



QUASAR #175

INFORMING AND ADVANCING OUR MEMBERS

www.therqa.com

MAY 2026 | ISSN 1463-1768

19 PAGES OF ARTICLES

FROM ATTENDANCE
TO COMPETENCE

LONDON CALLING:
QUALITY NEVER DIES

OF PRIDE AND PREJUDICE: THE GREAT INJUSTICE DONE TO TRAINING QUALITY IN CLINICAL RESEARCH

ARCHIVING WITH INTEGRITY:
TURNING 'STORAGE' INTO
A COMPLIANCE ASSET

FROM SUPPORT TO
SYSTEM IMPACT

THE LATEST
COURSES P27





Erika Reategui

ARCHIVING WITH INTEGRITY: TURNING 'STORAGE' INTO A COMPLIANCE ASSET

Archival is often treated as the quiet end of a record's life: a final folder, a long-term box, an IT backup and 'job done'. However, in regulated environments, this mindset is risky. Archival is not just storage, it is an extension of your Quality Management System with a direct impact on data integrity (Availability in ALCOA+ terms) for both paper and electronic records.

Whether working with paper or electronic GxP records, validation packages, batch records, training evidence, complaint files or clinical and laboratory data, the archive is where regulators and customers expect you to retain records to demonstrate what happened, when it happened, who did it and why it was acceptable. A strong archive does not just reduce findings, it protects data, products, patients and your organisation's credibility.

REGULATORY REQUIREMENTS AND GUIDANCE

Archiving and data integrity expectations are not 'best practice' add-ons; they are embedded in GxP regulatory frameworks and repeatedly reinforced through inspectorate guidance. Across regions, regulators expect organisations to maintain records that remain complete, accurate, protected from unauthorised change and readily retrievable throughout their required retention period, in whatever format the records are retained.

Key requirements and expectations include:

- EU GMP (EudraLex Volume 4) – Documentation governance and retention. EU GMP Chapter 4 defines expectations for GMP documentation, including good documentation practices, control of records and retention principles
- EU GMP Annex 11 – Computerised systems used in GMP. Annex 11 sets expectations for validated applications/qualified infrastructure, risk management, appropriate access control and controls supporting data integrity (e.g. accessibility and audit trails where needed)
- US FDA – 21 CFR Part 211 (CGMP) (selected recordkeeping/retention requirements). These sections define the minimum expectations your archival programme has to support for creation, completeness, review and retention of GMP records:

- 21 CFR 211.180 – General requirements. Establishes overarching expectations for records and reports (including retention timeframes) and supports retaining required records as originals or true copies under controlled conditions
- 21 CFR 211.186 – Master production and control records. Requires approved, controlled master records (prepared/dated/signed and independently checked) to assure batch-to-batch uniformity
- 21 CFR 211.188 – Batch production and control records. Requires batch records for each batch with complete information related to production and control, including an accurate reproduction of the applicable master record
- 21 CFR 211.194 – Laboratory records. Requires lab records to contain complete test data necessary to show conformance to specifications/standards, supporting traceability of what was tested and reported
- US FDA – 21 CFR Part 58 (GLP) (archiving and retention requirements). Where GLP applies, Part 58 includes explicit expectations for controlled archive facilities, storage/retrieval and retention of study records and data:
 - 21 CFR 58.51 – Specimen and data storage facilities. Requires space for archives with restricted access for storage and retrieval of raw data and specimens from completed studies
 - 21 CFR 58.190 – Storage and retrieval of records and data. Establishes expectations for orderly storage and expedient retrieval, and storage conditions that minimise deterioration; allows use of qualified commercial archives
 - 21 CFR 58.195 – Retention of records. Defines record retention periods and explicitly allows retention as originals or true copies (e.g., photocopy/microfilm/other accurate reproductions), supporting both paper and electronic strategies where applicable
- US FDA – 21 CFR Part 11. For electronic records/e-signatures, Part 11 requires, among other things, secure, computer-generated, time-stamped audit trails for actions creating/modifying/deleting electronic records, with audit trail retention at least as long as the underlying records and availability for review/copying
- FDA guidance on Part 11 scope and enforcement discretion. FDA's Part 11 guidance clarifies the Agency's approach and highlights focus areas, such as validation, audit trails, record retention, and record copying
- MHRA (UK) GxP Data Integrity Guidance. MHRA's guidance defines data integrity expectations for paper and electronic records and explicitly links them to ALCOA+/ALCOA+ concepts
- PIC/S PI 041-1 – Data management and integrity in GMP/GDP. PIC/S provides detailed expectations on governance, risk-based controls and practical measures to ensure data integrity in regulated environments, commonly used by inspectorates and industry globally
- WHO guidance on data integrity. The updated WHO guidance (replacing the earlier TRS 996 Annex 5) outlines controls and recommendations to strengthen data integrity, supporting product quality, safety and efficacy
- ICH Q7 – Records and documentation for APIs. ICH Q7 includes requirements and expectations for documentation/records within API GMP, including review/approval and retention concepts that feed directly into archival practices
- OECD GLP – Archiving expectations (where GLP applies). OECD GLP principles specify archive controls, such as indexing for orderly storage/retrieval, restricted access and recording movement of archived materials.

WHY ARCHIVING IS A DATA INTEGRITY ISSUE

Data integrity is commonly summarised by principles such as ALCOA+: records must be Attributable, Legible, Contemporaneous, Original, Accurate and complete, consistent, enduring and available. Archiving touches at least three of these directly:

- Enduring: can the record remain reliable and readable for the full retention period?
- Available: can you retrieve it quickly, completely and in a usable form with the same context as the original?
- Complete and consistent: can you demonstrate version history, approvals and associated metadata without gaps?

A record that cannot be retrieved, cannot be read or cannot be proven authentic may as well not exist. Regulators will view poor archiving as a systemic weakness, not a clerical oversight.

DEFINE WHAT 'ARCHIVE' MEANS IN YOUR ORGANISATION

A surprising number of organisations lack a precise definition of their archive. Is it:

- A controlled repository with defined access, indexing and retrieval?
- A long-term storage location for original records?
- A disaster recovery backup?
- A legacy system you 'still have somewhere'?

These are not interchangeable. Backups are not archives. Backups are designed for system restoration; archives are designed for record preservation, controlled access and regulated storage and, if necessary, retrieval. The first step in improving archiving is agreeing on its purpose, ownership and scope.

BUILD ARCHIVING INTO THE RECORD LIFECYCLE

Archiving should be designed from the start of the record lifecycle, not bolted on at the end. A practical lifecycle view may look like this: see Figure 1.

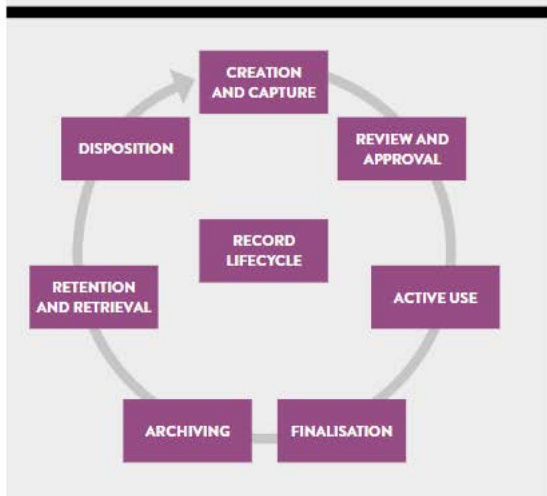
1. Creation and capture: are templates controlled? Are records uniquely identifiable?
2. Review and approval: are workflows secure, traceable and role-based?
3. Active use: are record changes controlled? Are audit trails enabled and reviewed?
4. Finalisation: Is the 'final' state clearly defined (e.g. released, approved, locked)?
5. Archiving: are records transferred with integrity, context, index metadata and controls intact? Is access to archives restricted?
6. Retention and retrieval: are retention rules enforced and is retrieval periodically tested, including during any system migrations or upgrades?
7. Disposition: are records destroyed securely and only when permitted?

If you cannot confidently describe these steps, you are likely carrying compliance risk.

PAPER VS ELECTRONIC: DIFFERENT RISKS, SAME EXPECTATIONS

Paper records face classic threats: fading ink, water or fire damage, incomplete packets, unclear signatures, missing attachments and poor indexing. A 'paper archive' must include control of the basics: environmental conditions, fire protection, access logs, pest control, version control and secure access.

FIGURE 1. PRACTICAL RECORD LIFECYCLE VIEW



Electronic records have different failure modes: incomplete records (missing metadata or audit trail), obsolete file types, system migrations, broken links, missing metadata, inadequate audit trails, weak access controls and uncontrolled copies. Yet regulators expect the same fundamentals: authenticity, integrity, confidentiality (where applicable), traceability and availability.

A robust approach is to define 'record type families' (e.g. QA approvals, validation, manufacturing, training) and set specific archival rules for each – format, metadata requirements, retention – access rights and retrieval expectations.

THE THREE CONTROLS THAT MAKE OR BREAK AN ARCHIVE

If you only strengthen three areas, prioritise these:

1. AUTHENTICITY AND AUDIT TRAILS

For electronic records, audit trails are not optional – they are your evidence of integrity. For paper records, authenticity comes from controlled originals, controlled stamps, wet signatures (where required) and a documented chain of custody.

Ask yourself:

- Can we prove what changed, who changed it and when?
- Can we show approvals were valid at the time?
- Can we demonstrate that the archived version is the approved version?

2. INDEXING AND METADATA

A record that exists but cannot be located is a liability. Good archives are searchable and consistently indexed.

Minimum metadata typically includes:

- Unique identifier (document number/record ID)
- Title and record type
- Product/project/site (as applicable)
- Effective date and/or approval date
- Version and status (draft/final/obsolete)
- Owner and approver(s)
- Retention category and retention end date
- Location (physical box reference or electronic path).

For electronic archives, metadata should ideally be system-managed – not a user-edited spreadsheet.

3. ACCESS CONTROL AND SEGREGATION OF DUTIES

Archives must prevent unauthorised changes. Access should be role-based and 'write' privileges tightly limited. Separation between creators, approvers and archive administrators reduces both accidental and intentional integrity risks.

Key practices include:

- Restricted admin access
- Immutable or locked final records (where required)
- Controlled retrieval with logging
- Clear rules for copies (watermarked or clearly marked 'uncontrolled copy').

ARCHIVING DURING MIGRATION: WHERE INTEGRITY IS LOST

System changes – SharePoint restructures, eQMS upgrades, LIMS replacements, network drive cleanups – are the most common moments where records go missing or lose traceability.

A migration should be treated like a regulated activity:

- Defining scope and record populations
- Map metadata fields (old → new)
- Verify record completeness post-transfer
- Preserve audit trails or document justified alternatives
- Lock down 'source' repositories to prevent divergence
- Run retrieval tests (not just file counts).

The best migrations are data integrity-minded, creating documented evidence that the records within the archive remained trustworthy throughout the migration process.

GDPR AND CONFIDENTIALITY: ARCHIVING ISN'T 'ANYTHING GOES'

Archives often contain personal data, such as training records, CVs, deviation interviews, complaint details, supplier contacts or clinical information. GDPR and privacy requirements still apply in the archive. That means:

- Limit access to what's necessary
- Define lawful basis and retention justification
- Secure storage and transmission
- Apply controlled disposition when retention ends
- Ensure retrieval doesn't expose unnecessary personal data.

A strong archive balances two pressures: retain what you must for compliance and dispose of what you no longer have a lawful reason to keep.

COMMON PITFALLS (AND WHAT TO DO INSTEAD)

Pitfall: 'we have everything on a shared drive'

Instead: use a controlled repository with permissions, versioning and indexing.

Pitfall: 'archived means we moved it to a folder called 'Archive'

Instead: define archival status, locking rules and a documented transfer process.

Pitfall: 'we can retrieve it if we search long enough'

Instead: perform periodic retrieval drills with target times and success criteria.

Pitfall: 'backups cover us'

Instead: keep backups for disaster recovery and an archive for compliance retrieval

Pitfall: 'retention is handled by individuals'

Instead: implement retention categories and system-enforced retention where possible.

A PRACTICAL 'ARCHIVE HEALTH CHECK'

If you want a quick, high-value internal assessment, ask these ten questions:

1. Do we have an approved procedure defining archiving, retention, retrieval and disposition?
2. Are record types classified with defined retention periods and ownership?
3. Can we retrieve any record within an agreed timeframe (e.g. 24–72 hours) and demonstrate it is complete and accurate?
4. Is access controlled to prevent alteration of final records (electronic locking or controlled originals)?
5. Are access permissions reviewed periodically and documented?
6. Do we maintain a chain of custody for physical records?
7. Are audit trails enabled, protected and reviewed for electronic systems?
8. Are archives included in business continuity/disaster recovery planning?
9. Are migrations handled with documented verification of completeness and integrity?
10. Do we securely dispose of records at the end-of-retention (and can we prove it)?

If you cannot answer 'yes' to most of these, the archive is likely a hidden compliance risk and an easy place to gain maturity.

THE TAKEAWAY: TREAT THE ARCHIVE AS EVIDENCE, NOT STORAGE

Archiving is where your organisation proves its history. Done well, it becomes a strategic asset: faster investigations, smoother audits, stronger customer confidence and reduced operational friction. Done poorly, it quietly accumulates risk until the day you're asked to produce a record – and you cannot produce it with confidence.

'A record is only as good as your ability to retrieve it, trust it and explain it.'

Archiving with data integrity at the core makes that possible.

After all, in regulated environments, archiving is not the end of the record lifecycle; it is where your organisation proves its decisions, controls and outcomes, long after the work is done. Whether the record is paper, electronic or hybrid, the expectation is the same: it must remain authentic, complete, enduring and readily retrievable for the full retention period, with protections against loss, deterioration or unauthorised change. The strongest archival programmes treat archives as controlled evidence systems, not storage locations, built into the lifecycle, governed by clear procedures, supported by metadata and access controls, and verified through periodic retrieval and migration checks. When you approach archiving this way, you do not just prepare for inspections; you strengthen investigations, accelerate root-cause analysis, protect patients and products, and turn compliance into an operational advantage.

PROFILES

Erika is a seasoned molecular biologist with over 25 years in clinical research, over 15 years in QA and certification as a clinical research professional. She has operated under FDA, MHRA, Health Canada and EMA requirements. As VP, Operations and Compliance at QACV Consulting, Erika leads a global team in the areas of training, compliance, operations, QMS, audits, inspection readiness, vendor oversight, risk-based compliance planning and continuous improvement across the company and GLP, GCP, GMP and GVP.