Publications

February 17, 2026 • Updates

The Hidden Risks of AI Notetakers: What Organizations Need to Evaluate Before Deployment

Key Takeaways:

- Organizations are rapidly deploying AI notetaking tools, creating new legal, privacy and security exposure.
- Those records can undermine privilege, expand cybersecurity risk and trigger domestic and international compliance obligations.
- Before deployment, organizations should establish internal policies on appropriate use, conduct security and contractual vetting, assess data transfer mechanisms, obtain required disclosures or consent and restrict use in privileged or highly sensitive settings.

Organizations are rapidly adopting AI notetaking and meeting assistant tools for their potential to improve efficiency and automate documentation. While these tools may enhance productivity, they also introduce new legal, privacy, security and compliance risk that organizations should carefully evaluate before implementation.

Below, we outline key data privacy and compliance risks and practical considerations for businesses that are integrating AI notetaking tools.

Third-Party Processing Can Undermine Confidentiality and Attorney-Client Privilege

For legal departments and law firms, AI notetakers create challenges for maintaining confidentiality and privilege. When an external AI provider processes meeting audio or transcripts, that third party may be considered outside the attorney-client relationship. Depending on the circumstances and safeguards in place, the involvement of this third party could risk a waiver of attorney-client privilege.

AI-generated transcripts also create permanent, searchable records of informal conversations that likely went undocumented in the past. Additionally, these AI-generated transcripts and summaries may not be completely accurate or fully reflect the conversation that took place — meaning having an AI notetaker in meetings may result in an inaccurate, non-privileged record of a sensitive or potentially damaging topic.

Related People

- Pavel (Pasha) A. Sternberg
- Caitlin A. Smith

Related Capabilities

- Privacy & Cybersecurity
- Artificial Intelligence & Machine Learning
- Technology

Centralized Audio and Transcript Storage Expands Cybersecurity Exposure

AI notetaking platforms are attractive targets for threat actors because of their centralized storage of meeting audio and transcripts. This means that the confidential information of organizations could be at risk in the event of vendor security failures, misconfigured access controls, unauthorized internal access or employees adopting tools outside of IT oversight. An added risk comes from “shadow IT” users deploying AI tools can that bypass existing IT controls and increase exposure to data security incidents.

Cloud-Based Processing and Vendor Rights Raise Data Control and Retention Concerns

AI notetaking tools generally process audio and text in the cloud. As a result, sensitive business discussions may be transmitted to and stored on third-party servers. Vendor terms of service may grant providers rights to access, store or analyze meeting content and, in some cases, use your organization’s input for product improvement or model training purposes. This means that without proper vetting, organizations may inadvertently expose sensitive data, strategic discussions or intellectual property outside their control.

Additional risk factors could include:

- Retention of information beyond the intended business use
- Inability to respond sufficiently to a destruction request
- Cross-border data transfers implicating unexpected privacy laws
- Broad integrations with a user’s calendar and email that expands access to organizational data
- Insufficient transparency into vendor security and subcontractor practices

Global Deployment May Trigger Cross-Border Compliance Obligations

For multinational organizations, deploying AI notetaking tools may trigger additional obligations under global data protection laws, including the EU GDPR and UK GDPR, PIPEDA in Canada and other international data privacy frameworks. Because the AI notetaking tools typically rely on cloud processing and global backend physical infrastructure, data may be transferred, accessed or stored across multiple jurisdictions.

International privacy laws generally require organizations to establish a lawful basis for processing personal data and limit data collection and data retention to that which is necessary and proportionate to the stated business purpose. Organizations may also be required to implement transfer impact assessments, standard contractual clauses or other lawful transfer mechanisms to account for cross-border data transfers.

International privacy frameworks also impose stricter obligations on data owners around vendor oversight, written data processing agreements and reasonable security safeguards. Where AI tools are used in the international employment context, disclosures to employees or employee representatives prior to implementation may be required.

Practical Next Steps for AI Notetaker Deployment

AI notetakers offer meaningful productivity benefits. However, without clear consent policies, governance frameworks, security controls and human oversight, they may introduce substantial legal, compliance and operational risk.

Organizations should:

- Establish clear governance structures and policies over when and how AI notetakers may be used
- Vet tools for security and data storage compliance
- Educate staff and obtain informed consent from meeting participants
- Limit use in privileged or highly sensitive contexts
- Implement appropriate contractual, technical and administrative safeguards to ensure privacy compliance

Careful evaluation and governance can help organizations reap the benefits of AI notetaking tools while mitigating associated risks. For more information regarding AI governance, privacy compliance or vendor risk management, please contact a member of Polsinelli’s Technology Transactions and Data Privacy team.