



UNDERSTANDING ISO 17025 CLAUSE 4.2 - CONFIDENTIALITY

Why Confidentiality Matters – Trust, Protection and Professional Integrity

Clause 4.2 is the second foundational clause in ISO/IEC 17025, and it sits directly beside impartiality for a reason. Confidentiality protects the laboratory's reputation, client trust, commercial relationships, and the integrity of sensitive information. It ensures that all data, results, records, communications and client-specific details are protected from unauthorised access, disclosure or misuse.

Confidentiality protects clients. It ensures that their information, samples, results and commercial interests remain secure and private.

Confidentiality protects personnel. It ensures that technicians are shielded from inappropriate requests, external pressure or attempts to access information improperly.

Confidentiality protects the management system. It ensures that records, communications and decisions remain controlled, traceable and protected.

Confidentiality protects the laboratory's credibility. It ensures that clients trust the laboratory with sensitive information, knowing it will be handled professionally and securely.

Clause 4.2 requires laboratories to define confidentiality responsibilities, protect information, control access, manage risks and demonstrate that confidentiality is maintained at all times. Confidentiality is not optional — it is a core requirement.

Confidentiality is not secrecy — it is protection.

Clause 4.2 ensures that the laboratory safeguards information with discipline, clarity and professionalism.

Risks to Confidentiality – Exposure, Access and Information Vulnerability

Clause 4.2 requires laboratories to identify risks to confidentiality. These risks may arise from people, processes, technology, communication channels or operational structures. Identifying risks is essential to protecting sensitive information.

Sources of Confidentiality Risks

Risks may arise from:

- Unauthorised access to records
- Improper handling of samples
- Weak digital security
- Inadequate physical controls
- Informal communication
- Client pressure
- Supplier interactions



- Shared workspaces
- Social media exposure
- External visitors
- Internal politics

Types of Confidentiality Risks

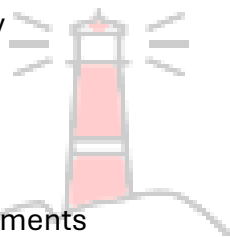
Risks may include:

- Disclosure of client information
- Sharing results without approval
- Discussing sensitive work publicly
- Leaving records unsecured
- Allowing unauthorised personnel into restricted areas
- Using personal devices for laboratory communication
- Storing data in uncontrolled locations

Why Risk Identification Matters

Identifying risks ensures that laboratories:

- Recognise vulnerabilities early
- Protect sensitive information
- Strengthen controls
- Maintain client trust
- Demonstrate compliance
- Uphold ISO/IEC 17025 requirements



Clause 4.2 ensures that confidentiality risks are not ignored — they are identified, documented and addressed.

Protecting Confidentiality – Controls, Access Management and System Safeguards

Clause 4.2 requires laboratories to implement controls that protect confidentiality. These controls must be practical, effective and aligned with daily operations.

Controls That Protect Confidentiality

Controls may include:

- Access restrictions
- Password protection
- Secure storage of records
- Controlled communication channels
- Confidentiality agreements
- Visitor management
- Segregation of sensitive information
- Controlled sample handling
- Secure disposal of records
- Monitoring of high-risk areas



Access Management

Access must be granted based on:

- Role
- Responsibility
- Competence
- Operational need

Access must be removed when roles change or when personnel no longer require it.

System-Level Safeguards

Safeguards may include:

- Policies
- Procedures
- Digital security controls
- Physical security controls
- Training
- Internal audits
- Risk registers
- Management review inputs

Clause 4.2 ensures that confidentiality is protected through structured, documented and effective safeguards.

Demonstrating Confidentiality – Evidence, Records and Professional Conduct

Clause 4.2 requires laboratories to demonstrate confidentiality. **Demonstration means evidence** — not assumptions. Laboratories must show, through records, actions and controls, that confidentiality is maintained.

Evidence of Confidentiality Includes:

- Signed confidentiality agreements
- Training records
- Access logs/records
- Visitor registers
- Secure communication records
- Controlled sample handling documentation
- Audit findings
- Corrective actions
- Management review inputs
- Digital security logs/records

Why Demonstration Matters

Demonstration ensures that laboratories:

- Prove confidentiality to accreditation bodies
- Protect client trust
- Strengthen transparency



- Reinforce professional conduct
- Support defensible operations
- Maintain alignment with ISO/IEC 17025

Professional Conduct

Confidentiality must be demonstrated daily through:

- Controlled communication
- Secure handling of information
- Respect for client privacy
- Evidence-based decisions
- Adherence to procedures

Clause 4.2 ensures that confidentiality is visible, traceable and defensible.

Technician and Management Responsibilities – Protection, Discipline and Leadership Accountability

Confidentiality is a shared responsibility. Clause 4.2 emphasises that both technicians and management must protect confidentiality through their actions, decisions and conduct.

Technician Responsibilities

Technicians must:

- Handle information securely
- Follow confidentiality procedures
- Report confidentiality risks
- Avoid discussing sensitive work publicly
- Protect client information
- Use approved communication channels
- Maintain professional boundaries
- Escalate concerns immediately

Technicians are the frontline protectors of confidentiality.

Management Responsibilities

Management must:

- Establish confidentiality policies
- Identify and evaluate risks
- Implement controls
- Protect personnel from inappropriate requests
- Allocate resources
- Ensure secure systems
- Review confidentiality during audits and management reviews
- Take action when confidentiality is threatened

Management provides the leadership that keeps confidentiality intact.



Together, technicians and management form a **dual-layer confidentiality structure** that protects trust, strengthens credibility and ensures defensible operations.

Information Protection, Professional Conduct and System Discipline

Clause 4.2 becomes unmistakably clear: **confidentiality is the laboratory's promise of protection**. It safeguards client trust, protects sensitive information, shields personnel from inappropriate requests, and preserves the integrity of the management system. Clause 4.2 is not administrative — it is strategic. It ensures that information is handled with discipline, professionalism and respect.

Why Confidentiality Matters – Trust, Protection and Professional Integrity

Confidentiality is the second foundational clause in ISO/IEC 17025. It protects clients, personnel, commercial interests and the laboratory's reputation. Confidentiality ensures that sensitive information — results, records, communications, sample details, client identities — is protected from unauthorised access or disclosure. Clause 4.2 ensures that confidentiality is not secrecy, but structured protection.

Risks to Confidentiality – Exposure, Access and Information Vulnerability

Confidentiality risks arise from people, processes, technology, communication channels and operational structures. Risks may include unauthorised access, improper sample handling, weak digital security, informal communication, social media exposure, shared workspaces or external visitors. Clause 4.2 requires laboratories to identify these risks proactively, document them and treat them as vulnerabilities that must be controlled. Risk identification is the first step in protecting sensitive information.

Protecting Confidentiality – Controls, Access Management and System Safeguards

Confidentiality becomes operational through controls. These include access restrictions, secure storage, password protection, confidentiality agreements, visitor management, controlled communication channels, segregation of sensitive information and secure disposal of records. System-level safeguards such as policies, procedures, digital security, physical security, training, audits and management reviews ensure confidentiality is embedded into the management system. Clause 4.2 ensures that information protection is structured, documented and effective.

Demonstrating Confidentiality – Evidence, Records and Professional Conduct

Confidentiality must be demonstrated — not assumed. Evidence includes signed agreements, access logs/records, visitor registers, secure communication records, audit findings, corrective actions and management review inputs. Professional conduct ensures confidentiality is visible in daily work through controlled communication, secure handling of information, respect for client privacy and adherence to procedures. Clause 4.2 ensures that confidentiality is traceable, defensible and transparent.



Technician-Level and Management Responsibilities – Protection, Discipline and Leadership Accountability

Confidentiality focuses on the shared responsibilities of technicians and management.

Technicians handle information securely, follow procedures, report risks, avoid discussing sensitive work publicly and use approved communication channels.

Management establishes policies, evaluates risks, implements controls, protects personnel, ensures secure systems, allocates resources and takes action when confidentiality is threatened. Together, they form a **dual-layer confidentiality structure** that protects trust and strengthens credibility.

Confidentiality is the laboratory's commitment to protection — and laboratories that protect information protect their reputation.

Clause 4.2 ensures that confidentiality is intentional, evidenced and led with discipline.

