



UNDERSTANDING ISO 17025 CLAUSE 7.5 – TECHNICAL RECORDS

The Foundation of Traceability – Why Technical Records Matter

Technical records are the backbone of laboratory credibility. Clause 7.5 requires laboratories to maintain records that allow any test or calibration to be **reconstructed, verified and defended**. These records are not administrative paperwork — they are the evidence that work was performed correctly, consistently and in compliance with ISO/IEC 17025.

Strong technical records include:

- **Raw data** from instruments, observations and measurements
- **Environmental conditions** that may influence results
- **Equipment identifiers**, calibration status and settings
- **Personnel involved**, including authorisation
- **Calculations**, transformations and statistical treatments
- **Deviations**, anomalies and corrective actions
- **Version-controlled amendments** that preserve original entries

Technical records must be clear, complete and chronological. They must tell the full story behind every result — what was done, how it was done, when it was done, who did it, with what it was done and under what conditions. When laboratories maintain disciplined records, they protect impartiality, strengthen traceability and ensure that results can withstand scrutiny from clients, regulators and accreditation bodies.

What Technical Records Must Contain – Building a Complete and Defensible Story

Clause 7.5 outlines the essential elements that must appear in technical records to ensure traceability and defensibility. These elements transform laboratory work from actions into **evidence**.

A complete technical record includes:

- **All original observations** — not just final results
- **Equipment identification** for equipment used
- **Instrument outputs**, screenshots, printouts or digital logs/records
- **Environmental conditions** such as temperature, humidity or vibration
- **Sample identifiers**, chain-of-custody links and preparation details
- **Method references**, including revisions and procedural notes
- **Calculations**, formulas, rounding rules and uncertainty considerations
- **Personnel identification**, names, surnames, signatures or electronic authentication
- **Dates** when work was performed
- **Any factor that may influence validity**, including anomalies

Records must be detailed enough that another competent person could follow the work step-by-step and reach the same conclusion. If a record cannot support reconstruction, it cannot support accreditation.



Clause 7.5 ensures that laboratories produce results that are not only accurate — but **defensible**.

Corrections, Amendments and Version Control – Protecting Data Integrity

Technical records must be accurate — but they must also be **transparent**. Clause 7.5 requires laboratories to correct errors without erasing original entries. This protects data integrity and prevents manipulation.

Key principles include:

- **No deletion of original data** — corrections must be traceable
- **Clear indication of changes**, including date, time and responsible person
- **Justification for amendments**, especially when results are affected
- **Version control** for electronic records, ensuring audit trails remain intact
- **Secure access controls** to prevent unauthorised editing
- **Tamper-evident systems** for both paper and digital formats

Corrections must never obscure what was originally recorded. Transparency builds trust, supports impartiality and ensures that records remain defensible during audits, disputes or regulatory reviews.

Clause 7.5 reinforces that integrity is not only about correct results — it is about **honest records**.

Electronic vs Paper Records – Managing Risks and Ensuring Control

Clause 7.5 applies equally to paper worksheets, spreadsheets, LIMS systems and hybrid formats. Regardless of the medium, records must remain **secure, accessible, complete and tamper-evident**.

Key controls for electronic records:

- **Audit trails** that track all edits, deletions and access
- **User authentication** and role-based permissions
- **Backups**, redundancy and disaster-recovery plans
- **Protection against overwriting**, corruption or unauthorised changes

Key controls for paper records:

- **Permanent ink**, controlled access and secure storage
- **Cross-referencing**, pagination and version control
- **Procedures for corrections** that preserve original entries
- **Protection from damage**, loss or environmental risks
- **Defined secure storage locations**

Hybrid systems must ensure consistency between digital and paper components. The medium may differ — but the requirements for integrity, traceability and security remain the same.

Clause 7.5 ensures that records remain trustworthy, regardless of format.



Retention, Security and Confidentiality – Safeguarding Records Over Time

Technical records must be protected long after testing is complete. Clause 7.5 requires laboratories to retain records for defined periods (retention period), store them securely and protect them from loss, damage or unauthorised access.

Key responsibilities include:

- **Retention schedules** aligned with regulatory, contractual and internal requirements
- **Secure storage**, whether physical or digital
- **Controlled access**, ensuring only authorised personnel can view or modify records
- **Protection from environmental risks**, including moisture, heat or physical damage
- **Confidentiality controls**, safeguarding client information
- **Disposal procedures** that ensure records are destroyed responsibly

Retention is not simply archiving — it is a continuation of traceability. Records must remain accessible, readable and complete for the entire retention period.

Clause 7.5 ensures that technical records remain reliable evidence throughout their lifecycle.

Turning Laboratory Work into Defensible Evidence

Clause 7.5 – Technical Records, one message stands out: **technical records are the evidence of competence**. They transform laboratory actions into defensible proof. Without clear, complete and traceable records, even accurate results lose credibility.

Technical Records – The Backbone of Traceability

Recognising that technical records are not paperwork — they are the laboratory's memory. They allow any test or calibration to be reconstructed, verified and defended. Raw data, observations, environmental conditions, equipment identifiers and calculations all combine to tell the full story behind every result.

What Records Must Contain – Building a Complete Picture

Clause 7.5 requires laboratories to capture every factor that may influence validity: instrument outputs, sample identifiers, method references, anomalies and corrective actions. A technical record must be detailed enough that another competent person could follow the work step-by-step and reach the same conclusion.

Corrections and Amendments – Protecting Data Integrity

Transparency is essential. Corrections must never erase original entries. Amendments must be dated, justified and traceable. Version control and audit trails protect laboratories from data manipulation and ensure that records remain trustworthy during audits or disputes.



Electronic vs Paper – Format Without Losing Control

Whether laboratories use LIMS, spreadsheets or paper worksheets, the requirements remain the same: security, accessibility, completeness and tamper-evidence. The medium may differ — but the integrity must not.

Retention and Security – Safeguarding Records Over Time

Technical records must be retained for defined periods, stored securely and protected from loss or unauthorised access. Responsible disposal ensures confidentiality and compliance.

Technical records are the laboratory's defence. They protect impartiality, support traceability and ensure that every result can withstand scrutiny.

Accurate results begin with accurate records.

