, einschließlich aller Aufzeichnungen sowie Prozess- bzw. Verfahrensbeschreibungen.	Mindestens zehn Jahre nachdem das letzte von der EU-Konformitätserklärung erfasste Produkt in Verkehr gebracht wurde. Bei implantierbaren Produkten mindestens 15 Jahre ab Inverkehrbringen des letzten Produkts. (Verordnung (EU) 2017/745, Artikel 10, Satz 8, Anhang IX, Kapitel III, Abschnitt 7.)
Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte	Technische Unterlagen über die Auslegung, die Herstellung und die Leistungsdaten des Produkts gemäss Anhang III, Abschnitt 3. Zum Antrag auf EG-Baumusterprüfung und eine Kopie der EG-Baumusterprüf-bescheinigung und ihrer Ergänzungen.	Mindestens fünf Jahre ab dem Zeitpunkt der Herstellung des letzten Produkts. Bei implantierten Produkten mindestens 15 Jahre ab der Herstellung des letzten Produkts. (Richtlinie 93/42/EWG, Anhang III, Abschnitt 7.3)
	Technische Dokumentation zur EG-Konformitätserklärung gemäss Richtlinie 93/42/EWG, Anhang VII, Abschnitt 3.	Mindestens fünf Jahre ab der Herstellung des letzten Produkts. Bei implantierten Produkten mindestens 15 Jahre ab der Herstellung des letzten Produkts. (Richtlinie 93/42/EWG, Anhang VII, Abschnitt 2.)
	Angaben zu den Erklärungen zu Produkten für besondere Zwecke gemäss Anhang VIII, Abschnitte 2.1, 2.2, 3.1, 3.2.	Mindestens fünf Jahre. Bei implantierbaren Produkten mindestens 15 Jahre. (Richtlinie 93/42/EWG, Anhang VIII, Abschnitt 4)
AITMP	EMA ISS GCP 856758 von 2018	Mindestens 30 Jahre nach Ablauf des Verfallsdatums des Produkts

8.2. Datenlöschung

Wie bereits im Kapitel „Datenverwaltung“ (Kapitel 5) angeführt, ergeben sich im Laufe der Lebensdauer der Archivobjekte Tätigkeiten zur Sicherstellung von deren Erhalt über die geforderte Aufbewahrungsdauer, deren Auffindbarkeit und dauerhaften Lesbarkeit.

Die Erstellung einer Aufbewahrungsrichtlinie, aus der sich sowohl rechtliche als auch unternehmerische Aufbewahrungsfristen entnehmen lassen, ist deshalb unerlässlich, um die Mindestaufbewahrungsdauer für die unterschiedlichen Archivobjekte bestimmen zu können.

Aber auch nach dem Ende der gesetzlich geforderten Aufbewahrungszeit (s. Übersicht Aufbewahrungsdauer), kann es aus unternehmerischer Sicht sinnvoll, ggf. auch zwingend erforderlich sein, Daten aufzubewahren. Daten, die einem „Legal Hold“, also einer Aufbewahrung aus juristischen Gründen (z.B. wegen eines anhängigen Rechtsstreits) unterliegen, dürfen z.B. nicht gelöscht werden. Da es auch im Laufe der Aufbewahrungsfrist Änderungen in gesetzlichen sowie organisationsinternen Aufbewahrungsfristen geben kann, dürfen archivierte Daten nicht nach Ende der ursprünglich festgelegten Aufbewahrungsdauer ungeprüft oder gar automatisch gelöscht werden. Bei bestimmten Informationen ist eine Löschung/ Anonymisierung von personenbezogenen Daten nach Ablauf der Aufbewahrungspflicht zwingend erforderlich (siehe Kapitel 9 Schutz personenbezogener Daten).

Die Nutzung der Metadaten für die Aufbewahrungsfristeinhaltung bietet, je nach Archivsystem, die Möglichkeit, Archivobjekte mit einer Markierung zu versehen („flaggen“). Diese Markierung würde die Objekte nach Ende der Aufbewahrungsfrist als zur Löschung vorgesehen kenntlich machen. Der Archivar informiert den Dateneigner, der die Löschung prüft und freigibt oder die Aufbewahrungsfrist verlängert. Der Archivar löscht das freigegebene Objekt, bzw. gibt die entsprechenden Anweisungen an eine ausführende Abteilung (IT) weiter.

Dem Audit Trail des Archivsystems kommt hierbei zentrale Bedeutung zu, da er als Nachweis der Löschung dient. Allerdings bieten nicht alle Audit Trails die Möglichkeit, den Löschgrund mit anzugeben.

Zusätzlich muss eine Möglichkeit der teilweisen Löschung von Informationen aus dem Archiv vorgesehen werden, die notwendig werden kann. Gründe hierfür können vielfältig sein, z.B.:

- „File splits“ im Rahmen des Verkaufs eines Produktes oder ganzer Firmenteile und die damit verbundene Herausgabe der zugehörigen Daten
- Firmentrennungen
- Auflösung von externen Archiven

Deshalb müssen bereits bei der Planung eines Archivs diese Punkte bedacht werden, damit eine Entnahme/ Löschung aus dem Archiv tatsächlich auch technisch möglich ist. Auch getrennte Zugriffsmöglichkeiten müssen implementiert werden, da Archivobjekte je nach Inhalt zwar aufbewahrt werden müssen, aber nicht von allen Nutzern des Archivs einsehbar sein dürfen. Ein Beispiel hierfür sind Studien- / Patienteninformationen, die Prüfärzten zur Verfügung stehen müssen, durch den Studiensponsor aber nicht eingesehen werden dürfen.

Nach erfolgter Risikobetrachtung ist eine Qualifizierung/ Validierung des Löschprozesses im Archivsystem durchzuführen und deren Dokumentation vorzuhalten. Die Löschung kann manuell erfolgen, oder, bei großen Informationspaketen hilfreich, auch automatisiert. Dies ist im Falle einer externen Auftragsvergabe, im Rahmen eines Audits des Archivanbieters zu prüfen (siehe Kapitel 3.4.2 und 3.4.3 Dienstleister). Relevante Details gilt es im entsprechenden Vertragswerk zu regeln.

9. Schutz personenbezogener Daten

Werden in einem GxP-Archiv personenbezogene Daten gespeichert, sind neben den jeweiligen GxP-Regularien auch die gesetzlichen Datenschutzbestimmungen zu beachten. Für den Europäischen Raum ist dies die seit Mai 2018 gültige Datenschutzgrundverordnung (DS-GVO).[100]

[100] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), im Folgenden DS-GVO). Für Deutschland existiert dafür ein Anpassungsgesetz. Darüber hinaus gilt für die Speicherung in Deutschland das „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/680 (Datenschutzanpassungs- und Umsetzungsgesetz EU – DSAngUG-EU

Personenbezogene Daten sind gemäß der DS-GVO definiert als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“ (s. DSGVO Art. 4, Nr.1). Zu dieser Kategorie gehören z. B. auch IP-Adressen, E-Mail-Adressen (wenn darin ein Personenname Bestandteil der Adresse ist) und pseudonymisierte Daten.

Wesentliche, den Bereich der Archivierung betreffende Bestimmungen sind:

- Personenbezogene Daten dürfen nur dann verarbeitet[101] werden, wenn die betroffene Person die Zustimmung dafür erteilt hat oder wenn eine gesetzliche Norm die Verarbeitung erlaubt bzw. vorschreibt. (Art. 6 DSGVO)
- Bestehen die Grundlagen für die Verarbeitung nicht mehr, müssen die Daten gelöscht werden (Art. 17 DSGVO).
- Es besteht ein Auskunftsrecht über die verarbeiteten Daten (Art. 15 DSGVO).
- Unter Umständen besteht ein Recht auf Berichtigung (Art. 16 Art. 16 DSGVO).
- In den Verzeichnissen von Verarbeitungstätigkeiten (Art. 30 DSGVO) sind u.a. Fristen für die Löschung der Daten anzugeben, was in der Regel den Aufbewahrungsfristen entsprechen dürfte.
- Archivierungssysteme können Gegenstand der technischen und organisatorischen Maßnahmen sein (Art. 32 DSGVO)
- Das Archivierungssystem kann auch im Rahmen einer Datenschutzfolgeabschätzung beurteilt werden müssen, beispielsweise im Falle der Archivierung pseudonymisierter Patientendaten.[102]

[101] „Verarbeitung“ wird in der DSGVO definiert als „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO)

[102] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“/ angenommen am 4. April 2017/zuletzt überarbeitet und angenommen am 4. Oktober 2017/Hrsg,: DATENSCHUTZGRUPPE NACH ARTIKEL 29; 17/DE, WP 248 Rev.01; S. 14

Für den Prozess der elektronischen Archivierung bedeutet oben Genanntes, Archivsysteme mit personenbezogenen Daten zu identifizieren und klassifizieren, diese Systeme den technischen und organisatorischen Maßnahmen zu unterziehen sowie Löschprozesse in Gang zu setzen, sobald die gesetzliche Grundlage für die Verarbeitung entfallen ist. Alternativ kann auch eine Anonymisierung der Daten in Betracht gezogen werden.[103]

Ansprechpartner in den Unternehmen/Institution sind die jeweils benannten Datenschutzbeauftragten, denen die Aufgabe obliegt, für die gesetzeskonforme Umsetzung des Datenschutzes zu sorgen. (Art. 39 DSGVO). Letztendlich verantwortlich für die Einhaltung der DSGVO ist die Unternehmens-/Institutions- oder Behördenleitung (Art. 4 Nr. 7 DSGVO).

10. Business Continuity und Disaster Recovery

Zur Sicherstellung der „Business Continuity“ müssen Notfallkonzepte vorliegen, die gewährleisten, dass kritische (Roh)Daten, Informationen oder ganze Archivsysteme wiederhergestellt werden können (Disaster Recovery). Bei Ausfällen sind Wiederherstellungszeiten und -fristen in Service Level Agreements und SOPs festzulegen. Die Notfallkonzepte und die darin definierten Maßnahmen sind von der verantwortlichen Organisation in regelmäßigen Abständen zu überprüfen. Deren Eignung, kritische Funktionen aufrecht zu erhalten bzw. wiederherzustellen, ist mittels regelmäßiger Übungen nachzuweisen. Die Organisation sollte die aus den kontinuierlichen Überlegungen und Übungen gewonnen Erkenntnisse nutzen, um vorbeugende Maßnahmen zu definieren und zu implementieren.[104]

[103] Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“: Arbeitshilfe zur Pseudonymisierung/Anonymisierung, Stand: 29. Juni 2018

[104] GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems; February 2008 Appendix O13 (Archiving and retrieval)

Die Notfallkonzepte und deren zugrundeliegenden Risikobetrachtungen müssen die spezifischen Charakteristika der gewählten Archivlösung berücksichtigen, die die Unveränderbarkeit, Authentizität und Verfügbarkeit der archivierten Daten/Informationen, gewährleisten. Zu diesen Charakteristika gehören beispielhaft:

a. Die obligatorische Alterung des Speichermediums und damit einhergehendes Risiko des Datenverlusts bei Hardware-basierten Archivlösungen[105].
b. Die Nutzung vorhandener Virtualisierungssoftware, Server-Infrastruktur sowie Betriebssystemen und das Risiko eingeschränkter Kompatibilität durch zukünftige Updates oder Upgrades bei Software-basierten Archivlösungen
c. Detaillierte Ausgestaltung des Vertrages hinsichtlich recovery time objective – RTO und recovery point objective – RPO, Datenlokalisation (auch für physisch getrennte "Disaster Locations"), Anforderungen an Datenschutz und Verschlüsselung, Recht auf Audit durch den Auftraggeber, etc. bei "Archiving as a Service" (AaaS) Lösungen. Durch die weitestgehende Abgabe der Kontrolle an den externen Anbieter müssen Risiken rechtzeitig identifiziert und in entsprechenden Vertragsklauseln mitigiert werden.

Für die Wiederherstellung kommt dem Sicherungsprozess (Backup) eine wichtige Rolle zu. Umfang und Frequenz der Sicherung müssen der Kritikalität der Daten/Information entsprechend definiert werden und ebenso wie die Wiederherstellung regelmäßig getestet werden.[106]

In allen Fällen und abhängig von der Kritikalität der archivierten Daten/Informationen ist die jeweilige Archivlösung durch geeignete organisatorische Vorkehrungen zu flankieren (z.B. Risikobewertung und –management, strenge Nutzerkontrolle, regelmäßige und unabhängige Audits, kontinuierliche Überwachung im Betrieb).[107]

---

[105] GAMP Good Practice Guide: Electronic Data Archiving, 2007; OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 15, Establishment and Control of Archives that Operate in Compliance with the Principles of GLP, 2007

[106] GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems; February 2008 Appendix O13 (Archiving and retrieval); Pharmaceutical Inspection Co-Operation Scheme (PIC/S) – PI 011-3, 2007

[107] GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems; February 2008 Appendix O13 (Archiving and retrieval); GAMP Good Practice Guide: Electronic Data Archiving, 2007, S. 35ff

11. Glossar

Begriff/Abkürzung	Erläuterung
Active Directory	Verzeichnisdienst zur Verwaltung von Nutzern, Nutzergruppen, Freigaben sowie Computern oder Servern in einem Netzwerk
ALCOA / ALCOA+	Englischsprachiges Akronym für Dateneigenschaften **A**ttributable = zurückführbar **L**egible = lesbar **C**ontemporaneous = zeitnah/zeitgleich **O**riginal = original/ursprünglich **A**ccurate = korrekt **+** Complete = vollständig **+** Consistent = konsistent **+** Availible = verfügbar **+** Enduring = dauerhaft
AIP	Archival Information Package = Archivinformationspaket
Archiv	Eine definierte Räumlichkeit oder ein Bereich (z.B. Schrank, Raum, Gebäude oder computergestütztes System) zur sicheren Archivierung und Aufbewahrung von Aufzeichnungen und Materialien
Archivar	Durch die Leitung der Organisation bestimmte Person, die für die Führung des Archivs (z.B. für Tätigkeiten und Verfahren) verantwortlich ist.
Archivprozess	Übertragung von Daten in eine gesicherte und definierte Umgebung zur Sicherstellung der Unveränderbarkeit und Einhaltung der Aufbewahrungsfristen sowie des kontrollierten Zugriffs.
Audit Trail	Protokollfunktion in einem IT-System, welche automatisch aufzeichnet, wann welcher Nutzer Daten eingibt, ändert oder löscht und so die Nachvollziehbarkeit von Änderungen ermöglicht. Der Audit Trail muss in menschenlesbare Form umgewandelt werden können.
Authentizität	Überprüfbarkeit der Echtheit und Vertrauenswürdigkeit von digitalen Dokumenten
Backup (Datensicherung)	Eine Kopie der aktuellen Daten, Metadaten und Systemkonfigurationseinstellungen, die für eine (Notfall-) Wiederherstellung des Systems, unter Wahrung der

Begriff/Abkürzung	Erläuterung
	Datenintegrität, aufbewahrt werden Ein Backup stellt keine Archivlösung dar!
Berechtigungskonzept	Ein Berechtigungskonzept ist ein formelles Verfahren zur Festlegung und Steuerung von Zugriffsrechten auf ein computergestütztes System und von Rechten in einem computergestützten System.
Change-Management Process/ Änderungsmanagement	Ein Verfahren, welches gewährleistet, dass Änderungen, die den validierten Zustand des computergestützten Systems beeinflussen könnten, dokumentiert und kontrolliert umgesetzt werden
Daten	Daten sind unabhängig vom Format und Medium (papierbasiert oder elektronisch). Diese werden zum Zeitpunkt der GxP-Aktivität erzeugt und ermöglichen eine vollständige und lückenlose Rekonstruktion der GxP-Aktivitäten Definition von Daten: Eine in formalisierter Weise rückinterpretierbare Repräsentation von Information, die zur Kommunikation, Interpretation oder Verarbeitung geeignet ist. Beispiele für Daten beinhalten eine Bitsequenz, eine Zahlentabelle, die Buchstaben auf einer Seite, die Tonaufnahmen einer sprechenden Person oder eine Mondgesteinsprobe[108].
Datenformat	Festlegung der Daten sowie deren Darstellung (z.B. xml, proprietär)
Datenintegrität	Umfang, in dem eine Sammlung von GxP-Daten durch effektive organisatorische, betriebliche und technische Mechanismen verwaltet wird, um die Zuverlässigkeit, Lesbarkeit und Interpretierbarkeit bzw. Deutbarkeit im Ursprünglichen Sinne der GxP-Daten zu gewährleisten
Datenkonvertierung	Datenkonvertierung: - von einer Datenbank in eine andere - in ein anderes Datenformat

[108] nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland (Hrsg.): Referenzmodell für ein Offenes Archiv-Informations-System - Deutsche Übersetzung 2.0 (nestor-materialien 16), S. 9

Begriff/Abkürzung	Erläuterung
	- Formatänderung in Zusammenhang mit einem Software Upgrade
digitale Daten	siehe elektronische Daten
DIP	Dissemination Information Package = Auslieferungsinformationspaket
Dynamische Daten	Dynamische Daten basieren auf unveränderlichen Originaldaten, deren editierbare (optische) Darstellung es erlaubt, die Bedeutung und Interpretation des Datensatzes zu beeinflussen (Suche, Auswertung oder Zusammenfassung.)
elektronisches Archiv	Computergestütztes System zur Archivierung digitaler Daten.
elektronische Daten	Daten in elektronischem Format deren Integrität, Identität, Authentizität und Lesbarkeit über die Dauer der Aufbewahrungsfrist zu gewährleisten ist.
EMA	European Medicine Agency
Emulation	Die Simulation der Eigenschaften eines Systems mit Hilfe geeigneter Software
eTMF	electronic Trial Master File
FDA	U.S. Food and Drug Administration
flaggen	Kennzeichnen von Daten in einer Datenbank
GxP	Zusammenfassende Abkürzung für GLP, GCP, GMP und ggf. für weitere „Gute Praxis“ Qualitätssicherungssysteme.
Hashwert / Prüfsumme	Mittel zur Erkennung von Veränderungen an Datenfiles. Bei Änderungen an den Datenfiles ändert sich auch der Hashwert.
Human readable format/ Menschen lesbares Format	Ein Datenformat ist „Menschen lesbar / human-readable“ wenn es Daten mit einer Software für Menschen lesbar oder interpretierbar darstellen kann
Indexierung	Verzeichnis zur Wiederauffindung von archivierten Daten
ISO	International Organization for Standardization
Legal Hold	Aufbewahrung (von Daten) aus juristischen Gründen
Metadaten	Metadaten beschreiben Eigenschaften anderer Daten und liefern Informationen über Kontext und Bedeutung.

Begriff/Abkürzung	**Erläuterung**
	Üblicherweise handelt es sich um Daten zur Beschreibung von Struktur, Datenelementen sowie Beziehungen zu anderen Daten.
MHRA	Medicines and Healthcare products Regulatory Agency
Migration	Transfer digitaler Information unter Erhalt der vollen Inhaltsinformation und Metadaten.
Offline - Archivierung	Archivierung auf Speichermedien (z.B. ext. Festplatten, USB-Sticks, WORM) oder einer Archivdatenbank
Online - Archivierung	Verbleib der zu archivierenden Daten im Produktivsystem (logisch oder physisch getrennt) unter der Kontrolle des Archivars
PDF	Portable Document Format
PDF/A	Elektronisches Dokumentenformat das für eine Langzeit-archivierung geeignet ist
Record(s)	Dokument(e)
Retention period	Festgelegter Zeitraum zur Aufbewahrung von Daten, häufig durch gesetzliche Vorgaben bestimmt
RTO	recovery time objective, tolerierbare Zeitspanne, die benötigt wird, um vom Ausfall zur Wiederherstellung einer Anwendung zu gelangen bzw. die Zeitspanne, die ein Netzwerk, ein computerisiertes System, eine Anwendung ausfallen kann ohne signifikanten Schaden hervorzurufen
SIP	SIP=Submission Information Package = Übergabeinformationspaket
SOG-IS	Senior Officials Group Information Systems Security
SOP	Standard Operating Procedure / Standard Arbeitsanweisung
Speichermedien	Digitale Datenträger
Transformation	Änderung des Datenformates unter Beibehaltung der Inhaltsinformation und Metadaten

Quellen- und Literaturverzeichnis

Anmerkung: Alle hier angegebenen Quellen, die im Internet verfügbar sind, wurden zuletzt am 22. August 2021 erfolgreich abgerufen.

Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV) vom 3. November 2006 (BGBl. I S. 2523), zuletzt geändert durch Artikel 48 des Gesetzes vom 29. März 2017 (BGBl. I S. 626). https://www.gesetze-im-internet.de/amwhv/AMWHV.pdf

Appel, Bernhard et al.: Archivierung elektronischer Daten im GxP Umfeld. Teil 3. Umsetzung der Archivierung elektronischer Daten – Ein Konzeptionspapier der Fachgruppe Informationstechnologie der APV, In: Die Pharmazeutische Industrie (Pharm Ind) 73 (2011), Nr. 7

Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme (ENV/JM/MONO(2016)13), (OECD-Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung ; 17), Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Paris 22. Apr. 2016. https://www.oecd.org/env/ehs/testing/OECD%20Advisory%20Document%2017%20GermanGQMA-final-OECD.pdf

Beratungsdokument der Arbeitsgruppe Gute Laborpraxis: Einrichtung und Betrieb von Archiven in Übereinstimmung mit den Grundsätzen der GLP (ENV/JM/MONO(2007)10) (OECD Schriftenreihe über Grundsätze der Guten Laborpraxis und Überwachung ihrer Einhaltung ; 15), Umweltdirektorat, Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Paris 2007. http://www.bfr.bund.de/cm/343/einrichtung-und-betrieb-von-archiven-in-uebereinstimmung-mit-den-grundsaetzen-der-glp.pdf

BSI Technische Richtlinie 03125 Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-M.2: Krypto-Modul (BSI TR-ESOR-M.2), Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Version 1.2.1 (auf Basis der eIDAS-Verordnung), 15.03.2018. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_M2_V1_2_1.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, 15. Ergänzungslieferung 2016, Kapitel G 4.47 Veralten von Kryptoverfahren. https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium Edition 2021, APP.4.3 Relationale Datenbanken, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6,

Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium, Bonn 2020.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

Bundesamt für Sicherheit in der Informationstechnik (BSI): Umsetzungshinweise zum Baustein OPS.1.2.2 Archivierung, o. O., o. J.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_OPS_1_2_2_Archivierung.pdf?__blob=publicationFile&v=1

Bundesministerium für Wirtschaft und Technologie: Handlungsleitfaden zur Aufbewahrung elektronisch signierter Dokumente, Dokumentation Nr. 564, Stand August 2007.
https://www.securepoint.de/fileadmin/securepoint/downloads/uma/bmwi-leitfaden.pdf

CEF Digital Connecting Europe: eSignature Standards.
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature

Code of Federal Regulation Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A – General, Part 11 Electronic Records; electronic Signatures.
CFR - Code of Federal Regulations Title 21 (fda.gov)

Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A – General, Part 58 (21 CFR 58): Good Laboratory Practice for Nonclinical Laboratory Studies.
https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=efe9768ef020e2f3b920dac105d868a9&mc=true&r=PART&n=pt21.1.58

Code of Federal Regulations Title 21 – Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter H - Medical Devices, Part 820 Quality System Regulation (21 CFR 820).
https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1&subpartNode=21:8.0.1.1.12.13

Code of Federal Regulations, Title 40 - Protection of Environment, Environmental Protection Agency, Vol. 24, Part 160 Good Laboratory Practice Standards (40 CFR 160).
https://www.gpo.gov/fdsys/pkg/CFR-2011-title40-vol24/xml/CFR-2011-title40-vol24-part160.xml

Data Integrity and Compliance with CGMP Guidance for Industry, Food and Drug Administration, (Pharmaceutical Quality/Manufacturing Standards (CGMP)), December 2018.
https://www.fda.gov/media/119267/download

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (Hrsg.): Arbeitshilfe zur Pseudonymisierung/Anonymisierung, Stand: 29. Juni 2018.
https://www.gesundheitsdatenschutz.org/download/Pseudonymisierung-Anonymisierung.pdf

PIC/S Guidance (PI 041-1) Good Practices for Data Management and Integrity in regulated GMP/GDP Environments, Pharmaceutical Inspection Co-operation Scheme (PIC/S), 10 August 2016.
https://www.picscheme.org/layout/document.php?id=714

Durchführungsverordnung (EU) Nr. 520/2012 der Kommission vom 19. Juni 2012 über die Durchführung der in der Verordnung (EG) Nr. 726/2004 des Europäischen Parlaments und des Rates und der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vorgesehenen Pharmakovigilanz-Aktivitäten, Artikel 21 (2).
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:159:0005:0025:DE:PDF

Elektronische Signaturen: Empfehlung der Fachgruppe Informationstechnologie der Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik e. V. (APV) sowie der Expertengruppe Elektronische Signatur; Stand: 01.12.2010; Version 2.0.
https://www.apv-mainz.de/fileadmin/dateiablage/Dokumente/Publikationen/Elektronische_Signatur_APV_Dokument_2.0_01.pdf

eSignature standards, zuletzt aufgerufen am 09.08.2021
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature

EudraLex - The Rules Governing Medicinal Products in the European Union Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use.
URL: http://ec.europa.eu/health/documents/eudralex/vol-4_en

Federal Register Vol. 81, No 164, Part IV, Department of Health and Human Services, Food and Drug Administration, 21 CFR Parts 16 and 58 Good Laboratory Practice for Nonclinical Laboratory Studies; Proposed Rule.
https://www.gpo.gov/fdsys/pkg/FR-2016-08-24/pdf/2016-19875.pdf

GAMP Good Practice Guide Electronic Data Archiving, International Society for Pharmaceutical Engineering (ISPE), Tampa, Fl., 2007

Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz - AMG) in der Fassung der Bekanntmachung vom 12. Dezember 2005 (BGBl. I S. 3394), zuletzt geändert durch Artikel 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2757).
https://www.gesetze-im-internet.de/amg_1976/AMG.pdf

Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz - TFG) vom 28. August 2007 (BGBl. I S. 2169), zuletzt geändert durch Artikel 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2757).
https://www.gesetze-im-internet.de/tfg/TFG.pdf

Good Clinical Practice : A Guide to Archiving, Scientific Archivists Group (SAG), 2nd ed. Jul. 2014.
https://the-hsraa.org/wp-content/uploads/2017/12/GCPArchiveGuideJul2014.pdf

Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz - TFG) vom 28. August 2007 (BGBl. I S. 2169), zuletzt geändert durch Artikel 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2757).
https://www.gesetze-im-internet.de/tfg/TFG.pdf

Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application; U.S. Department of Health and Human Services, Food and Drug Administration; August 2003.
https://www.fda.gov/media/75414/download

Guideline on good pharmacovigilance practices (GVP) Module I – Pharmacovigilance systems and their quality systems, European Medicines Agency (EMA) (EMA/541760/2011), 22 Jun. 2012.
http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2012/06/WC500129132.pdf

Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 06. Dec. 2018.
https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-content-management-archiving-clinical-trial-master-file-paper/electronic_en.pdf

Guidelines for the Archiving of Electronic Raw Data in a GLP Environment, Swiss Working Group on Information Technology (ArbeitsGruppe InformationsTechnologie, AGIT), o. O., Release Date: 31.01.2018, Version 2.0.
https://www.anmeldestelle.admin.ch/dam/chem/de/dokumente/download-listen/aagit/agit-guidelines-archiv-electr-raw-data.pdf.download.pdf/AGIT_Guidelines_Archiving_Electr_Raw_Data_EN.pdf

Guideline for good clinical practice EG(R2) Step 5 (EMA/CHMP/ICH/135/1995).
https://www.ema.europa.eu/en/documents/scientific-guideline/ich-e-6-r2-guideline-good-clinical-practice-step-5_en.pdf

Keitel, Christian ; Schoger, Astrid: Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644 (Beuth Kommentar), Beuth Verlag GmbH, Berlin 2013

Kriterienkatalog vertrauenswürdige digitale Langzeitarchive: Version 2, nestor-Arbeitsgruppe Vertrauenswürdige Archive - Zertifizierung (nestor-materialen 8), Frankfurt am Main, 2008.
http://d-nb.info/1000083241/34

Koordinierungsstelle für die dauerhafte Archivierung elektronischer Unterlagen (KOST): Katalog archivischer Dateiformate.
https://kost-ceco.ch/wiki/whelp/KaD/index.php

Kusber, T. et al.: Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation. In: H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg): Open Identity Summit 2020, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, S. 49 ff.
https://dl.gi.de/bitstream/handle/20.500.12116/33181/proceedings-04.pdf?sequence=1&isAllowed=y

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risikomit sich bringt“/ angenommen am 4. April 2017/zuletzt überarbeitet und angenommen am 4. Oktober 2017. https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

nestor Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung, Version 2.3, 2010, hrsg. v. H. Neuroth, A. Oßwald, R. Scheffel, S. Strathmann, K. Huth im Rahmen des Projektes: nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen für Deutschland nestor – Network of Expertise in Long-Term Storage of Digital Resources. http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch_23.pdf

nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen für Deutschland (Hrsg.): nestor Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung 11.2 Digitale Speichermedien.
http://nestor.sub.uni-goettingen.de/handbuch/artikel/nestor_handbuch_artikel_249.pdf

nestor - Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland (Hrsg.): Referenzmodell für ein Offenes Archiv-Informations-System - Deutsche Übersetzung 2.0 (nestor-materialien 16).
https://d-nb.info/104761314X/34

MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018, Medicines and Healthcare Regulatory Agency (MHRA), o. O., March 2018.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997) (ENV/MC/CHEM(98)17), OECD Veröffentlichungen zur Umweltsicherheit und -hygiene (EHS) (Schriftenreihe über Grundsätze der Guten Laborpraxis und Überwachung ihrer Einhaltung ; 1), Umweltdirektorat Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Paris 1999.
https://mobil.bfr.bund.de/cm/343/oecdgs97.pdf

Reflection paper on GCP compliance in relation to trial master files (paper and/or electronic) for management, audit and inspection of clinical trials, Draft (EMA/INS/GCP/636736/2012), European Medicines Agency (EMA), Good Clinical Practice Inspectors Working Group (GCP IWG), 15 June 2015.
http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2013/02/WC500138893.pdf

Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:de:PDF

Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001L0083:20070126:de:PDF

Richtlinie 2002/98/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Gewinnung, Testung, Verarbeitung, Lagerung und

Verteilung von menschlichem Blut und Blutbestandteilen und zur Änderung der Richtlinie 2001/83/EG.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0098:20090807:DE:PDF

Richtlinie 2003/63/EG der Kommission vom 25. Juni 2003 zur Änderung der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel.
https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2003_63/dir_2003_63_de.pdf

Richtlinie 2003/94/EG der Kommission vom 8. Oktober 2003 zur Festlegung der Grundsätze und Leitlinien der Guten Herstellungspraxis für Humanarzneimittel und für zur Anwendung beim Menschen bestimmte Prüfpräparate.
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003L0094&from=EN

Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates vom 31. März 2004 zur Festlegung von Qualitäts- und Sicherheitsstandards für die Spende, Beschaffung, Testung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen.
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32004L0023&from=DE

Richtlinie 2005/28/EG der Kommission vom 8. April 2005 zur Festlegung von Grundsätzen und ausführlichen Leitlinien der guten klinischen Praxis für zur Anwendung beim Menschen bestimmte Prüfpräparate sowie von Anforderungen für die Erteilung einer Genehmigung zur Herstellung oder Einfuhr solcher Produkte.
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32005L0028&from=SK

Richtlinie (EU) 2017/1572 der Kommission vom 15. September 2017 zur Ergänzung der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates hinsichtlich der Grundsätze und Leitlinien der Guten Herstellungspraxis für Humanarzneimittel.
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017L1572&from=DE

Richtlinie 2006/86/EG der Kommission vom 24. Oktober 2006 zur Umsetzung der Richtlinie 2004/23/EG des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an die Rückverfolgbarkeit, der Meldung schwerwiegender Zwischenfälle und unerwünschter Reaktionen sowie bestimmter technischer Anforderungen an die Kodierung, Verarbeitung, Konservierung, Lagerung und Verteilung von menschlichen Geweben und Zellen.
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32006L0086&from=ET

Schneider, Holger: Digitale Amnesie : Langzeitarchivierung digitaler Dokumente im betrieblichen Umfeld, Books on Demand, Norderstedt, 2012

Scientific Archivist Group: A Guide to Archiving of Electronic Records, Scientific Archivists Group Limited, 2014.
https://the-hsraa.org/wp-content/uploads/2017/12/AGuidetoArchivingElectronicRecordsv1.pdf

Terhechte, Arno et al: Datenintegrität: Static Data vs. Dynamic Data, In: Die Pharmazeutische Industrie (Pharmind), 79 (2017)

Universität Konstanz (Hrsg.): Forschungsdateninfo: Formate erhalten.
https://www.forschungsdaten.info/themen/veroeffentlichen-und-archivieren/formate-erhalten/#c290996

Verordnung (EU) Nr. 536/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über klinische Prüfungen mit Humanarzneimitteln und zur Aufhebung der Richtlinie 2001/20/EG.
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0536&from=DE

Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (Text von Bedeutung für den EWR).
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0745&from=DE

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE

Verordnung über die Anwendung der Guten Klinischen Praxis bei der Durchführung von klinischen Prüfungen mit Arzneimitteln zur Anwendung am Menschen (GCP-Verordnung - GCP-V).
https://www.gesetze-im-internet.de/gcp-v/GCP-V.pdf

WHO Guidance on Good Data and Record Management Practices, World Health Organization (WHO Technical Report Series, No. 996), Annex 5, o. O., 2016.
https://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf

Zivilprozessordnung (ZPO): § 371a Beweiskraft elektronischer Dokumente.
https://www.gesetze-im-internet.de/zpo/__371a.html