AI Recording and Data on Projects: Contractor-Specific Guardrails

(Part 2 of our series on AI Data and Preservation in Construction Projects)

As artificial intelligence (AI) tools move from the back office to the jobsite trailer, contractors face new risks that extend beyond data preservation. AI assistants that record meetings, capture field conditions, or generate summaries can trigger consent, confidentiality, and data-leakage issues—sometimes before anyone realizes the tool was even active.

This second article in our AI series focuses on practical guardrails contractors should adopt before disputes arise.

1. Jobsite Note-Taking Bots: Consent and Disclosure

Meeting bots such as OtterPilot, Fireflies.ai, or Copilot in Teams often record automatically when invited to a meeting or added to a recurring channel. Contractors should:

- **Disclose and obtain consent** before recording project meetings, especially if outside participants (owners, subs, or inspectors) are present.
- **Coordinate with counsel** to confirm compliance with federal and state consent laws and with project-specific confidentiality obligations. *Never record a meeting with legal counsel without consulting first.*
- **Identify the recording system** (*e.g.*, "recorded by OtterPilot for internal documentation") in invitations or meeting chat.

A short, standardized disclosure or footer—similar to safety or EEO notices—can reduce risk while maintaining transparency.

2. For General Contractors: Lead by Policy and Practice

GCs sit at the center of the information ecosystem. They should:

- **Publish a short AI use and recording protocol** that governs subcontractor and vendor practices (*e.g.*, consent, approved tools, and data routing).

- **Incorporate flow-down clauses** into subcontracts requiring disclosure of AI use and adherence to privacy and recording policies.
- **Integrate AI review** into project startup checklists—alongside safety, site security, and document control procedures.
- **Manage risk across multiple platforms**. GCs often use project management suites (Procore, Autodesk Build, etc.) that integrate AI; they should ensure connectors do not replicate or leak data outside the governed environment.
- **Coordinate with the owner** on notice templates and data-retention settings to ensure consistency across tiers; owner sets the standard and GC standardizes and enforces it.

GCs are the "traffic controllers" of AI governance—responsible for harmonizing compliance between owners and subs.

3. Subcontract Clauses on Recording and AI Use

Many standard subcontracts were written before AI meeting assistants or transcription tools existed. Contractors should now include:

- **Explicit clauses** addressing whether subcontractors may use AI recording or summarization tools on project communications.
- **Obligations to notify** the general contractor (and possibly the owner) before deploying AI that captures jobsite data or voice/video.
- **Limitations on disclosure** of recordings or transcripts outside the project team, tying back to confidentiality and data-use clauses.

Well-drafted clauses prevent later disputes over "unauthorized recordings" or mishandled AI data.

4. Protecting Proprietary Information from AI Tool Leakage

Large language models and AI assistants often send prompts or context data to cloud servers. Without guardrails, that could expose specifications, estimates, bid strategies, or means-and-methods.

Practical steps include:

- **Use enterprise or private AI environments** that do not retain or train on project data.
- **Classify prompts as confidential** when drafting or reviewing specs. Suggestions for where and how to do this follow:

- Define AI prompts and outputs as “Confidential Information” in contracts.
- Label prompts (*e.g.*, “CONFIDENTIAL PROJECT PROMPT – SPECIFICATION DRAFTING”).
- Store prompts and outputs with project records under restricted access.
- Avoid including proprietary or identifying data in public AI tools.
- Enable or require platform confidentiality and audit features.
- Require NDAs or addenda covering AI use by consultants or vendors.
- Include AI prompts in document retention and legal hold policies.

- **Train teams** never to paste proprietary schedules, estimating sheets, or pricing data into public or consumer AI tools.

Consider integrating this into your cybersecurity or IT acceptable-use policies. Review those policies regularly, to troubleshoot and update.

5. BYOD and Fleet Device Configurations

Bring-Your-Own-Device (BYOD) policies are another weak spot. Phones, tablets, and wearables may have microphones, cameras, or AI assistants that record inadvertently.

To mitigate:

- **Disable automatic voice capture** or “always-listening” features on devices used in secure project areas.
- **Apply mobile device management (MDM)** settings to separate personal from project data.
- **Educate field users** about when recording features must be turned off—especially during walkthroughs of sensitive facilities.

Post signage, and revisit posting locations as project progresses.

6. Standardized Owner/GC “AI Recording” Notices

Owners and general contractors can promote consistency by adopting a short, project-wide notice or policy such as:

“AI-enabled recording, transcription, or summarization tools may only be used with prior written approval of the Owner/GC and after all participants are notified and consent obtained.”

Including this in project kickoff packets or orientation meetings helps align expectations across multiple subcontractors and consultants.

7. Avoiding Incidental Capture

Projects in healthcare or education environments add another layer of compliance. AI recording tools could inadvertently capture:

- **Protected Health Information** under HIPAA, or
- **Student information** protected under FERPA.

Contractors should ensure these areas are designated as **no-record zones**, and that any video, audio, or AI-generated summary from such spaces is either redacted or deleted under counsel's direction.

8. Coordinating with Preservation Obligations

As noted in *Part 1* ("Preserving AI-Generated Artifacts in Construction"), once a dispute or claim arises, recordings and AI-generated summaries may become evidence subject to a litigation hold. The front-end controls above make those obligations easier to meet by ensuring AI data is (1) created lawfully, (2) stored predictably, and (3) mapped to the right custodians.

Conclusion

AI tools can enhance communication and documentation, but they also create new discovery and privacy risks. Contractors who proactively define when and how AI may record, summarize, or store project data—and who align those practices with contract terms and preservation duties—will minimize surprises later.

Think of AI recording not just as a technology issue, but as part of a contractor's evolving information governance program—one that bridges privacy, contracts, and litigation readiness.

For a quick reference "Guardrails by Role" chart click here.

For further information on these developments, please contact Kristi Belt and Susan Broach.