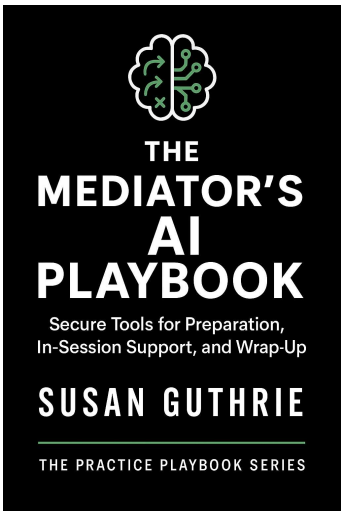

The Mediator's AI Playbook: Secure Tools for Preparation, In-Session Support, and Wrap-Up

"The Cheat Sheet"

Executive Summary

Artificial Intelligence offers powerful tools for mediation practice management and pre-mediation analysis, but maintaining client confidentiality and attorney-client privilege requires careful selection of enterprise-grade solutions designed specifically for legal professionals.

Practice Management AI Tools by Category

Client Intake and Screening

- **FourthParty**: Customizable booking intake and automated client notifications - designed specifically for ADR professionals
- **ADR Notable**: Dynamic data capture screens and streamlined intake processes for dispute resolution practitioners

Calendar and Scheduling Management

- **CalendarHero**: Automated meeting scheduling with participant communication
- **FourthParty**: Instant appointment setup with automated reminders
- **ADR Notable**: Multi-party meeting coordination with CalendarHero integration

Document Generation and Templates

- **ADR Notable**: Document builder with auto-transferred notes and template library
- **ChatGPT / Claude / Gemini / CoPilot:** For general form and template creation, the widely available AI tools can be very helpful.

Communications Management

- **FourthParty**: Automated multi-party email communication and reporting
- **Sonix**: Meeting summaries and encrypted transcripts

Billing and Financial Management

- **FourthParty**: Custom invoicing, Stripe payments, and automated collections
- **ADR Notable**: Split invoicing, payment tracking, and account management

---

Pre-Mediation Analysis Tools (Confidential & Private)

Specialized Mediation AI Platforms

NexLaw AI

- Bank-grade 256-bit encryption for data at rest and in transit
- Client data never used to train AI models, remains within specified jurisdictions
- ISO 27001 and SOC 2 certified infrastructure
- **Use Case**: Pre-mediation analysis, case management, settlement predictions

NextLevel Mediation

- Decision Sciences and AI tools for smarter mediation decisions
- Analytical Hierarchical Process and Decision Trees for litigation outcome analysis
- **Use Case**: Pre-mediation analysis, risk assessment, decision support

Confidential Computing Platforms

Opaque Systems

- Confidential AI workflows on sensitive data without exposure or compliance risks
- Pre-verified agents with cryptographic proof of compliance and verifiable audit trails

- **Use Case**: Multi-party data analysis, confidential case research

Fortanix Confidential AI

- Secure environment for sensitive datasets using confidential computing
- Azure AKS with SGX enabled nodes for hardware-level security
- **Use Case**: Predictive analytics, pattern analysis in dispute data

---

In-Session Support Tools for Mediators

These AI tools can be used during mediation sessions to support option generation, visual aid creation, risk analysis, and decision support. All listed tools meet or can be configured to meet legal/ethical confidentiality requirements when used with proper safeguards.

Secure Option Generation & Brainstorming

NexLaw AI (Enterprise):

- Secure brainstorming prompts for solution generation without exposing confidential details.
- Supports anonymization features and does not train on your data

Microsoft Copilot for Legal (Enterprise):

- In-session generation of creative settlement options directly in Word, Excel, or Whiteboard.
- Integrated with Microsoft Purview for compliance, privilege protection, and sensitivity labeling

Casetext CoCounsel:

- Facilitates secure drafting and reframing of proposals, with legal-grade privilege protections

Visual Aid Creation (Secure & Confidential)

Canva for Teams (Enterprise):

- Use Magic Design to securely generate diagrams, timelines, and flowcharts without public data exposure.
- Store files in controlled cloud locations with SSO and DLP access restrictions

Lucidchart Enterprise:

- Create process maps, decision trees, or org charts in real time with bank-grade encryption

Microsoft Whiteboard with Copilot (Enterprise):

- Collaboratively build visual frameworks during a mediation session, secured within Microsoft 365 compliance boundaries

Risk Analysis & Reality Testing

NextLevel Mediation:

- Uses secure decision science models (AHP, decision trees) for in-session outcome analysis and BATNA/WATNA comparison

Microsoft Copilot in Excel:

- Build and adjust damages models, cost-of-delay calculations, and probability matrices live with parties, while keeping data inside a privileged environment

Opaque Systems:

- Conduct multi-party, sensitive data modeling without revealing source data through confidential computing protocols

Real-Time Summarizing & Note Capture (Requires informed consent from all participants)

NexLaw AI:

- Privilege-protected session summaries and anonymized caucus notes

Bliro:

- Secure, no-recording-stored note transcription with GDPR compliance and encrypted key storage

Microsoft Teams Premium with Intelligent Recap:

- In-session recap of discussion points stored securely in Microsoft 365 with compliance controls

---

Post-Mediation Support Tools for Mediators

These AI tools can be used after mediation sessions to assist with drafting memoranda, preparing settlement agreements, generating summaries, organizing case files, and following up with parties. All listed tools are suitable for mediators and legal professionals operating under ethical confidentiality obligations.

Drafting Memoranda of Understanding (MOUs) and Settlement Agreements

Microsoft Copilot for Legal (Enterprise)

- Drafts agreement language directly from structured notes taken during mediation.
- Integrates sensitivity labels to prevent unauthorized sharing.

Casetext CoCounsel

- Generates first drafts of legal clauses or entire agreements using legal-grade privilege protections.

NexLaw AI

- Creates secure clause libraries and populates settlement terms without training on client data.

Best Practice: Always review and edit AI-generated agreements manually, and clearly mark drafts as non-final until reviewed by the parties and their counsel.

Generating Session Summaries and Recap Notes

Bliro

- Creates encrypted bullet-point recaps without storing recordings.
- Separates joint and caucus notes for secure record-keeping.

Microsoft Teams Premium Intelligent Recap *(with consent)*

- Identifies key discussion points and next steps, stored in a compliance-controlled environment.

NexLaw AI

- Summarizes anonymized case data into concise mediator notes for future reference.

Best Practice: Store summaries in secure, access-controlled systems. Never send full caucus notes to the other party; redact or separate as needed.

Preparing Follow-Up Communication

Wordtune AI (Enterprise)

- Refines tone and clarity of follow-up emails to parties or counsel.
- Produces multiple tone versions (formal, collaborative, encouraging).

Microsoft Copilot in Outlook

- Generates follow-up messages summarizing agreements reached and outlining action items.
- Applies compliance metadata and sensitivity labels automatically.

Best Practice: Apply "Confidential" or "Attorney-Client Privileged" labels before sending, and verify all generated text for accuracy.

Organizing and Archiving Case Materials

Microsoft Copilot in OneNote / SharePoint

- Sorts and tags post-mediation documents, agreements, and notes for easy retrieval.

ADR Notable with AI Search

- Performs secure keyword searches across all case materials without leaving the encrypted platform.

Best Practice: Follow jurisdictional record retention requirements and delete AI processing files after finalization.

Clause and Agreement Language Optimization

Casetext CoCounsel

- Compares proposed clauses against legal best practices and similar settlements.

NexLaw AI

- Suggests plain-language versions of complex clauses for client understanding.

Best Practice: Keep original legal language intact for enforceability, but offer plain-language explanations in a separate, clearly labeled section.

Ethical Safeguards for Post-Mediation AI Use

- Use only enterprise-grade, legal-industry-compliant tools with documented privilege protections.
- Obtain explicit informed consent if processing any party-identifiable data through AI.
- Always anonymize inputs when possible.
- Clearly label AI outputs as drafts until reviewed by the mediator and/or counsel.
- Store all AI-assisted documents in secure, access-controlled environments with audit trails.

Legal-Specific Enterprise AI Tools

Microsoft Copilot for Legal (Enterprise)

- Microsoft Purview data security and compliance protections
- Can restrict AI from summarizing files based on sensitivity labels
- **Features**: Document analysis, case preparation, privilege-aware processing

Casetext CoCounsel

- AI legal assistant built specifically for attorneys and dispute resolution professionals
- **Features**: Legal research, document review, brief drafting

---

Security & Privacy Best Practices

"Confidentiality by Design" Approaches

- **Anonymization and Data Minimization**: Training models on anonymized data
- **Local Processing**: Running AI tools on secure, dedicated servers

- **Data Masking**: Replacing real names with generic identifiers

Implementation Requirements

- **Zero Data Retention**: Data never stored or used for training
- **Encryption**: Bank-grade 256-bit encryption at rest and in transit
- **Compliance**: ISO 27001, SOC 2, HIPAA, or FedRAMP certifications
- **Access Controls**: Granular permissions and audit trails

Legal Protections Needed

- **Attorney-Client Privilege**: Explicit protection of privileged communications
- **Confidentiality Agreements**: Business Associate Agreements (BAAs)
- **Data Sovereignty**: Control over where data is processed and stored
- **Audit Trails**: Complete logging for compliance and transparency

---

What NOT to Use: High-Risk AI Tools

Consumer-Grade AI Platforms (AVOID)

- **ChatGPT (Free/Plus)**: Data used for training, no privilege protection, can be subpoenaed
- **Google Bard**: No confidentiality guarantees
- **Claude.ai (Consumer)**: Lacks enterprise privacy controls
- **Private-GPT.ai**: Still relies on OpenAI infrastructure, lacks legal privilege protection

Why These Are Dangerous

- OpenAI CEO confirmed "ChatGPT does not provide legal privilege or legal confidentiality"
- Conversations can be subpoenaed and used in court
- Data may be used to train models and shared with other users
- Risk of attorney-client privilege waiver

Implementation Checklist

Before Adopting Any AI Tool:

- [ ] Verify enterprise-grade security certifications
- [ ] Ensure zero data retention policies
- [ ] Confirm attorney-client privilege protections
- [ ] Review vendor's legal industry experience
- [ ] Obtain client consent when required
- [ ] Establish clear usage policies for staff
- [ ] Implement regular security audits

Vendor Evaluation Questions:

- Do you serve legal/mediation clients?
- Can you provide attorney-client privilege protections?
- Will you sign legal industry compliance agreements?
- Do you have experience with legal discovery requirements?
- Where is data processed and stored?
- Can you guarantee data will never be used for training?

Key Takeaways

✅ **DO**: Use enterprise-grade AI tools designed for legal professionals

✅ **DO**: Prioritize tools with zero data retention and privilege protection

✅ **DO**: Obtain explicit client consent for AI-assisted processes

✅ **DO**: Implement comprehensive security policies and training

❌ **DON'T**: Use consumer-grade AI platforms for confidential information

❌ **DON'T**: Assume all "private" AI tools actually protect privilege

❌ **DON'T**: Input sensitive client data without verified security protections

❌ **DON'T**: Skip vendor security verification and compliance review

---

Contact Information

For questions about implementing secure AI tools in your mediation practice, consult with:

- Your bar association's ethics committee
- Cybersecurity and privacy legal counsel
- Enterprise AI vendors directly for security certifications

This guide is for educational purposes only and does not constitute legal advice. Always consult with qualified legal counsel regarding ethical obligations and technology implementation in your specific jurisdiction.