Archivierung elektronischer Daten im GxP-Umfeld

Teil 3*): Umsetzung der Archivierung elektronischer Daten – Ein Konzeptionspapier der APV-Fachgruppe Informationstechnologie

Dr. Bernhard Appel[1], Dr. Christoph Hornberger[2], Dr. Jannis Batoulis[3], Konstantin Clevermann[4], Ralf Hössel[5], Dieter Weiser[6]

Roche Diagnostics GmbH[1], Mannheim, EMR Engineering GmbH[2], Ingelheim, Bayer Business Services[3], Leverkusen, Software AG[4], Düsseldorf, Boehringer Ingelheim Pharma GmbH & Co. KG[5], Ingelheim, Nycomed GmbH[6], Konstanz

Im dritten und letzten Teil der Reihe zur Archivierung elektronischer Daten im GxP-Umfeld wird das Thema Umsetzung der Archivierung elektronischer Daten beleuchtet. Aus dem System-Lebenszyklus werden die Phasen Systemanforderungen sowie Entwurf und Test behandelt, wobei speziell auf die Festlegung der aufzuzeichnenden Daten, der Aufbewahrungsgrundsätze und der Archivierungsstrategie eingegangen wird. Der Artikel schließt mit einem kurzen Abriss über die Lebenszyklusphasen Implementierung und Betrieb ab.

1. Einleitung

Der folgende Beitrag ist der dritte Teil einer mehrteiligen Reihe zum Thema Archivierung elektronischer Daten im GxP-Umfeld, die von der Fachgruppe Informationstechnologie der APV erarbeitet wurde. Im ersten Teil [1] wurden die Prozesse und Rollen bei der elektronischen Archivierung vorgestellt. Im zweiten Teil [2] ging es um die Anforderungen zur Reproduzierbarkeit von GMP-Daten. Im vorliegenden dritten und letzten Teil beschäftigen wir uns mit der Umsetzung der Archivierung.

Wie im GAMP Good Practice Guide [3] zur Archivierung und im ersten Teil unserer Artikelserie zur Archivierung bereits beschrieben, folgt die Archivierung allgemein einem Lebenszyklus bestehend aus

1. Festlegen der Systemanforderungen
   - Festlegen der GxP-Aufzeichnungen und der Daten
   - Festlegen der Aufbewahrungsgrundsätze (z. B. SOP) und des Sicherheitsniveaus
2. Entwurf und Test, Festlegen der Archivierungsstrategie / Erstellen des Archivierungskonzepts
3. Systemimplementierung
4. Betrieb bis zur Stilllegung
   - Umsetzung der Archivierungsstrategie(-konzepts)
   - Verifizieren der Archivierungsaktivitäten
   - Auffrischen oder Regenerieren (Datenaufnahme in das Archiv)
   - Datensuche und Abruf (Search/Retrieve)
   - Überwachung der laufenden Verfügbarkeit (Datenmaintenance)
   - Aufzeichnen der Vernichtung von Daten entsprechend der Grundsätze über das Löschen archivierter Daten

Im vorliegenden Artikel beschäftigen wir uns mit den Punkten 1 bis 4.

*) Teil 2 siehe Pharm. Ind. 2010;72(2):218-222 (Weiser).

2. Festlegen der Systemanforderungen

Klar definierte Anforderungen an das Archivsystem, eine Beschreibung des Archivierungsprozesses und eine Festlegung der zu archivierenden Daten sind wichtige Bestandteile eines erfolgreichen Archivierungsprojekts.

Mit Hilfe von klar definierten Anforderungen und gut strukturierten Archivierungsprozessen kann der nötige Aufwand und die Komplexität einer Archivierungslösung maßgeblich gesteuert werden. Zur Ermittlung der Anforderungen an das Archivsystem sollten die Aufbewahrungsanforderungen der zu archivierenden elektronischen Daten und die User Requirements des Quellsystems der zu archivierenden Daten (Produktivsystem) herangezogen werden. Aus diesen Dokumenten können dann die Anforderungen abgeleitet werden, die für die Archivierung der elektronischen Daten erforderlich sind.

Für eine effiziente und regelgerechte Archivierung sind ebenso die Prozesse der Archivierung, des Datenabrufs und der Datenlöschung vorher zu planen und festzulegen. Die Kenntnis der genauen Prozessabläufe erlaubt es die konkreten IT-spezifischen Anforderungen zu formulieren.

Bei der Festlegung der Prozesse sind regulatorische Anforderungen zu berücksichtigen. So kann der Ablauf der Archivierung – und Wiederverwendung – einer präklinischen Prüfung grundsätzlich anders verlaufen als der Ablauf der Archivierung einer Chargendokumentation.

■ 2.1 Festlegen der GxP-Aufzeichnungen und der Daten

Es ist wichtig vorher festzulegen, welche Daten zu archivieren sind und diese Entscheidung entsprechend zu dokumentieren. In vielen Fällen hat nur eine Teilmenge der Daten Einfluss auf die Patientensicherheit und Produktqualität oder dienen dem Nachweis der Patientensicherheit und Produktqualität und sind somit GMP-relevant. Unter Umständen kann es jedoch technisch einfacher sein, einen kompletten Datenbestand zu archivieren, statt die GMP-relevanten Daten zu selektieren.

Bei einfachen, dateibasierten Daten ist eine Festlegung der zu archivierenden Daten vergleichsweise einfach, bei Daten in komplexen Datenbanken stellen sich folgende Fragen:

- Muss die komplette Datenbank erhalten werden?
- Sind nur einzelne Datensätze relevant?
- Welche Eigenschaften/Metadaten der Daten müssen archiviert werden?
  - Welche Relationen sind zum Erhalt der Information erforderlich?
  - Sind die Daten mit den Signaturen verknüpft und ggf. verschlüsselt?
  - Müssen Audit-Trail-Informationen mit abgespeichert werden?
  - Sind Zugriffsberechtigungen zu erhalten?
  - Müssen Daten reprozessierbar sein (siehe Teil 2 der Artikelserie)?
  - Müssen Daten auswertbar sein (Statistik, Trendanalyse)?
- Ist es ausreichend, lediglich entsprechend erzeugte Berichte aus der Datenbank zu archivieren?

Ebenso wichtig ist eine generelle Abklärung und Festlegung zur Frage, was an den archivierten Daten geändert werden darf. Relevante Informationen dürfen sicherlich nicht verändert werden. Die Datenintegrität und Datenauthentizität ist sicherzustellen und die ursprünglichen Informationen, die eigentliche Bedeutung der Daten, dürfen nicht verfälscht werden. Jedoch können sich während der Aufbewahrungszeit Ergänzungen zu den Daten ergeben, die für die Datenpflege notwendig sind, z. B. die erneute Signatur eines Datensatzes.

Auch Metadaten liegen im Fokus der Archivierungsstrategie. Zwar sind Metadaten in vielen Fällen nicht archivierungsrelevant, jedoch muss in Abhängigkeit zur Bedeutung der Metadaten bewertet werden, ob einzelne Metadaten nicht doch zu archivieren sind. Es bietet sich an, eine Klassifizierung für Metadaten vorzunehmen.

In der Praxis sind diejenigen Metadaten archivierungsrelevant, die für die Bedeutung und/oder den Kontext der Daten oder zur Interpretation der Daten benötigt werden. Dabei ist zu berücksichtigen, dass die heute verwendeten Metadaten, d. h. Metadaten, die heute im täglichen Betrieb zum Verständnis der eigentlichen Daten beitragen, möglicherweise nicht ausreichen, um dieselben Daten in 20 Jahren auch interpretierbar zu machen. Ist etwa die Abkürzung einer Abteilungsbezeichnung wichtig für die Interpretation der Daten, dann kann man davon ausgehen, dass die Verwendung dieser Abkürzung das spätere Verständnis der Daten erschweren wird. Mit anderen Worten: Es kann im Einzelfall durchaus sinnvoll sein, einige weitere Metadaten hinzuzufügen. Zur weiteren Aufdeckung solcher Abhängigkeiten kann es empfehlenswert sein, eine Risikobetrachtung/Risikoanalyse über die zu archivierenden Metadaten durchzuführen.

■ 2.2 Festlegung der Aufbewahrungsgrundsätze

2.2.1 Festlegen des Sicherheitsniveaus

Das zu erreichende Sicherheitsniveau lässt sich wie folgt charakterisieren:

- Erfüllung gesetzlicher sowie organisationsinterner Anforderungen an den Schutz der Daten bei der Archivierung sowie darüber hinaus (z. B. nach Entsorgung der Datenträger),
- Widerstandsfähigkeit gegen versehentlichen Datenverlust und unbeabsichtigte Datenbeschädigung,
- Widerstandsfähigkeit gegen Manipulation,
- Widerstandsfähigkeit gegen interne und externe Angriffe auf die gespeicherten Daten sowie das IT-System selbst.

Es bietet sich an, Daten und Dokumente risikobasiert zu klassifizieren. Das Sicherheitsniveau kann dann anhand dieser Klassifikation detaillierter differenziert werden. Abhängig von der Klassifikation können unterschiedliche Sicherheitsstandards gefordert werden. Hier ein Beispiel für eine stufenweise Erhöhung der Sicherheit:

1. Das Archiv-System hat einen Backup.
2. Die archivierten Objekte werden zusätzlich zu 1. in einem weiteren System kopiert.
3. Zusätzlich zu 2. wird an dritter Stelle ein hash-Wert der archivierten Objekte geführt, sodass man bei einem auftretenden Unterschied der archivierten Daten entscheiden kann, welches Objekt „das richtige“ ist.
4. Zusätzlich zu 3. werden Original und Kopie nochmals kopiert und an einem geographisch weit entfernten Ort gehalten

2.2.2 Aufbewahrungsdauer

Die Aufbewahrungsdauer ergibt sich normalerweise zwangsläufig aus GxP-Regularien z. B. der AMWHV. Weitere Beispiele hierzu finden sich auch im GAMP Good Practice Guide

Pharm. Ind. 73, Nr. 7, 1207–1215 (2011)

Electronic Data Archiving. Die Anforderungen können firmenspezifisch deutlich höher liegen. Neben der Mindestaufbewahrungsdauer ist in vielen Fällen auch eine maximale Aufbewahrung definiert, die firmenintern definiert wird und sich aus dem Datenschutzgesetz und AMWHV § 20 ergibt.

Achtung! Daten, die länger als gesetzlich gefordert aufbewahrt wurden, dürfen im Falle einer Prozessanbahnung nicht gelöscht werden (Pflicht zur Datensicherung für Prozesszwecke, litigation hold).

Um sowohl die geforderte Aufbewahrung als auch die geforderte Löschung von Daten unter Kontrolle zu haben, bedarf es einer strukturierten Vorgehensweise und einer klaren Zuordnung der Ablaufzeiten zu den Daten.

Im Folgenden ein Auszug der gesetzlich geforderten Aufbewahrungsdauern:

2.2.2.1 GMP

AMWHV § 20 Aufbewahrung der Dokumentation

Alle Aufzeichnungen… sind vollständig und mindestens bis ein Jahr nach Ablauf des Verfalldatums, jedoch nicht weniger als fünf Jahre aufzubewahren…

(2) Abweichend von Absatz 1 sind bei Blutzubereitungen… in lesbarer Form in einem geeigneten Speichermedium mindestens 30 Jahre und die anderen Aufzeichnungen über die Spendenentnahme und die damit verbundenen Maßnahmen gemäß § 11 Abs. 1 des Transfusionsgesetzes mindestens 15 Jahre aufzubewahren oder zu speichern. Die Angaben müssen gelöscht werden, wenn die Aufbewahrung oder Speicherung nicht mehr erforderlich ist.

Good Manufacturing Practice Medicinal Products for Human and Veterinary Use Chapter 4: Documentation

Specific requirements apply to batch documentation which must be kept for one year after expiry of the batch to which it relates or at least five years after certification of the batch by the Qualified Person, whichever is the longer. For investigational medicinal products, the batch documentation must be kept for at least five years after the completion or formal discontinuation of the last clinical trial in which the batch was used.

Critical documentation, including raw data (for example relating to validation or stability), which supports information in the Marketing Authorisation should be retained whilst the authorization remains in force.

2.2.2.2 GLP

Im GLP-Umfeld ergeben sich Anforderungen aus dem Chemikaliengesetz, hier ein Auszug:

10 Archivierung und Aufbewahrung von Aufzeichnungen und Materialien

…

10.2 Folgendes ist 15 Jahre in den Archiven aufzubewahren:

(a) Prüfplan, Rohdaten, Rückstellmuster von Prüf- und Referenzgegenständen, Proben und Abschlussbericht jeder Prüfung;

(b) Aufzeichnungen über alle nach dem Qualitätssicherungsprogramm vorgenommenen Inspektionen sowie das Verzeichnis mit Status aller Prüfungen (Master Schedule);

(c) Aufzeichnungen über die Aus-, Fort- und Weiterbildung sowie praktische Erfahrung des Personals, ferner die Aufgabenbeschreibungen;

(d) Aufzeichnungen und Berichte über die Wartung und Kalibrierung der Geräte;

(e) Validierungsunterlagen für computergestützte Systeme;

(f) chronologische Ablage aller Standardarbeitsanweisungen;

(g) Aufzeichnungen zur Kontrolle der Umweltbedingungen.

Falls für bestimmte prüfungsrelevante Materialien kein Archivierungszeitraum in Satz 1 festgelegt wurde, ist deren Entsorgung zu dokumentieren. Falls Rückstellmuster von Prüf- und Referenzgegenständen vor Ablauf des festgelegten Archivierungszeitraums entsorgt werden, ist dies zu begründen und zu dokumentieren. Rückstellmuster von Prüf- und Referenzgegenständen sowie Proben müssen nur so lange aufbewahrt werden, wie deren Qualität eine Beurteilung zulässt.

2.2.2.3 GCP

Im GCP-Umfeld sind die in Tab. 1 und 2 aufgeführten gesetzlichen Bestimmungen in Deutschland zu berücksichtigen.

2.2.2.4 Röntgenverordnung (RöV)

Die RöV ist gültig für klinische Prüfungen, in denen zum Zweck der medizinischen Forschung Röntgenstrahlung am Menschen angewendet wird (Tab. 3).

2.2.2.5 Strahlenschutzverordnung

Die Strahlenschutzverordnung ist gültig für klinische Prüfungen, in denen zum Zweck der medizinischen Forschung radioaktive Stoffe und ionisierende Strahlung am Menschen angewendet wird (Tab. 4).

2.2.2.6 Medizinproduktegesetz

Das Medizinproduktegesetz (§ 12, § 20 und § 24) ist gültig für klinische Prüfungen von Medizinprodukten (Tab. 5).

■ **Tabelle 1**

GCP-Verordnung nach § 42 AMG (gültig für alle klinischen Prüfungen von Arzneimitteln, andere Vorschriften zur Aufbewahrung von medizinischen Unterlagen bleiben unberührt).

Zu archivierende Unterlagen	Mindest-Archivierungsdauer	Verantwortlicher
Alle wesentlichen Unterlagen der klinischen Prüfung einschließlich der Prüfbögen	10 Jahre nach Beendigung oder dem Abbruch der Prüfung	Sponsor, Prüfer (auf Veranlassung des Sponsors)

Tabelle 2

Arzneimittelprüfrichtlinie nach § 26 AMG (gültig für klinische Prüfungen von Arzneimitteln, deren Ergebnisse in einem Zulassungsantrag verwendet werden).

Zu archivierende Unterlagen	Mindest-Archivierungsdauer	Verantwortlicher
Medizinische Akte	Gemäß den geltenden Rechtsvorschriften und in Übereinstimmung mit der in der Klinik, in der Einrichtung oder der privat üblichen Höchstaufbewahrungsdauer	Klinik bzw. Einrichtung bzw. private Praxis
Die wesentlichen Unterlagen für die klinische Prüfung einschließlich der Prüfbögen	– 15 Jahre nach Abschluss oder Abbrechen der Prüfung – *oder* mindestens zwei Jahre nach Erteilung der letzten Zulassung in der Europäischen Gemeinschaft, bis keine Zulassungsanträge in der EG mehr anhängig sind oder in Aussicht stehen, – *oder* mindestens zwei Jahre nach dem formellen Abbruch der klinischen Entwicklung des Prüfpräparats.	Die Zulassungsinhaber müssen Sorge tragen für die Aufbewahrung durch die Eigentümer der Daten
Prüfplan, SOPs, alle schriftlichen Stellungnahmen zum Prüfplan und zu den Verfahren, die Prüferinformation, die Prüfbögen, der Abschlussbericht, ggf. Auditbescheinigungen	Solange wie das Arzneimittel zugelassen ist	Sponsor bzw. andere Personen, in deren Besitz sich die Daten befinden
Abschlussbericht	Weitere 5 Jahre, nachdem das Arzneimittel nicht mehr zugelassen ist	
Bei innerhalb der EG 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.		

Tabelle 3

Archivierung gemäß Röntgenverordnung.

Zu archivierende Unterlagen	Mindest-Archivierungsdauer	Verantwortlicher
Siehe RöV § 28 c bzw. Anlage 4	30 Jahre	Inhaber der Genehmigung nach RöV § 28 a

Tabelle 4

Archivierung gemäß Strahlenschutzverordnung.

Zu archivierende Unterlagen	Mindest-Archivierungsdauer	Verantwortlicher
Siehe StrlSchV § 87 bzw. Anlage 4	30 Jahre	Inhaber der Genehmigung nach StrlSchV § 23 a

Tabelle 5

Archivierung gemäß Medizinproduktegesetz.

Medizinprodukt	Zu archivierende Unterlagen	Mindest-Archivierungsdauer nach Beendigung der Prüfung	Verantwortlicher
Aktive implantierbare Medizinprodukte	Siehe Richtlinie 90/385/EWG [4]	10 Jahre	Auftraggeber der klinischen Prüfung
Sonstige Medzinprodukte	Siehe Richtlinie 93/42/EWG [5]	5 Jahre	Auftraggeber der klinischen Prüfung
In-vitro-Diagnostika	Siehe Richtlinie 98/79/EG [6]	5 Jahre	Auftraggeber der Leistungsbewertungsprüfung

Pharm. Ind. 73, Nr. 7, 1207–1215 (2011)

2.2.2.7 Internationale Guidelines

Die ICH-GCP Guideline gibt eine Mindest-Archivierungsdauer für klinische Prüfungen mit Arzneimitteln an bzw. verweist auf die jeweiligen nationalen Vorschriften der Länder, in denen die Zulassung besteht oder beabsichtigt ist.

2.2.3 Zeitnahe und eindeutige Auffindbarkeit

Die zeitnahe und eindeutige Auffindbarkeit in komplexen Datenbeständen ist vom Gesetzgeber gefordert, siehe dazu z. B. AMWHV § 10 Allgemeine Dokumentation:

Werden die Aufzeichnungen mit elektronischen, fotographischen oder anderen Datenverarbeitungssystemen gemacht, ist das System ausreichend zu validieren. Es muss mindestens sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und innerhalb einer angemessenen Frist lesbar gemacht werden können …

In anderen Regularien ist von „… *readily available*" die Rede. Was darunter zu verstehen ist, sollte in den Archivierungsvorgaben klar festgelegt werden, ggf. unter Zuhilfenahme einer Risikobewertung. Ob es bei der Auffindbarkeit um die Erfüllung der Anforderungen in Inspektionen geht oder die Daten für einen evtl. Produktrückruf erforderlich sind, kann zu unterschiedlichen Interpretationen von *zeitnah* führen. Die Forderung nach Lesbarmachung bedeutet, dass für Menschen lesbare Kopien zur Verfügung gestellt werden müssen.

Im Chemikaliengesetz (GLP) ist folgende Formulierung zu finden:

10 Archivierung und Aufbewahrung von Aufzeichnungen und Materialien

…

10.3 Archiviertes Material ist zu indexieren, um ein ordnungsgemäßes Aufbewahren und Wiederauffinden zu erleichtern.

2.2.4 Berechtigungen auf Archivdaten

Zu der Regelung der Berechtigungen auf Archivdaten sind die gesetzlichen Vorgaben zu berücksichtigen.

2.2.4.1 GMP

Im GMP-Umfeld siehe dazu u. a. AMWHV § 20 (1) …

Die Zugriffsberechtigung zu den Aufzeichnungen nach Satz 1 ist durch geeignete Maßnahmen auf dazu befugte Personen einzuschränken …

Da die Systemnutzer keinen Zugriff auf das Archiv haben, können die Anforderungen im Archiv von den ursprünglichen Anforderungen im Originalsystem abweichen. Die Archivzugriffe sind in einem Berechtigungskonzept zu regeln. Der Archivar vergibt die Leseberechtigung.

2.2.4.2 GLP

Im GLP-Umfeld ergeben sich weitere Anforderungen aus dem Chemikaliengesetz, hier ein Auszug:

10 Archivierung und Aufbewahrung von Aufzeichnungen und Materialien

10.1 Zu den Archiven dürfen nur von der Leitung dazu befugte Personen Zutritt haben. Über Entnahme und Rückgabe sind Aufzeichnungen zu führen.

…

10.4 Wenn eine Prüfeinrichtung oder ein Vertragsarchiv die Tätigkeit einstellt und keinen Rechtsnachfolger hat, ist das Archiv an die Archive der Auftraggeber der Prüfungen zu überführen.

Dabei ist zu definieren, wie die Forderung 10.1 in einem elektronischen Archiv umzusetzen ist. Hierbei ist zu berücksichtigen, dass

- die Einschränkung des Zugriffs für Papierarchive einen anderen Sinn und Zweck hat als für ein elektronisches Archiv,
- eine Entnahme der Daten im eigentlichen Sinn nicht sinnvoll ist und daher auch für ein elektronisches Archiv nicht umgesetzt werden sollte. Stattdessen werden die elektronisch archivierten Daten bei jeder Abfrage in eine menschenlesbare Form neu als Kopie zusammengestellt und zur Verfügung gestellt.

Daraus ergibt sich, dass

- die Forderung nach Zugriffsberechtigung entsprechend angepasst werden muss,
- die Forderung bezüglich 10.1 Entnahme und Rückgabe entfällt,
- aber eine neue Anforderung hinzukommt, nämlich dass die beim Abruf erzeugte Zusammenstellung der archivierten Daten in menschenlesbarer Form genau das Dokumentenobjekt erzeugen muss, das es zu archivieren gilt.

Um eine Zusammenstellung der Daten erzeugen zu können, benötigt das elektronische Archiv daher nicht nur die Daten, sondern auch Informationen über ihre korrekte Zusammenstellung (zusammen auch mit ihren Metadaten) zu Objekten.

3. Entwurf und Test, Festlegen der Archivierungsstrategie / Erstellen des Archivierungskonzepts

Erst wenn die Fragen aus dem Abschnitt *Festlegen der Systemanforderungen* geklärt sind, kann eine Archivierungsstrategie festgelegt werden.

Am Anfang steht die Auswahl eines der drei im GAMP GPG Electronic Data Archiving benannten Archivierungsstrategien:

1. Nicht-elektronische Archivierung
2. Online-Archivierung (Daten im System halten)
3. Elektronische Archivierung

■ 3.1 Option 1, Nicht-elektronische Archivierung

Mit dieser Option, der nicht-elektronischen Archivierung, wollen wir uns in diesem Artikel nicht beschäftigen.

■ 3.2 Option 2, Online-Archivierung

Option 2, die Online-Archivierung, stellt eine häufig genutzte Alternative dar. Die Machbarkeit und Zukunftstauglichkeit dieser Variante ist von der Größenordnung des Datenanfalls abhängig. Es ist zu klären, wie lange das vorhandene System den Datenanfall bewältigen kann bzw. in welchen Abständen Hardwareerweiterungen nötig sind. Hier wird häufig mit billiger werdendem Speicherplatz spekuliert, wobei die Folgen wie steigendem Bedarf an Backup-Kapazitäten oftmals nicht mit einkalkuliert werden. Auch erfor-

derliche Bandbreiten fürs Backup bzw. bei zu geringen Bandbreiten Anstieg der Zeiten fürs Backup sind zu bedenken. Ferner ist zu klären, ob die Software darauf ausgelegt ist, die wachsenden Datenmengen zu bewältigen.

Der Umgang mit Daten, deren Archivierungsfrist abgelaufen ist, ist zu regeln (siehe 5.1). Werden die Daten gelöscht oder wird nur der lesende Zugriff eingeschränkt.

Spätestens zum Zeitpunkt der Stilllegung des Systems sind Strategien zu entwickeln, wie weiter mit den Daten zu verfahren ist. Wird das System trotz operativer Außerbetriebnahme als Datenarchiv weiter betrieben oder muss man sich nun, mit zeitlicher Verzögerung, mit der elektronischen Archivierung beschäftigen.

3.2.1 Option 3, Elektronische Archivierung

Bei der elektronischen Archivierung sind alle zu archivierenden Datenformate zu erfassen und zu analysieren. Sind die zu archivierenden Daten in proprietären Formaten gespeichert, so ist eine Strategie zur künftigen Lesbarkeit dieser Daten zu entwickeln. Wird zum Lesen der Daten spezifische Software benötigt, was speziell bei Laborsystemen nicht ungewöhnlich ist, so ist diese entsprechende vorzuhalten. Bei der Aufbewahrung von IT-Systemen zur Erhaltung der Lesbarkeit von proprietären Formate, sind weitere Punkte zu beachten (siehe 5.1). Es ist sinnvoll, die Entwicklung von Industriestandards zu verfolgen und dies bereits bei der Systemauswahl zu berücksichtigen, um spätere Überraschungen zu vermeiden. Eine Alternative kann die Archivierung in einem von den Originaldaten abweichenden Datenformat darstellen, was auf eine Datenmigration hinausläuft.

Die Struktur des Archivsystems ist festzulegen: Wird die gleiche Struktur wie im Originalsystem verwendet oder die Hard- und/oder Software emuliert. Im letzteren Fall wäre die elektronische Archivierung vergleichbar mit der Online-Archivierung, jedoch auf einer Systemkopie.

Aus den GMP-Regularien lässt sich keine Forderung nach Reprozessierbarkeit von analytischen Rohdaten ableiten, siehe dazu Teil 2 unserer Artikelserie. Im GLP-Umfeld existieren abweichende Anforderungen. Wenn die Reproduzierbarkeit gefordert oder angestrebt wird, sind entsprechende Maßnahmen zu treffen. Speziell bei der Archivierung in anderen Datenformaten als den Originaldatenformaten kann dies einen erheblichen Aufwand darstellen.

Soll bei der Archivierung das Datenformat geändert werden, wird also eine Datenmigration durchgeführt, muss folgendes beachtet werden:

- Inhalt und Bedeutung (Information) der Daten müssen erhalten bleiben.
- Ursprungs- und Ziel-Datentypen müssen eindeutig festgelegt werden
- Ob die Darstellung der Inhalte erhalten bleiben muss ist festzulegen. Was sich ändern darf und was konstant bleiben muss, ist zu spezifizieren.
- Die Aussagekraft elektronischer Signaturen muss erhalten bleiben.
- Metadaten müssen bewertet werden und der Umgang mit den Metadaten muss festgelegt werden (archivieren ja/nein und wie).

Eine Migration in die Formate pdf oder xml ist nicht immer die geeignete Lösung. Auch eine Migration zu nicht-elektronischen Medien ist nur in wenigen Fällen ein sinnvoller Ausweg.

3.2.2 Audit Trail

Zumindest ein Teil der Audit Trail-Informationen wird in der Regel als archivierungsrelevant eingestuft. Dabei treten unterschiedliche Probleme auf, die zu regeln sind. Hierzu einige Beispiele:

- Wie geht man mit dem Audit Trail bei Teilarchivierung um? Erzeugt die Verschiebung ins Archiv einen neuen Audit Trail-Eintrag? Falls ja, ist dieser auch zu archivieren? Hier empfiehlt sich eine logische Argumentation für die gewählte Vorgehensweise. Beispielsweise könnte man den Teil des Audit Trail, der sich auf die direkte Änderung an Daten bezieht, mit archivieren und die Audit Trail-Information, die den Transfer ins Archiv beschreibt, als Systeminformation des Online-Systems deklarieren, die nicht ins Archiv wandern muss. Die Information dient der Übersicht welche Daten im Archiv zu finden sind. Ob ein solcher Weg gewählt wird, ist abhängig davon, wie die Datensätze verknüpft sind und ob eine Trennung technisch realisierbar ist.
- Gibt es im Archivsystem einen Audit Trail auf den archivierten Daten? Wie ist dieser zu behandeln. Wie sind diese Audit Trail-Informationen beim Sichtbarmachen der Daten (Retrieval) zu behandeln.

Bei allen Fragestellungen sollte ein risikobasierter Ansatz zur Auswahl der zu archivierenden Audit Trail-Daten und allgemein zum Umgang mit Audit Trail-Informationen gewählt werden. Generell ist zu beachten, dass für Audit Trails die gleiche Aufbewahrungsdauer wie für die Daten (electronic records) gilt.

3.2.3 Signatur

Wo elektronisch signierte Daten archiviert werden müssen, sind entsprechende Vorkehrungen zu treffen.

Sinnvoll erscheint eine Unterscheidung nach dem Typ der Signatur

- Signatur eines Dokumentes,
- an Datensätze gebunden Signatur.

Der Archivierung signierter Dokumenten gestaltet sich in der der Regel einfacher als datensatzbezogene Signaturen. Bei der Archivierung ist sicherzustellen, dass die Verknüpfung von Daten zu Signatur inkl. aller Signatureigenschaften erhalten bleibt. Zu bedenken ist auch, dass die Gültigkeit von Signaturen über den Archivierungszeitraum ablaufen kann bzw. deren eigentliche Beweiskraft abnimmt. Dies ist ein entscheidender Unterschied zur manuellen Unterschrift auf Papier. Ein Grund hierfür kann die Schlüssellänge sein, die nicht mehr dem Stand der Technik entspricht. Orientierungspunkt kann

Pharm. Ind. 73, Nr. 7, 1207–1215 (2011)

hier der von der deutschen Bundesnetzagentur veröffentlichte „Algorithmenkatalog“ sein, der geeignete und nach Stand der Technik ausreichend sichere Algorithmen und Schlüssellängen auflistet [7].

Für diese Problematik gibt es verschiedene Strategien. In einigen Fällen kann risikobasiert entschieden werden, dass die Schlüssellänge dennoch eine ausreichende Sicherheit gewährleistet, da im Archiv ein sehr strikter Zugriffschutz besteht und eine Manipulation darüber verhindert werden kann.

Eine andere Strategie besteht in der Nachsignatur. Hierbei müssen nicht die ursprünglichen Unterzeichner signieren, was in der Realität auch meist nicht möglich ist. Das Nachsignieren dient zum einen der Bestätigung, dass vor Ablauf der Signatur die Daten vorlagen und zum anderen dem Anpassen des Sicherheitsstandards.

Dabei bestätigt die *ursprüngliche Unterschrift*, dass die richtige Person die Verantwortung übernommen hat, und erst nachrangig, dass die Daten nicht verfälscht wurden.

Die *Nachsignatur* bestätigt, dass die Daten nicht verfälscht wurden, mitunter dass seinerzeit die richtige Person die Verantwortung übernommen hatte. Ein Nachsignieren kann daher durchaus sinnvoll sein. Es hat nicht den Zweck, erneut Verantwortung für die Dateninhalte zu übernehmen, sondern nur für deren Erhaltung. Die Strategie sollte in einer SOP dargelegt werden. Auch bei der Migration in andere Strukturen kann es erforderlich sein, den Inhalt anschließend in Form einer Neusignatur zu bestätigen.

3.2.4 Suchfunktionen

Im Archiv sollten Suchfunktionalitäten implementiert sein. Diese sind u. a. wegen der Anforderung an die zeitnahe und eindeutige Auffindbarkeit in komplexen Datenbeständen wichtig (s. Abschnitt 2.2.3). Intelligente Suchkriterien sind ggf. Metadaten. Ob diese Metadaten im Archiv enthalten sind, hängt von den Festlegungen in Abschnitt 2.1 ab. Die Entscheidungen sollten risikobasiert und nach der erzielbaren Performance getroffen werden.

3.2.5 Sicherheit

Abhängig von den Überlegungen in Abschnitt 2. 2. 1 sind die nachfolgenden Themen zu behandeln.

3.2.5.1 Sicherheit vor Manipulation

In komplexen Datenbanken ist ein Teil des Manipulationsschutzes durch gestaffelte Zugriffsberechtigungen auf Daten geregelt. Die Berechtigungen auf Daten sind meist Metadaten. Ob und wie diese Metadaten archiviert werden, muss festgelegt werden. Risikobasiert kann hier auch entschieden werden, dass diese Berechtigungen nicht ins Archiv übernommen werden müssen, da der Zugriffschutz auf das Archiv selbst sehr restriktiv gehandhabt wird (s. Abschnitt 2.2.4). Ist ein Zugriff von außen auf das Archiv durch eine größere Nutzergruppe vorgesehen, ist hierfür ein Berechtigungskonzept erforderlich. Auch die Rechte des Archivars müssen klar geregelt werden. Wie beim Zurückspielen archivierter Daten der Manipulationsschutz gewährleistet wird, muss ebenfalls spezifiziert werden.
Erweiterte Manipulationssicherheit kann durch kryptographische Verfahren erreicht werden. Zusätzlich oder alternativ können Veränderungen durch Hashcodes über Archivdaten erkennbar gemacht werden.
Zu regeln ist auch das Change Management für das Archiv. Hierbei ist festzulegen, wie der Dateneigentümer eingebunden wird.

3.2.5.2 Sicherheit vor Datenverlust

Die Sicherheit vor Datenverlust hängt stark von der Auswahl der geeigneten Medien und dem Umgang mit den Medien ab. In Tab. 6 sind die Eigenschaften verschiedener Medien genannt.

Auf Basis der Aufbewahrungsdauer und der Anforderungen sollten die Medien ausgewählt werden. Zur erleichterten Einordnung sind auch Daten von nicht-IT-gestützten Archivierungsmedien mit aufgeführt.

■ 3.3 Auswahl, Qualifizierung und Validierung

Nach der Erstellung/Genehmigung des Archivierungskonzepts kann mit der Systemauswahl und der Auswahl der Systemkomponenten inklusive des Speichersystems begonnen werden. Das Archivsystem setzt sich dabei typischerweise aus den Anwendungen, die die zu archivierenden Daten generieren, dem Archivverwaltungssystem und dem Archivspeicher zusammen (Abb. 1). Um ein zukunftsfähiges Archivsystem zu implementieren, ist es sinnvoll, bei den Schnittstellen zwischen den Einzelkomponenten auf etablierte und gut dokumentierte Schnittstellen zu achten, damit im weiteren Lebenszyklus des Archivsystems auch Komponenten leicht an den Stand der Technik angepasst werden können.

Es ist empfehlenswert, die eingesetzte Hardware, insbesondere den Archivspeicher zu qualifizieren. Der Umfang der Qualifizierung wird risikobasiert festgelegt. Wie bei IT-Projekten üblich, sollte auch hier eine Test-, Validierungs- und Produktivumgebung etabliert werden. Neben der technischen Qualifizierung wird eine Validierung des Archivierungskonzepts durchgeführt. Alle zum Betrieb des Archivsystems notwendigen Regelungen und Arbeitsanweisungen müssen vorliegen. Dazu gehören die Themen

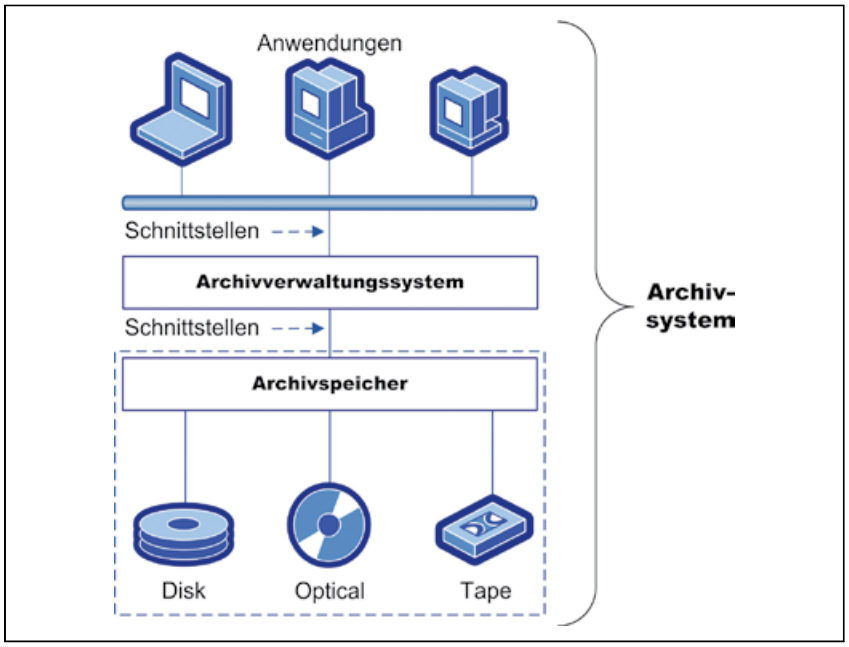
- Regelungen zum Service/Dienstleistungen,
- Monitoring,
- Vorfall-Management,
- Korrektur- und Vorbeugemaßnahmen,
- Change- und Konfigurations-Management,
- Reparaturmaßnahmen,
- Periodische Prüfung,
- Datensicherung und Wiedereinspielung,
- Geschäftsprozess-Kontinuitäts-Management,
- Sicherheits-Management,
- System-Administration

■ **Tabelle 6**

Eigenschaften verschiedener Archivierungsmedien (nach [8]).

Medium	Preis (Euro) pro GByte	Preis (Euro) pro Medium	Kapazität (GByte) pro Medium	Transferrate (MByte/s) (schreiben)	Lebens-zyklus	Erwartete Lebensdauer (Jahre)
Externe 3,5-Zoll-Festplatte	0,12 – 0,40	50 – 400	160 – 3000	20 – 100	ausgereift, Weiterentwicklung läuft	3 – 5
DVD-R	0,04 – 0,20	0,20 – 2	4,7 oder 8,5	10	ausgereift, eher auslaufend	1 – 30
Blu-Ray (BD) (ROM-Typ)	0,03 – 1	5 – 50	50	4 – 40	aufkommend, Weiterentwicklung läuft	1 – 50
MOD (WORM-Typ)	0,76	70	0,65 – 9,1	0,8	ausgereift, keine Weiterentwicklung	50
UDO (ROM-Typ)	0,57	40 – 70	30 – 60	0,8	ausgereift, Weiterentwicklung?	50
Holo-Disc (WORM)	N/A	N/A	500 – 1600	N/A	Entwicklung läuft	50
WORM-Tape (LTO-4)	0,04 – 0,09	30 – 70 €	800	15	ausgereift, Weiterentwicklung läuft	30
WORM-Tape (LTO-5)	0,04 – 0,05	70 – 80 €	1500 GB	18	ausgereift, Weiterentwicklung läuft	30
Solid State Drive (SSD)	12 – 14	100 – 900	8 – 64	4 – 40	ausgereift, Weiterentwicklung läuft	10
Zum Vergleich:						
Steintafel	1 – 10 Mio.	10 – 100	10^{-5}	10^{-8}	ausgereift	5000
Buch (säurefreies Papier)	100 – 1000	10 – 30	0,002	10^{-3}	ausgereift	200 – 500
Buch (säurehaltiges Papier)	100 – 1000	10 – 30	0,002	10^{-3}	ausgereift	50 – 100

■ **Abbildung 1**



Aufbau eines Archivierungssystems mit Schnittstellen (nach [9]).

4. Systemimplementierung

Nach der erfolgreichen Validierung erfolgt die eigentliche Implementierung der Archivierungsstrategie. Hier können die üblichen Vorgehensweisen genutzt werden.

5. Betrieb bis zur Stilllegung

■ 5.1 Umsetzung der Archivierungsstrategie(-konzepts)

Für den Betrieb eines Archivsystems ist nach den Vorgaben laut Abschnitt 3.3 vorzugehen. Im Zuge der periodischen Prüfungen des Archivsystems (ca. alle 2 Jahre) ist zu prüfen, ob es noch tauglich für den Einsatzzweck ist. Ansonsten muss eine Migrationsstrategie entwickelt werden. Bei der periodischen Prüfung sind besonders die folgenden Themen zu berücksichtigen:

Pharm. Ind. 73, Nr. 7, 1207–1215 (2011)

- *Verifizieren der Archivierungsaktivitäten*
  - Sicherung der archivierten Daten gegen Veränderung.
  - Aufzeichnung notwendiger Metadaten wie Archivierungsdatum, Archivbenutzer, Datenursprung (Quellsystem/-software/-anlage), Datenformat (Informationen zur Interpretation der gespeicherten Daten müssen verfügbar sein), Dateneigner der zu archivierenden Daten, Eindeutige Bezeichnung des Datensatzes, ggf. Audit Trail-Informationen zu den Originaldaten (Benutzer am Originalsystem), Daten zur Verschlagwortung der Daten (Benutzer am Originalsystem, Aufzeichnungsdatum im Originalsystem, Beschreibung der Daten, Zuordnung der Daten zu allgemeinen Parametern – z. B. produziertes Fertigmaterial/ Charge, Regulatorischer Bereich, dem die Daten unterliegen (z. B. GLP, GMP, …)).
- *Auffrischen oder Regenerieren (Datenaufnahme in das Archiv)*
- *Datenpflege (Update) / Datenmigration bei Systemwechsel*
  Auch das Archivierungssystem selbst unterliegt der Alterung. Im Rahmen der periodischen Prüfung sollte hinterfragt werden,
  - ob die Archivierungsstrategie korrekt umgesetzt ist,
  - ob die Archivierungsstrategie noch geeignet ist.

  Sowohl Hardware als auch Software des Archivierungssystems werden spätestens nach 10 Lebensjahren einer Erneuerung bedürften, damit das Archivsystem zukunftsfähig erhalten bleibt (nach [9]). Dabei sind die veralteten Bestandteile zu ersetzten und im Besondern auch die Daten auf neue Datenträger zu übertragen. Hierbei ist darauf zu achten, dass die Daten mitsamt den Metadaten auch im neuen System lesbar bleiben. Dies sollte sichergestellt und getestet werden, wie es auch im neuen EU-GMP Annex 11 gefordert wird. Der Migrationsprozess sollte als neuer Eintrag in den Metadaten erfasst werden, um auch nach der Migration den Lebenszyklus der archivierten Daten nachvollziehbar zu erhalten.
- *Datenmaintenance – Überwachung der laufenden Verfügbarkeit*
  Die Verfügbarkeit, Lesbarkeit und Datenintegrität sollte durch entsprechendes Monitoring überwacht werden, wie es auch im neuen EU-GMP Annex 11 gefordert wird.
- *Datensuche und -abruf (Search/ Retrieve)*
- *Aufzeichnen der Vernichtung entsprechend der Grundsätze über das Löschen archivierter Daten*
  Auch wenn es gute Gründe gibt, Daten „unendlich“ aufzubewahren, sollten Daten am Ende ihrer vorgesehenen Aufbewahrungszeit auch kontrolliert gelöscht werden. Der Zeitpunkt der Löschung von Dokumente im Archivierungssystem ergibt sich dann aus regulatorischen Anforderungen (wie GMP, GLP, Datenschutz, etc.) und aus technisch-organisatorischen Erwägungen (Minimierung des Aufwands).
  Vor der Vernichtung von Aufzeichnungen sollte überprüft werden, ob die Daten auch im Archivspeicher unlesbar gemacht wurden. Ein lediglich Löschen eines „Links“ zum Ablageort der Daten im Archivverwaltungssystem entspricht nicht den Anforderungen einer regelgerechten Vernichtung.
  Ebenso sollte bestimmt werden, ob (falls vorhanden) auch alle Audit Trial-Informationen zu den gelöschten Daten ebenso gelöscht werden sollen. Auch sollte berücksichtig werden, dass sich die Daten, die im Archivierungssystem gelöscht sind, oft noch auf mehreren Sicherungsmedien befinden können.
  Eine weitere Herausforderung stellen Daten dar, deren Aufbewahrungszeit zwar abgelaufen ist, die aber noch explizit aufzubewahren sind (z. B. „litigation hold“). Hier sollten entsprechende organisatorische Maßnahmen und Softwarefunktionen sicherstellen, dass diese Daten nicht einem automatischen Löschprozess am Ende ihrer Aufbewahrungszeit zum Opfer fallen.
- *Zugriffsberechtigungen*
  Zugriffsberechtigungen sollten ebenfalls im Rahmen der periodischen Prüfungen hinterfragt werden.

LITERATUR

[1] Batoulis J, Kwiatkowski E, Appel B, Schulz M. Prozesse und Rollen bei der elektronischen Archivierung. *Pharm Ind.* 2010;72 (1):51–54.
[2] Weiser D. Reprozessierbarkeit von GMP-Daten. Pharm. Ind. 2010; 72(2): 218–222.
[3] GAMP® Good Practice Guide: Electronic Data Archiving. Tampa: ISPE; 2007.
[4] Richtlinie 90/385/EWG über aktive implantierbare medizinische Geräte vom 20. 7. 1990, zuletzt geändert am 29. September 2003.
[5] Richtlinie 93/42/EWG des Rates über Medizinprodukte vom 14. Juni 1993, zuletzt geändert am 16. 11. 2000.
[6] Richtlinie 98/79/EG des europäischen Parlaments und des Rates vom 27. Oktober 1998 über *In-vitro*-Diagnostika vom 07. 12. 1998 (ABl. L 331 S. 1–37).
[7] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 01. Februar 2011 im Bundesanzeiger Nr. 17, S. 383. *http://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html*
[8] Rink J, Haustein N. Für die Ewigkeit – Digitale Dokumente archivieren. c't 2008;16:128–131.
[9] Haustein N. Hohle Gasse – Schnittstellen für Archivsysteme. ix 2010;02:113–115.

Korrespondenz:
Dr. Christoph Hornberger,
EMR Engineering GmbH,
Talstr. 142 a,
55218 Ingelheim (Germany),
e-mail: christoph.hornberger@emr-engineering.de