SQM Auto QA Trial

Secure Audio File Upload, Storage, and AI Evaluation

SQM's Auto QA Trial Web Application is a self-hosted secure platform, designed to protect highly sensitive call recordings at every stage. From upload through storage, access, retention, transcription, and AI evaluation. Security is embedded into the architecture, not added as an afterthought.

End-to-End Encryption by Design

- All uploads and downloads are protected using modern Transport Layer Security (TLS) encryption to prevent interception.
- Every recording is encrypted using industry-standard cryptographic algorithms before storage.
- Files are encrypted with unique keys per recording, ensuring that even in the unlikely event of infrastructure access, data remains unreadable.
- Encryption keys are managed separately from application data using secure key management practices, reducing risk and limiting blast radius.

Zero Public Access Architecture

- Audio files are never stored in publicly accessible web directories.
- All access requests are validated through authenticated application endpoints.
- Direct file URLs are never exposed.
- Time-limited, permission-validated access ensures strict control.

Granular Access Control

Our platform enforces strict access governance:

- Role-based access control (RBAC)
- Organization-level isolation (multi-tenant separation)
- Least-privilege principles
- Full audit logging of every upload, download, and access attempt

Every interaction with a file is logged for traceability and compliance.

Upload Validation & Threat Protection

All uploads are treated as untrusted input and undergo:

- File type verification
- Size and format enforcement
- Virus and malware scanning

- Secure storage handling

Self-Hosted, Fully Controlled

- Deployed within your environment
- No third-party storage dependency
- No cloud storage
- Infrastructure separation between application, database, storage, and key management

Your sensitive data never leaves our controlled infrastructure. Only redacted data is sent to a cloud service to perform the call evaluation.

Data Protection for Recordings & Transcripts

Sensitive conversation data is handled with strict controls.

- Controlled access to audio, transcripts, and QA outputs
- Encryption in transit and at rest
- Call recordings are not retained and not used for AI training
- Redaction of Personally Identifiable Information (PII) and Protected Health Information (PHI) from transcripts

Security extends to both original recordings and derived AI outputs.

Secure AI Design to Reduce Leakage & Misuse

Built-in controls reduce common AI failure modes.

- Guardrails to limit unintended disclosure
- Controls to reduce prompt manipulation risks
- Tenant segmentation to prevent cross-customer exposure

AI workflows are engineered to minimize sensitive data leakage.

LLM-Specific Threat Modeling & Guardrails

Aligned with OWASP guidance for LLM applications.

- Input/output handling controls to reduce unintended disclosure
- Prompt injection mitigation strategies
- Isolation controls to prevent cross-tenant data exposure

We proactively design against known LLM security risks.

Monitoring, Quality & Continuous Improvement

AI systems are continuously evaluated and monitored.

- Monitoring for drift, anomalies, and unexpected outputs
- Human review pathways for high-impact or exception cases
- Detection of anomalous access or export behavior
- Documented AI-specific incident response processes
- Post-incident reviews and control improvements

Our AI security program evolves as threats and customer expectations change.

Why This Matters

Highly sensitive audio often contains confidential, financial, medical, or regulated information. Our platform is purpose-built to protect that data with enterprise-grade security, operational transparency, and compliance-ready controls.

Because AutoQA processes sensitive customer conversations using AI, SQM applies a structured, lifecycle-based AI risk management program aligned to ISO/IEC 23894 guidance. This ensures AI risks are identified, assessed, and managed throughout design, deployment, and ongoing operations.

For more information regarding SQM's AI security practices, visit our website Data Security page.