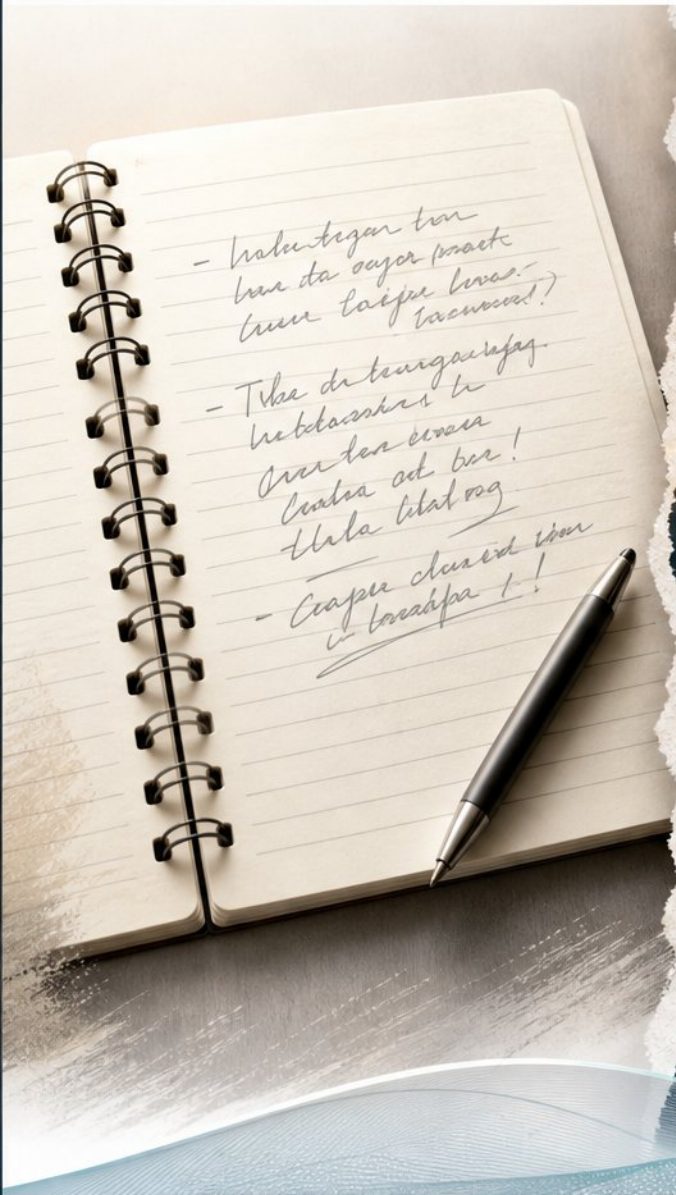


Call Recording Tools for User Research

- Covers tool selection, configuration, and governance for call recording
- Core tension: durable evidence versus consent, security, and compliance
- Built for UX researchers, research ops, and privacy-conscious product teams
- Scope: capture, tool choice, secure storage, analysis, and responsible retention



Why Recording Beats Notes Alone



- Notes capture only 20–40% of conversation content; recordings preserve verbatim language and nuance



- Recordings enable re-analysis, asynchronous review, and reduce observer bias



- Evidence trail links decisions and quotes back to original sessions



- Recording without synthesis is just expensive storage

Build the Privacy and Consent Foundation First



- Gain separate consent: study, record, transcribe, store, share



- Consent: specific, informed, granular, plain-language, opt-in



- Regulatory touchpoints: GDPR, CCPA/CPRA, HIPAA



- Voice/face may be biometric: justify video, get explicit consent



- DPAs required for every third-party handler in workflow



Map the Tool Landscape: Capture, Analysis, or Both



- Four shapes: meeting tools, browser recorders, research platforms, sales call recorders
- Separate capture from analysis—one tool rarely does both well
- Browser recorders capture clean, per-participant tracks for quoting
- Reserve mixed-track Zoom recordings for archives, not evidence
- AI-native platforms shift your role from moderator to interpreter

Select the Right Tool for Your Context

- Match the tool to your bottleneck: recruitment, analysis, or repository management
- For enterprise teams, a clean security review often outweighs feature depth
- Ask vendors about data residency, subcontractors, and retention APIs
- Evaluate integration depth with your existing research toolkit
- Pilot two or three tools on real studies before committing



Capture Clean Audio and Screen Evidence

- Prioritize audio quality over video; use headphones and quiet rooms
- Configure screen share and picture-in-picture capture
- Set up backup recording for unstable connections
- Label recordings with participant ID, study ID, and date
- Confirm verbal consent on the recording for audit



Secure Storage and Least-Privilege Access

- Store recordings in encrypted, dedicated systems, separate from chat and drives
- Apply least-privilege access: separate view, download, share, and delete rights
- Define roles for researchers, research ops, legal, and observers
- Revoke access immediately when roles change
- Use automated, purpose-based retention tiers by file type and identifiability
- Maintain audit logs for every access, download, and deletion event



Transcription, Search, and Analysis Workflows



- Review only risky details before sharing transcripts



- Timestamps, tags, and clips link findings to source evidence



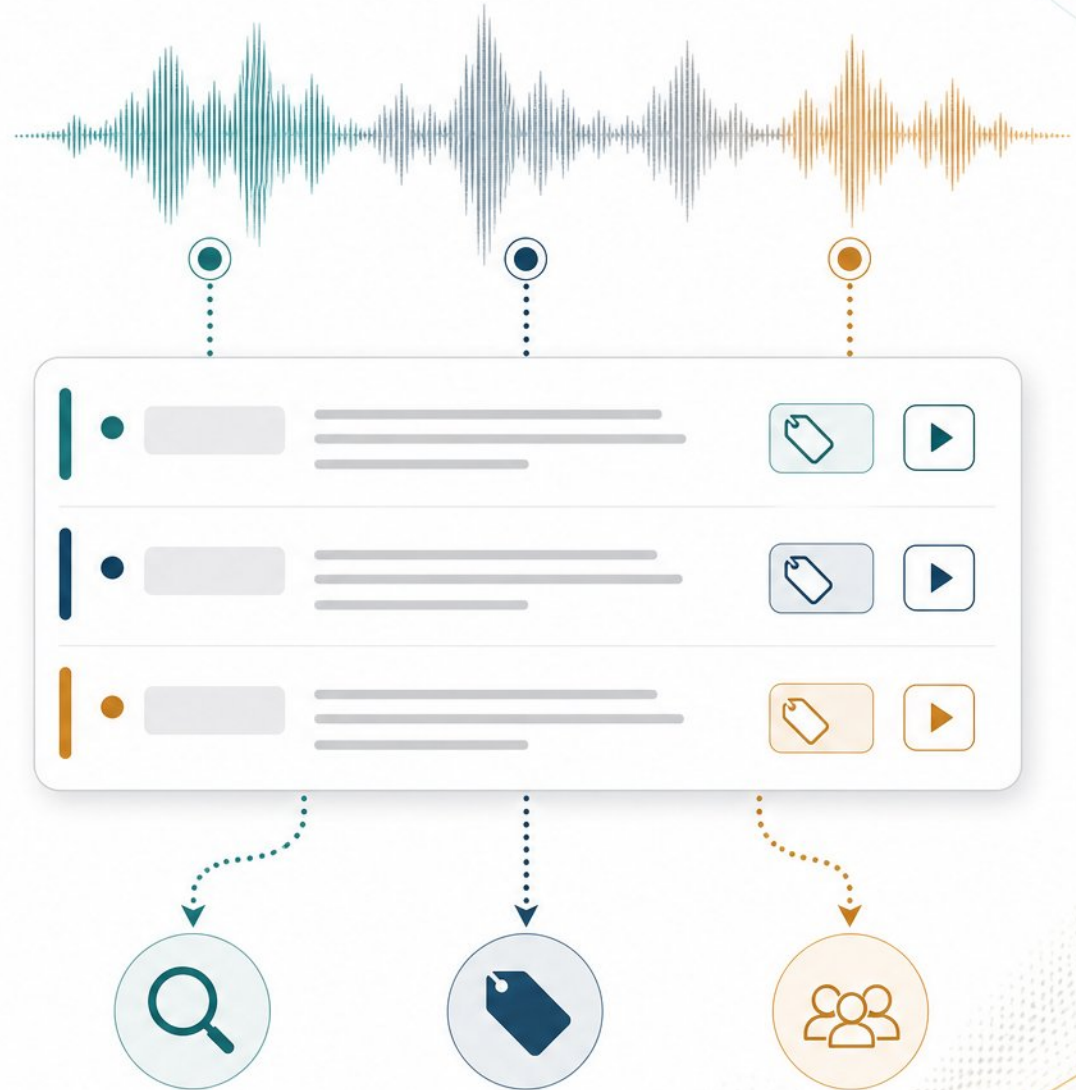
- Traceability from insights back to recordings builds credibility



- AI drafts themes, but humans own interpretation and decision



- Transcripts are raw evidence, not the final output



Share Clips with Stakeholders Responsibly



Match artifact to audience:
raw recording, clip, transcript,
or summary



Brief stakeholders on context,
confidentiality, and usage limits



Redact names, company details,
sensitive workflow data before sharing



Revoke access after project close;
document who viewed what



Make sharing a deliberate
governance step, not ad hoc
file transfer



From Recording to Durable Research Artifact



- Transform call evidence into findings logs, journey maps, and decision records



- Keep only what supports future decisions; practice data minimization



- Tie recordings to study IDs, consent records, and participant metadata



- Retain raw audio shortest; de-identified insights longest



- Reusable evidence packets: claim, quote, timestamp, and why it matters



RECORDING



ORGANIZE



GOVERN



CREATE ARTIFACTS

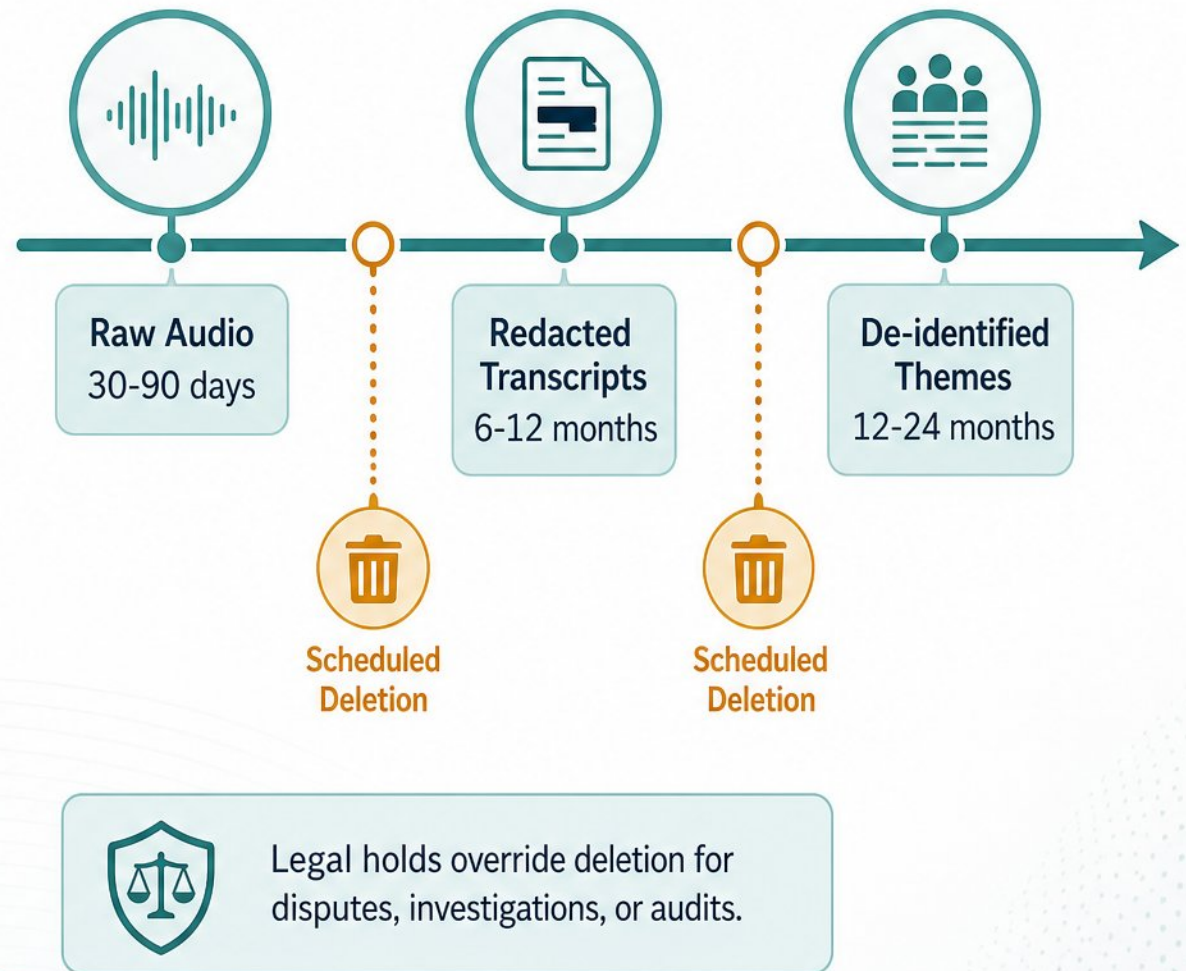


RETAIN & PRESERVE

CHAIN OF CUSTODY

Retention and Deletion Policies That Actually Work

- Align policies with scope, purpose, storage, access, and legal holds
- Use tiered retention: raw audio 30-90 days, redacted transcripts 6-12 months, de-identified themes 12-24 months
- Automate deletion workflows and log every destruction event
- Legal holds override deletion for disputes, investigations, or audits
- Over-retention is a liability—store only as long as necessary



Design a Consent Flow That Holds Up

- Separate checkboxes for participation, audio, video, screen recording, transcription, and quotes
- Name data controller, purpose, data access, retention period, and transfer mechanisms
- Use plain language; avoid vague claims and bundled approvals
- Verbal consent is permissible, but written or email consent provides a cleaner audit trail
- Provide easy withdrawal and honor deletion requests within stated timelines

☐

Participation

☐

Audio Recording

☐

Video Recording

☐

Screen Recording

☐

Transcription

☐

Use of Quotes



Data Controller

Name of the entity responsible for your data



Purpose

Why we collect and use your data



Data Access

Who can access your data



Retention Period

How long we retain your data

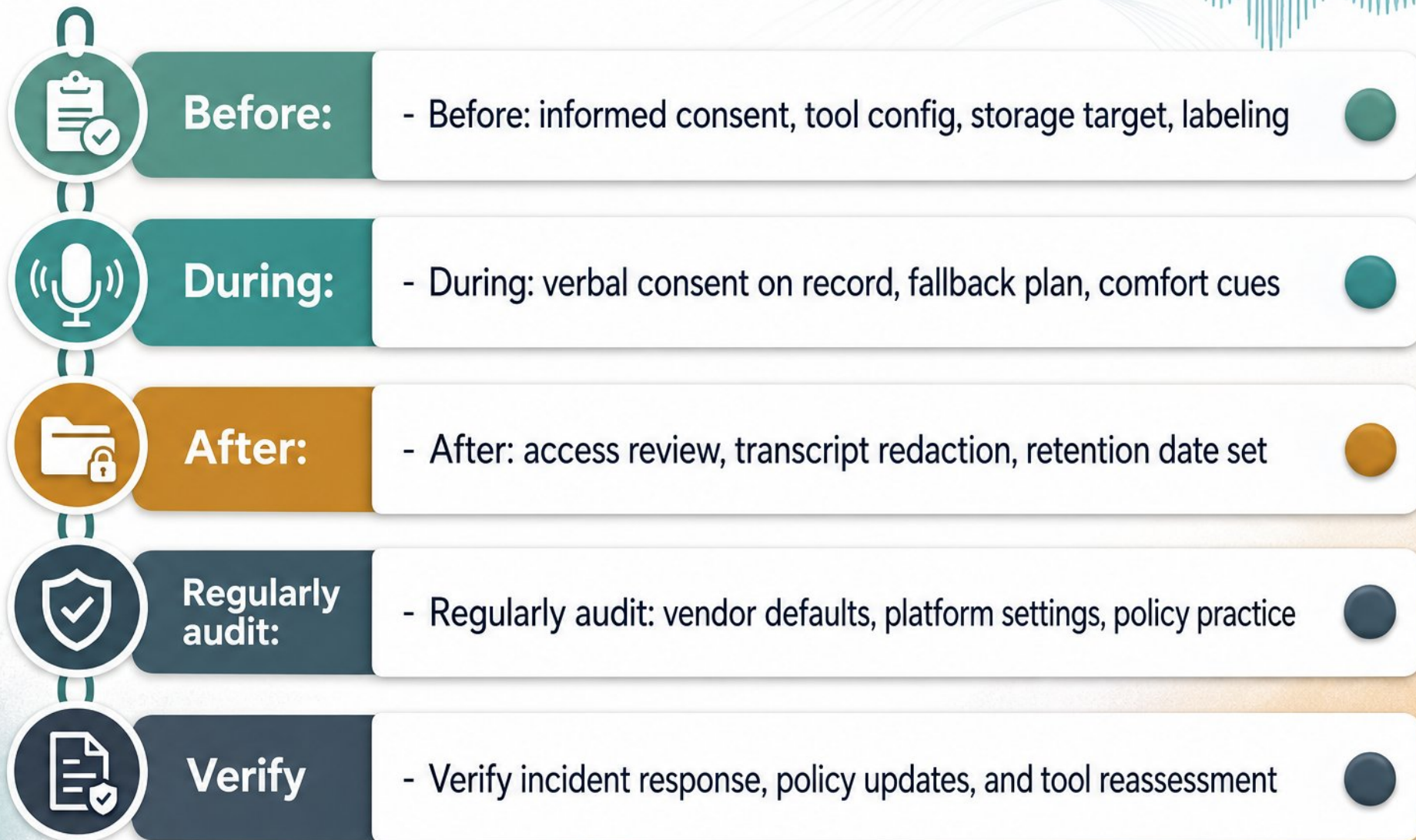


Transfer Mechanisms

How your data may be transferred



Checklist for Privacy-Conscious Recording Programs



From Policy to Practice: Run a Recording Program That Lasts



Treat recording as governance,
not a feature toggle



Align tools with the most
restrictive jurisdiction



Document lawful basis, consent
flow, retention, and access



Reassess your stack as the
research program evolves



Capture the right evidence,
safely, for decisions



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/bb7022e4/public