

ZOOM • AI & PRIVACY

Maintaining Privacy in Zoom Meetings

What AI hears, what it keeps, and how to stay in control

Updated August 2026
University of Wyoming, Information Technology

When AI Joins the Meeting

AI tools aren't private by default

Depending on the platform and its terms, some AI tools do not keep your data private. Learn to anonymize data and use aliases.

Sensitive talk gets captured

AI can capture and share private information with others — and there is potential for information to leak across users.

Notification gaps

Zoom alerts everyone when AI is enabled — but people who join after it starts receive no notification at all.

High-sensitivity settings

Many organizations prohibit AI in clinical, telehealth, healthcare, and IRB meetings; some disable it entirely.

Zoom's AI Companion

AVAILABILITY

- Requires a paid Zoom Pro or Enterprise account — not available on free accounts
- Your organization must enable it; healthcare organizations often cannot
- Each individual must enable and configure every AI feature from the Zoom web portal

FEATURES

- In-meeting AI assistant — a helping hand during the meeting
- AI meeting summaries and notes that save time, and can be fed into other assistants
- AI smart recording for cloud recordings, letting anyone search and jump to a segment

Convenience is the point — and the exposure. Every summary is a searchable record of what was said.

Third-Party AI Notetakers

Apps like Otter.ai, Read.ai and Fireflies.ai can join your meeting and take notes for a participant.

Unknown handling

You do not know what is being done with the information these apps capture.

Invited by anyone

Any participant can bring one in — the host may never have agreed to it.

Often identifiable

They join as a separate instance and are frequently labeled as AI.

What to do: Tell participants before the meeting that these apps are not allowed — and that you will share Zoom AI Companion notes instead. Use a waiting room to screen them out.

Steps to Maintain Privacy

1

Know when not to use it

- Do not use Zoom AI Companion for clinical, telehealth or healthcare settings, IRB meetings, or other especially sensitive sessions
- Organizations can disable Zoom AI completely where the privacy risk outweighs the benefit

2

Configure AI Companion for privacy

- Turn off automatic start — get in the habit of starting and stopping features manually in the meeting
- Set "Automatically share summary with" to "Only me (meeting host)" so you can review before anything is sent

Steps to Maintain Privacy

3

Alert everyone that AI is in use

- Ask attendees to refrain from sharing private or sensitive information while AI is enabled
- Late joiners get no notification — say it out loud; the sparkle icon shows AI Companion is on

4

Disable it — then review before sharing

- Turn AI off for sensitive segments, or move that discussion to a breakout room where AI Companion is unavailable
- Always review summaries and recording notes, redacting sensitive details in the Zoom web portal before sharing