



Before you hit record: 7 security checks for AI meeting notetakers

The AI-savvy employee checklist



Quick context

AI meeting notetakers are showing up everywhere. They can feel like magic: joining your calls, taking down notes, and spitting out tidy recaps while you focus on the conversation. But not all AI notetakers are created the same when it comes to privacy and security of your meeting data.

In fact, some AI notetakers have already landed in hot water for secretly recording and storing conversations without proper consent. Cases like this are a reminder that even popular platforms can mishandle sensitive data and put both employees and companies at risk.

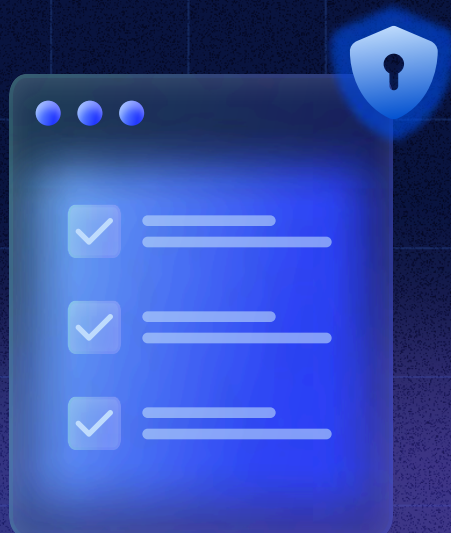
Why does this matter to you? Because when you bring a new AI tool into the workplace, even something as simple as a meeting notetaker, you're dealing with company information, customer conversations, and sometimes sensitive data that your security team is on the hook to protect.

The good news:

You don't have to be an IT expert to make smart choices when it comes to AI tooling.

By following a few simple steps, you can enjoy the productivity perks of an AI meeting notetaker without putting your company (or your reputation) at risk.

Use this checklist if you're thinking of recording your meetings or want to double-check if your current AI notetaker is actually secure.



Your secure AI meeting notetaker checklist:

☐ Check that the AI notetaker doesn't train on your data

Some AI tools improve their systems by learning from customer data, but that can mean your private conversations are being fed back into their models. That's risky for sensitive information and a red flag for your IT department.

A trustworthy AI notetaker will clearly state that your meeting data is never used to train their AI. This ensures your notes, transcripts, and recordings stay private to you and your organization.

You can usually find this in the tool's security or privacy policy page, or by searching something like *"Does [Tool Name] train on your meeting data?"*.

If they don't explicitly state that they don't train on your data, assume that they do.

☐ Check for SOC 2 or ISO27001 compliance

We know these sound a little technical, but here's the simple version: SOC 2 and ISO 27001 are internationally recognized certifications that prove a company takes security seriously. They show that an AI notetaker has gone through strict audits to make sure your data is protected and handled properly.

The good news? You don't need to be an expert to check. Most companies list this on their website, or you can do a quick search like *"[Tool Name] SOC 2"* or *"[Tool Name] ISO 27001."*

For example, type *"Fellow.ai SOC 2 Compliance"* in Google Search or ChatGPT.

☐ If your meetings include personal health information (PHI), check for HIPAA compliance

HIPAA is a U.S. law that protects sensitive health information. If your meetings ever include personal health information (PHI), you'll want an AI notetaker that is HIPAA compliant. This means the company has strict safeguards in place to keep medical information private and secure. Most companies will highlight HIPAA compliance on their website, or you can do a quick search like "[Tool Name] HIPAA Compliance."

☐ Look for clear recording indicators

Recording a meeting comes with legal and ethical responsibilities. Everyone in the meeting should know when an AI notetaker is present and when recording starts. A secure AI meeting notetaker will make this obvious by giving you options such as:

- Displaying a clear message for all participants that the meeting is being recorded.
- Letting hosts send out [meeting recording disclosure emails](#) to all participants so everyone knows what to expect.
- Showing the notetaker as a clear participant in the call.

These indicators not only build trust with your team but also help you stay compliant with privacy and consent laws. If a tool makes it hard to tell when a recording is happening, or worse, records without notice, that's a red flag.

☐ Make sure you can pause and resume recordings

Sensitive topics, confidential numbers, or quick side conversations can come up unexpectedly. A secure AI notetaker gives you the option to pause recording with a single click and resume when it's safe. This way, you stay in control of what gets captured and what stays private.

If a tool doesn't offer this feature, you're stuck with an "all or nothing" recording, and that can create unnecessary risk for you and your team.

☐ Ensure redaction is possible

Sometimes confidential details slip into a conversation that shouldn't be saved. A secure AI notetaker should let you redact specific parts of the transcript, summary, recording, or action items so they're permanently removed. This feature gives you peace of mind and ensures sensitive information doesn't live on in searchable notes.

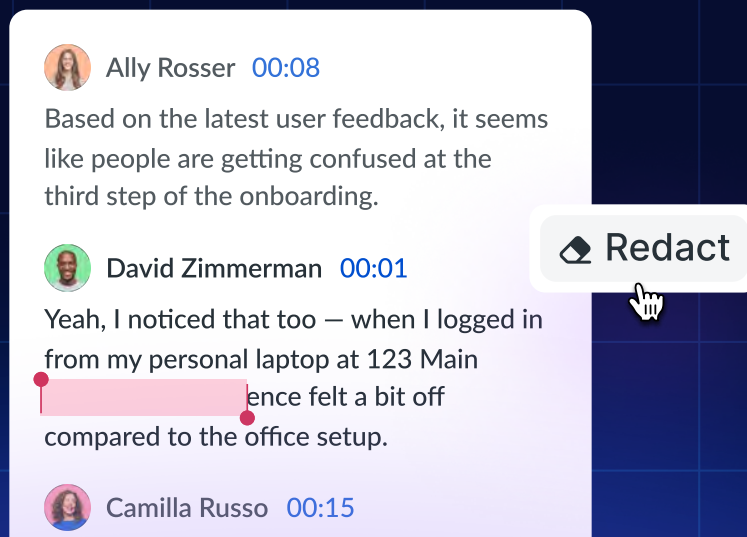
Without redaction, you're left with risky "forever records" that can be accessed or shared by mistake.

☐ Look for granular recording rules and sharing permissions

Not every meeting summary should be visible to everyone. A secure AI notetaker lets you control exactly who can access recordings, transcripts, and summaries through secure folders or channels that only certain people in the company can access.

With Recording Rules and Policies, you can also set granular meeting recording safeguards, deciding in advance which meetings can or cannot be recorded, so you stay in control of sensitive conversations across your team.

If a tool doesn't give you [access, storage, and recording controls](#), it's a sign your meeting data could end up in the wrong hands.



What if your current tool doesn't pass the test?

If you went through this checklist and noticed your AI meeting notetaker is missing key safeguards, don't panic. Here's what you can do instead:

1. Stop using it for internal conversations

Until you're certain it's secure, don't use the AI meeting notetaker in meetings where confidential company data is discussed.

2. Disable auto-join or recording features

Go to the tool's settings and make sure it can't automatically join your meetings moving forward.

3. Delete stored data

If possible, download only what you need and then delete past transcripts, recordings, or notes from the tool's platform to prevent "forever records."

4. Close or delete your account

If the tool fails on multiple safeguards, the safest option is to fully deactivate or delete your account and move to a secure alternative.

5. Get your IT team involved

Other employees might be using the same unapproved tool without realizing the risks. Your IT team can help investigate, put safeguards in place, and guide you toward a secure, company-approved alternative.



We did the research so you don't have to...



✅ All boxes checked: Fellow

We know you're already busy with your day-to-day work and responsibilities. The last thing you need is to stress over whether your AI notetaker is putting your company at risk.

If you want a secure AI meeting notetaker that checks all these boxes from the start, try [Fellow](#), the secure AI meeting assistant. Built with privacy, compliance, and user control at its core, Fellow makes your meetings more productive *and keeps your IT team happy*.