# Cautions When Using Artificial Intelligence Cloud Recording Software

## Overview

- Artificial Intelligence (AI) is reshaping the way we interact with technology and the world around us.
- While AI offers significant benefits, it also poses certain risks.
- This advisory reviews important considerations when using cloud-based AI meeting tools.

## AI Definition

Artificial Intelligence (AI) is not just a futuristic concept but a present reality that is reshaping how we interact with technology and the world around us. AI encompasses a range of technologies, such as machine learning, natural language processing, and computer vision. AI enables machines to perform tasks that once required human cognition, such as interpreting speech, identifying images, and making informed decisions. Through its ability to analyze vast amounts of data and learn from patterns, AI powers everyday applications like virtual assistants (e.g., Siri or Alexa), personalized recommendations (e.g., Netflix or Amazon), and even autonomous vehicles. As AI continues to evolve, it holds the potential to transform industries, enhance efficiency, and address some of the most complex challenges facing society today.

## AI Recording Bots

As part of NRECA's ongoing commitment to cybersecurity and data protection, we want to highlight important considerations when using cloud-based AI meeting tools. While these tools offer significant benefits, such as automated transcription, meeting summaries, and real-time insights, they can also raise privacy concerns, potentially make meetings feel intrusive, and also sometimes stifle open communication. Organizations handling sensative or regulated data must be expecially vigiliant about these risks.

## Key Data Protection Considerations

- **Knowing When AI Recording Software is Present is not Always Obvious**

  Remote meetings have become commonplace in business today. While you may be able to tell if AI recording software is present in a meeting room, it is less apparent over a Teams/Zoom call if a participant is using it. There are also wearable pendants that act like full-time listening AI, which someone could wear in a physical meeting or have on a table during a Teams/Zoom call.

**Action:** Be diligent to identify AI devices in meetings and set business policies around use of such recording devices. Consider announcing at the beginning of meetings whether you are using AI recording devices and require attendees to do the same. Some businesses take the approach to treat each meeting like the remote party is recording it, and that anything shared in the meeting space (verbally or otherwise) could be considered 'on the record.'

- **Terms and Agreements Can Change**

  Cloud-based AI tools operate under terms of service and privacy policies that can be updated at any time. These changes may affect how your data is used, stored, or shared.

  **Action:** Always review the terms of service and privacy policies before using any cloud recording application. Stay informed about updates, as changes could impact your compliance with cybersecurity standards or contractual obligations.

- **Data Storage and Sovereignty**

  Data recorded or processed by cloud-based AI tools may be stored in various locations, potentially outside your country. This raises concerns about data sovereignty and compliance with local laws, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

  **Action:** Verify where your data is being stored and ensure it aligns with your organization's data protection requirements. If handling sensitive information, consider whether local recording options might offer better control.

- **Data Private AI vs. Public AI**

  Public AI tools, such as those using large language models (LLMs), may use input data to train their models. This could lead to unintended exposure of sensitive information, even if the final output is scrubbed.

  Private AI solutions, on the other hand, may offer more control over data usage, but still require careful vetting.

  **Action:** Understand whether the AI tool you are using is public or private. For sensitive discussions, prioritize tools that explicitly state they do not use your data for model training or third-party sharing.

## Non-Disclosure Agreements (NDAs) and Confidentiality

Many organizations, including military-serving cooperatives, are bound by NDAs or other confidentiality agreements that may prohibit the use of AI recording tools in meetings. Recording a meeting without all participants' knowledge could violate these agreements, leading to legal or reputational risks if data is released.

**Action:** Consult with the meeting organizer and legal teams to get approval before joining the meetings.

## Before Removing the Application

Take a moment to think about the following to avoid unintended consequences when removing AI tools:

- Does the software hold any recordings, transcripts, or notes that you need? If so, download or back them up to a secure, compliant location before uninstalling.
- Does the software have any dependencies or any workflows, teams, or processes relying on this tool? For instance, if it has been used for meeting summaries, removing it might disrupt those activities. Identify who is using it and why.

**Alternative Solutions:** If the application serves a purpose (e.g., transcription for accessibility), plan for a replacement. Look for secure, organization-approved alternatives that comply with your privacy and security standards.

## Removing the Application

Here are some ways you can remove the application, if you find the software installed on devices and would like to remove them:

1. **Use the Standard Uninstallation Procedures for Your Operating System** (e.g., "Add or Remove Programs" on Microsoft Windows, dragging to Trash on Apple macOS).
2. **Disable Browser Extensions:** In your browser's extension menu, locate the unwanted tool and select "Remove" or "Disable."
3. **Revoke Access in Meeting Platforms:** For integrations with Microsoft Teams or similar platforms, go to "Apps" → "Manage your apps," and remove or revoke access for the tool.

## Proactive Steps Moving Forward

The following are some steps you can take to help mitigate the risks of using AI meeting tools in the future:

- Create clear rules about using cloud recording tools, especially in sensitive environments.
- Educate your employees to recognize the risks of unauthorized tools and encourage them to report suspicious software.
- Regularly audit all devices, browsers, and platforms for unapproved applications to catch issues early.

## Contact for Questions

**Wayne Koback**
Program Manager, Data Integration & Cloud Security
Wayne.Koback@nreca.coop

## Additional Information

NRECA offers a variety of resources and opportunities to assist our members in advancing their cybersecurity posture. Find out more on our website at: cooperative.com/cybersecurity.