FOLEY HOAG

SOUND JUDGMENT: NAVIGATING THE LEGAL FRONTIER OF AMBIENT AI

BEST PRACTICES FOR USING AI NOTETAKERS IN SENSITIVE MEETINGS

AI notetakers are rapidly becoming staples of corporate meetings—bringing efficiency alongside new questions about confidentiality and compliance. This tip sheet offers practical best practices to harness their benefits while safeguarding sensitive information and reducing legal, privacy, and security risks.

1. VENDOR DUE DILIGENCE

- Vet AI notetaker vendors for security, privacy, and contractual protections.

2. OBTAIN PROPER CONSENT

- In jurisdictions with two-party consent laws, ensure all participants explicitly consent to the use of AI notetakers or recordings.
- Clearly disclose the presence and function of the AI notetaker at the start of meetings.

3. PROTECT ATTORNEY-CLIENT PRIVILEGE

- Avoid using AI notetakers in meetings involving privileged legal consultations, especially when discussing sensitive or confidential legal matters.
- Remind participants that the use of AI notetakers may jeopardize privilege, particularly in cross-border contexts where discovery rules may differ.

4. MANAGE RECORD RETENTION, REVIEW, AND DISCOVERABILITY

- Establish clear protocols for the retention and deletion of recordings, transcripts, and AI-generated summaries, in line with internal data retention policies.
- Limit the retention of ephemeral recordings used to generate summaries and apply short retention periods for both recordings and AI-generated notes, especially for sensitive meetings.
- Develop a policy on whether and how AI notes are reviewed against recordings, and under what circumstances recordings should be destroyed.
- Be aware that any recordings or transcripts may become discoverable in litigation.

5. SAFEGUARD INTELLECTUAL PROPERTY AND TRADE SECRETS

- Restrict access to AI-generated notes and transcripts to only those who need them, using fine-grained permissions.
- Ensure that sensitive technical or trade secret discussions are not accessible to broader teams (e.g., sales or non-technical staff).
- Vet enterprise license terms to confirm that proprietary information is not used for AI training or shared with third parties.

6. CONTROL STORAGE AND JURISDICTION

- Prioritize solutions that allow control over where data is stored, ideally in advantageous jurisdictions for privacy and security.
- Consider on-premises or private cloud AI notetaker solutions for highly sensitive meetings.

7. CLARIFY THE STATUS OF AI-GENERATED NOTES

- Clearly label AI-generated notes as unofficial and not as formal meeting minutes.
- Provide internal documentation and training to ensure staff understand the limitations and appropriate uses of AI notetaker outputs.

8. POLICIES, TRAINING AND AWARENESS

- Regularly update policies, plans and training as technology and legal requirements evolve, including by ensuring use of AI notetakers are specifically addressed in all policies and incident response and data breach plans.
- Train staff on when it is appropriate to use or disable AI notetakers, particularly for privileged or highly sensitive discussions.
- Regularly update policies and training as technology and legal requirements evolve.

KEY CONTACTS

COLIN ZICK

Partner
Chair, Healthcare Compliance Practice
Co-Chair, Privacy and Data Security Practice

+1.617.832.1275
CJZ@foleyhoag.com

CHRIS HART

Partner
Co-Chair, Privacy and Data Security Practice

+1.617.832.1232
CHart@foleyhoag.com

SAMUEL HOFF

Associate

+1.617.832.3011
shoff@foleyhoag.com

ERIK HUESTIS

Partner
Co-Chair, Technology Industry Group,
Registered Patent Attorney

+1.212.812.0325
ehuestis@foleyhoag.com

ROSE STANDIFER

Partner in Charge Denver Office

+1.720.782.5076
rstandifer@foleyhoag.com

ALLIE CLARK

Partner

+1.720.782.5077
aclark@foleyhoag.com