



UNDERSTANDING ISO 17025 CLAUSE 7.11 – CONTROL OF DATA AND INFORMATION MANAGEMENT

Why Data Control Matters – Protecting Accuracy, Integrity and Trust

Data is the backbone of every accredited laboratory. It is the evidence that proves what was done, how it was done, and under what conditions. Clause 7.11 ensures that all data — raw measurements, calibration records, environmental logs, instrument outputs, calculations, metadata, amendments, audit trails and final reports — is **accurate, complete, secure, traceable and available**. Without strong data control, even technically sound results lose credibility.

Data errors, loss, corruption or unauthorised changes can compromise validity, damage trust and threaten accreditation. Clause 7.11 exists because laboratories operate in environments where digital systems, manual records, instruments, spreadsheets and communication channels interact continuously. Every point where data is generated, transferred, stored or retrieved introduces risk. Managing these risks is not optional — it is essential.

This clause requires laboratories to implement controls that protect data throughout its entire lifecycle: creation, processing, storage, backup, retrieval, retention and disposal. It ensures that data remains readable, retrievable, useable, and protected from unintended alteration. It also ensures that access is controlled, changes are documented, and systems are validated.

The core principle: **data integrity is measurement integrity**. A laboratory may produce excellent results, but if data is mishandled, the value of those results collapses. Clause 7.11 ensures that laboratories protect their digital backbone with the same discipline applied to technical work.

Managing Electronic and Paper-Based Data – Systems That Must Work Together

Clause 7.11 requires laboratories to manage both electronic and paper-based data under controlled conditions. Modern laboratories rely heavily on digital systems — Laboratory Information Management Systems (LIMS) platforms, spreadsheets, instrument software, servers, cloud storage and databases — but many still use paper records for sample logs, worksheets, environmental checks and manual calculations. Both electronic and paper-based data must be controlled with equal discipline.

Electronic data must be protected through:

- Validated software and spreadsheets
- Controlled templates and locked formulas
- Access restrictions and password protection
- Audit trails that record changes
- Regular backups and secure storage
- Version control and change management
- Reliable hardware and stable networks



Paper-based data must be protected through:

- Controlled forms and templates
- Legible entries and permanent ink
- Clear corrections with name, surname, signature and date
- Secure storage in designated locations
- Controlled access to sensitive records
- Documented retention and disposal procedures

Clause 7.11 emphasises that data systems must work together seamlessly. A laboratory cannot rely on digital discipline while allowing paper records to be informal or inconsistent. Likewise, strong manual controls cannot compensate for weak digital systems. Data integrity requires consistency across all formats.

This clause ensures that laboratories maintain reliable, traceable and secure information regardless of how it is generated or stored. When electronic and paper-based systems operate under unified control, the laboratory's data environment becomes stable, defensible and audit-ready.

Ensuring Data Integrity – Accuracy, Completeness and Protection Against Alteration

Data integrity means that information remains accurate, complete and unaltered throughout its lifecycle. Clause 7.11 requires laboratories to implement controls that prevent accidental or intentional changes to data. Integrity is not only a technical requirement — it is a trust requirement.

Data integrity is protected through:

- Controlled access to systems and records
- Password-protected accounts with defined roles
- Locked fields and validated formulas in spreadsheets
- Controlled templates for manual entries
- Documented amendments with name, surname, signature and date
- Audit trails that show who changed what and when
- Procedures that prevent informal shortcuts
- Regular verification of calculations and outputs

Laboratories must ensure that data cannot be altered without authorisation.

Uncontrolled spreadsheets, editable reports, shared passwords, informal notes and undocumented corrections all threaten integrity. Clause 7.11 requires laboratories to eliminate these risks through disciplined processes and secure systems.

Integrity also includes completeness. Missing data, partial records, incomplete logs or undocumented changes weaken traceability. Clause 7.11 ensures that data tells the full story — from raw measurements to final reports.



When data integrity is protected, results become defensible, traceable and trustworthy. Clients, auditors and regulators rely on the laboratory's ability to safeguard information. Clause 7.11 ensures that this responsibility is met with discipline and professionalism.

Backup, Security and Continuity – Protecting Data Against Loss

Data loss is one of the most serious risks in an accredited laboratory. Clause 7.11 requires laboratories to protect data against loss due to equipment failure, system crashes, environmental events, cyber threats or human error. Strong backup and security measures ensure that data remains available, readable and recoverable.

Backup systems must be:

- Regular (daily or scheduled)
- Verified to ensure data is recoverable and useable
- Stored in secure, controlled locations
- Redundant (multiple copies)
- Protected from unauthorised access
- Documented in the quality system

Security measures must include:

- Password protection and access control
- Firewalls and antivirus protection
- Secure networks and encrypted storage
- Physical security for servers and records
- Controlled access to sensitive information
- Monitoring for suspicious activity

Continuity planning ensures that the laboratory can recover quickly from disruptions. Clause 7.11 requires laboratories to have documented procedures for restoring data, resuming operations and protecting information during emergencies. Continuity is not optional — it is essential for reliability and accreditation.

When data is backed up, secured and protected, the laboratory demonstrates resilience and professionalism. Clause 7.11 ensures that data remains safe, accessible and intact, even under unexpected conditions.

Technician and Management Responsibilities – Discipline, Accuracy and Authoritative Oversight

Technicians and management play critical roles in protecting data integrity. Clause 7.11 emphasises that data control is not only a system requirement — it is a behavioural requirement. The discipline of staff determines whether data remains accurate, complete and secure.



Technician responsibilities include:

- Recording data accurately and legibly
- Using controlled templates and validated systems
- Avoiding informal notes or uncontrolled spreadsheets
- Following access and security rules
- Documenting amendments correctly
- Reporting data issues immediately
- Protecting passwords and accounts
- Ensuring records are complete before submission

Technicians generate and handle data daily. Their discipline protects traceability and prevents errors.

Management responsibilities include:

- Overseeing data systems and access controls
- Verifying data integrity and completeness
- Authorising changes and amendments
- Ensuring backups and security measures are effective
- Reviewing audit trails and system logs
- Ensuring compliance with retention and disposal requirements
- Protecting sensitive information
- Ensuring alignment with the quality system

Management provide authoritative assurance that data is managed responsibly. Their oversight reinforces trust and demonstrates accountability.

Together, technicians and management form a **defence** that protects the laboratory's digital backbone. Clause 7.11 ensures that data is not only collected — it is safeguarded with discipline, accuracy and integrity.

Digital Integrity, Accuracy and Responsible Information Control

Data integrity is measurement integrity.

Every accredited laboratory depends on the accuracy, completeness, security and traceability of its data. Clause 7.11 ensures that information is protected throughout its entire lifecycle.

Why Data Control Matters – Protecting Accuracy and Trust

Raw measurements, calibration records, environmental logs, instrument outputs, calculations, metadata, amendments and final reports all form the evidence that supports technical validity. Clause 7.11 ensures that this evidence remains accurate, complete and secure.



Managing Electronic and Paper-Based Data – Unified Discipline Across Systems

Laboratories must manage both electronic and paper-based data under controlled conditions. Digital systems must operate with validated templates, locked formulas, access restrictions and audit trails. Paper records must be legible, permanent, corrected properly and stored securely. Weakness in either environment threatens traceability and reliability.

Ensuring Data Integrity – Accuracy, Completeness and Protection Against Alteration

Data integrity requires protection against accidental or intentional alteration. Clause 7.11 demands controlled access, password protection, validated formulas, documented amendments and secure templates. Integrity also includes completeness — missing data, partial records or undocumented changes weaken the chain of evidence.

Backup, Security and Continuity – Safeguarding Data Against Loss

Data loss is one of the most serious risks in an accredited laboratory. Clause 7.11 requires regular backups, secure storage, redundancy, access control, encryption, physical security and continuity planning. Laboratories must be able to restore data quickly and accurately after disruptions.

Technician and Management Responsibilities – Discipline and Authoritative Oversight

Technicians discipline determines whether information remains accurate and complete. They must follow controlled procedures, avoid informal shortcuts and ensure records are correct before submission. Management oversee data systems, verify integrity, authorise changes, ensure compliance with retention rules and protect sensitive information.

Data is not just information — it is evidence. Protecting it is protecting the laboratory's credibility.