CCPA-aligned AI security practices for AutoQA

SQM's AutoQA service uses **LLMs** to generate quality insights from customer conversations. Because we process sensitive content like **call recordings and transcripts**, we operate with controls designed to support our customers' California Consumer Privacy Act (**CCPA)** privacy and security obligations, including the expectation that organizations implement **reasonable security procedures and practices appropriate to the nature of the information**.

Specifically, SQM's practices ensure that we are **compliant** with the CCPA requirements for how we **collect, use, share, sell, or "share" (for cross-context behavioral advertising)** and protect **California residents'** personal information.

How we use data

- **No model training on customer data:** We do **not** use customer recordings or transcripts to train foundation models.
- **Purpose limitation:** Customer data is processed to deliver the AutoQA service and related operational functions consistent with customer instructions (e.g., analytics, quality scoring, reporting).

"No sell / no share" posture and contract controls

CCPA draws an important line between using data to provide a service and **"selling" or "sharing"** data (including "sharing" for **cross-context behavioral advertising**).
Our approach is designed to align with service-provider/contractor expectations, including:

- Contract terms that prohibit **selling or sharing** customer personal information processed for the service.
- Controls intended to prevent **cross-customer data mixing** and limit data use to the contracted business purposes.

Security controls for recordings, transcripts, and AI outputs

To protect personal information handled by AutoQA, we apply layered safeguards such as:

- **Access controls:** role-based access and least-privilege permissions for audio, transcripts, and QA outputs
- **Encryption:** protections for data **in transit and at rest** (including derived artifacts like QA summaries and scoring outputs)
- **Logging and auditability:** monitoring and audit trails to detect and investigate unauthorized access patterns
  These controls are designed to support the CCPA security expectation for "reasonable security procedures and practices."