

AI GLASSES ENTER THE WORKPLACE: FAQs FOR EMPLOYERS

Insights

Mar 11, 2026

AI Glasses Enter the Workplace: FAQs For Employers

AI-enabled smart glasses – which combine eyewear with real-time audio, video, and AI functionality – are now entering the workplace. They provide productivity and accessibility benefits by allowing users to capture information, receive prompts, and interact with AI systems hands-free. But they also introduce legal risks that your existing policies and regulatory frameworks were likely not designed to address. As adoption increases, you should evaluate whether your existing workplace rules and compliance frameworks are equipped to manage the legal, privacy, and operational implications of AI-enabled eyewear. The following Insight provides answers to common questions employers are asking as AI glasses enter the workplace.

Do AI Wearables Raise Workplace Recording Concerns?

Yes – and in many cases, the risks are more significant than employers initially realize.

Unlike smartphones, AI-enabled glasses may:

- Operate hands-free and discreetly
- Record audio or video passively or continuously
- Connect automatically to cloud-based AI platforms
- Capture, analyze, and store data without obvious user action

Related People



Raeann Burgo

Partner

412.822.6630



Danielle Kays

Partner

312.260.4751

- Collect, use, and disclose biometric information

In many instances, smart glasses are indistinguishable from ordinary eyewear, making it difficult for managers or coworkers to determine whether recording is occurring. This creates enforcement challenges and potential compliance exposure if workplace communications are captured without authorization.

The risk is heightened by state recording laws, which vary across jurisdictions. Eleven states require all-party consent before conversations may be recorded. If an employee uses AI glasses to record workplace discussions without proper consent, the employer may face legal exposure, particularly where confidential internal meetings or customer-facing interactions are captured. Even if the employer did not direct or approve the recording, a lack of clear policies or enforcement protocols may complicate response efforts and increase litigation risk.

Do Restrictions on AI Glasses Raise NLRA Concerns?

Not necessarily.

Section 7 of the National Labor Relations Act (NLRA) protects employees' rights to engage in concerted activity concerning wages, hours, and working conditions. AI smart glasses, by their nature, typically include the ability to record audio and video, take photographs, and sometimes even stream content in real time. These functions may be analogous to those found in cell phones and other electronic devices previously considered by the National Labor Relations Board (NLRB).

In certain circumstances, recording workplace conditions may qualify as protected activity. This is particularly true where the recording documents safety concerns, harassment, discrimination, or union-related activity, and is undertaken to further a group interest, such as preserving evidence for collective action.

The [NLRB 2023 Stericycle standard](#) remains in effect despite [recent guidance from the Board's General Counsel](#), and it means that labor officials will scrutinize even facially neutral workplace policies that prohibit recording in the workplace. The current standard says that workplace rules are presumptively unlawful if a reasonable employee could interpret them as chilling protected concerted activity under



Chelsea Viola

Associate

213.403.9626

Service Focus

AI, Data, and Analytics

Labor Relations

Privacy and Cyber

Resource Hubs

AI Governance Hub

Section 7 of the NLRA. To overcome this presumption, employers have to demonstrate that the rule is narrowly tailored to address a legitimate and substantial business interest such as trade secrets, confidentiality, or customer privacy,

With this in mind, employers should review their policies governing AI glasses to ensure they are narrowly tailored and clearly tied to legitimate business justifications so as not to infringe on employees' Section 7 rights.

Do AI Glasses Create Data Security Risks?

Quite possibly. Data security risks associated with AI-enabled wearables could be significant and, in some cases, difficult to detect.

AI-enabled glasses could capture proprietary processes, trade secrets, internal communications, and customer or patient data. Since these devices often connect to third-party AI platforms, information may be transmitted, stored, or processed outside the employer's direct control.

Once data leaves the organization's internal systems, questions arise regarding retention practices, secondary use, security safeguards, and regulatory compliance. Employers may have limited visibility into how that information is handled, which can create exposure under confidentiality agreements, trade secret laws, and applicable privacy statutes.

Organizations in regulated industries, including healthcare and financial services, should be especially cautious. The inadvertent capture or transmission of protected or confidential information through wearable AI devices may implicate industry-specific privacy and security obligations.

How Do Disability Accommodation Obligations Apply to AI Glasses?

Many AI glasses are designed to look and function like ordinary eyewear and may even contain prescription lenses. While the glasses themselves may provide vision correction, the AI functionality embedded within the device is a separate consideration.

At present, ordinary prescription eyewear does not constitute a disability under the Americans with Disabilities Act (ADA), and employers are not required to permit AI-

enabled glasses simply because they include corrective lenses. In other words, presence of prescription lenses does not, by itself, transform the device into a protected accommodation.

However, this may change since wearable AI glasses can function as assistive technology. Emerging AI glasses now can provide real-time transcription, object recognition, navigation assistance, visual magnification, which may be in the future considered workplace accommodations for individuals with visual, auditory, or neurological impairments. As the technology continues to evolve, employers may consider conducting a case-by-case assessment if you identify the possible need or request for an accommodation. This may include evaluating whether the device is medically necessary, whether it addresses a documented limitation, whether there are alternative accommodations available, and whether the use of AI glasses presents safety, confidentiality, or operational concerns.

Can Employers Prohibit AI Glasses in the Workplace?

In most cases, yes.

Employers generally may restrict or prohibit AI-enabled glasses and other wearable devices where the policy supports legitimate business interests. Common justifications include maintaining workplace safety, protecting confidential or proprietary information, safeguarding customer, employee, or patient privacy, and ensuring compliance with applicable recording and data privacy laws.

If an employer decides to implement a ban, consistent enforcement is essential. Any uneven application of the policy may give rise to disparate treatment or retaliation claims.

What Steps Should Employers Take Now?

Given these new slate of risks, we recommend you consider the following steps.

1. Review and Consider Updating Applicable Policies

- Audit electronic device, recording, confidentiality, and acceptable use policies to determine whether they

expressly encompass AI-enabled glasses and other recording-capable wearables

- Identify outdated language that references only “phones” or “cameras” or broadly prohibits “unauthorized recording.”
- Revise policies to clearly define the scope of covered devices to include wearable AI technology and ensure that legitimate business justifications for such restrictions are articulated.

2. Consider Building an Accommodation Framework That Considers AI Glasses

- Ensure workplace policies allow for case-by-case assessment where an employee asserts that AI glasses are medically necessary as a reasonable accommodation.
- Establish a clear internal process for engaging in the interactive process, including evaluating medical documentation, identifying the specific limitation at issue, and determining whether the device enables the employee to perform essential job functions.
- Document the analysis and decision-making process to support defensibility in the event of future challenges.

3. Train Managers on AI Glasses and How to Deal With Them

- Ensure supervisors understand what AI-enabled glasses are, how they function, and how to identify potential recording, safety, or confidentiality concerns.
- Provide guidance on how to respond if a manager observes an employee wearing AI glasses, including when to escalate issues to HR, compliance, or legal.
- Train relevant stakeholders on how to handle accommodation requests appropriately and avoid making unilateral decisions that could create ADA or retaliation risk.

4. Consult Experienced Legal Counsel

- Engage workplace counsel, like your Fisher Phillips attorney, that understands the intersection of data

privacy, cybersecurity, workplace safety, labor law, and disability accommodation to evaluate and mitigate risks associated with AI glasses in the workplace.

Conclusion

We will continue to monitor developments related to AI wearable technology. Make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information. If you have questions about your organization's use of AI in recruiting or hiring, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our [AI, Data, and Analytics Practice Group](#) or our [Privacy and Cyber Practice Group](#).