An Employer's 5-Step Guide to AI Interviewing and Hiring Tools

Insights
1.30.26

AI-enabled interviewing tools have emerged as a common solution for the administrative burdens associated with hiring. These tools improve efficiency, streamline operations, allow you to consider more candidates without expanding your hiring team, keep evaluations consistent across applicants, and make high-volume hiring easier. But their adoption also raises important legal considerations, including potential bias, compliance risks, and data privacy and cybersecurity obligations – all while we face a growing regulatory and litigation landscape targeting the use of these tools. This Insight reviews the most common tools being deployed by employers and their associated risks, and provides a five-step suggested plan for minimizing liability.

AI Interviews Tools and Systems

Rather than solely focusing on tools that assist with logistics or document review (like simple schedulers or resume screeners), the newest generation of AI hiring tools can analyze and organize interview responses in ways that can directly shape hiring decisions.

- **Transcription and summarization tools.** These tools convert spoken interview responses into written text using speech recognition technology, making interviews easier to review, search, and compare across candidates. Many platforms also generate summaries, highlights, or structured interview notes to support recruiter review.
- **Interview analysis and evaluation tools.** These systems analyze recorded interview responses to assess factors such as speech patterns, tone, pacing, word choice, facial expressions, and other nonverbal cues. Some tools incorporate emotion or sentiment analysis or natural language understanding to evaluate both how candidates communicate and the substance of their responses, and may produce scores, rankings, or qualitative insights to support early-stage screening.
- **Adaptive or dynamic interview systems.** These tools adjust interview questions in real time or across interview stages based on a candidate's prior responses. The goal is to probe specific competencies, behaviors, or skills more deeply by tailoring follow-up questions rather than relying on a fixed interview script.
- **Behavioral, personality, and multimodal assessment tools.** Certain AI interview platforms attempt to infer behavioral tendencies or personality traits by combining data from audio, video, and text responses. These multimodal systems may draw on behavioral frameworks to assess

characteristics such as communication style, adaptability, or collaboration, and may tailor evaluations to competencies associated with a specific role.

- **Skills and assessment platforms.** These tools use simulations, technical challenges, situational judgment tests, or role-specific exercises to evaluate how candidates perform job-related tasks, often producing standardized results that allow for comparison across applicants.
- **Video interview platforms.** These platforms support live or asynchronous video interviews and often serve as the foundation for other AI-driven features. In addition to hosting interviews, they may integrate automated screening, adaptive questioning, communication analysis, and structured candidate summaries to support early interview stages and recruiter review.

Legal, Ethical, and Organizational Risks Associated with AI Interview Tools

As with other AI systems, AI interviewers are shaped by the data used to design and develop them, which can give rise to legal, ethical, and organizational risks similar to those associated with other AI tools. These issues are further heightened by the collection and analysis of sensitive data, such as biometric identifiers, behavioral patterns, and other personal signals generated during AI interviews.

- **Race and Disability Bias.** Candidates with disabilities may claim to be disadvantaged when their communication or behavior differs from the patterns these systems are trained to recognize as indicators of qualification. For example, a pending discrimination complaint filed by the ACLU with the Colorado Civil Rights Division and the EEOC highlights these concerns, alleging that an employer's use of AI interview tools adversely affected a deaf, Indigenous employee. The complaint asserted that automated speech recognition features misinterpreted or inaccurately evaluated her communication style, particularly in ways that may disadvantage non-white or accented speakers.
- **State Data Privacy.** AI interviewers can collect and process a significant amount of sensitive data, including video and audio recordings, behavioral signals, and, in some cases, biometric identifiers derived from facial or voice analysis. While the state data privacy law landscape continues to expand, we'll face increased instances of plaintiffs and regulators alleging that the use of AI hiring tools run afoul of state law. As a result, organizations must individually determine how interview data is handled across its life cycle, including how it is used, whether it is retained or repurposed beyond the initial hiring decision, and the extent to which it may be shared with or reused by technology vendors to improve or train AI systems.
- **Organizational Security and Deepfakes.** Another potential pitfall is the challenge AI interview tools face when encountering deepfakes, which involve the use of synthetic or manipulated video, audio, or real-time AI-generated content to alter or replace a person's appearance, voice, or responses. In these situations, AI systems may analyze fabricated signals rather than authentic candidate behavior, particularly in asynchronous interviews where live verification is limited.

- **Vendor Liability.** Organizations may face legal and compliance exposure based on the design and operation of third-party AI interview tools, even when the underlying technology is developed and managed by a vendor. In a 2023 enforcement action, *EEOC v. iTutorGroup Inc.*, the EEOC challenged an employer's use of automated recruiting software that screened out applicants based on age, resulting in a settlement and remedial obligations under federal anti-discrimination laws. Although that particular enforcement action did not involve AI interviewers, it highlights a similar. Employers remain responsible for how AI interviewer tools and systems function and the outcomes they produce, even when the technology is designed and operated by a third party.
- **Reputational and Trust Risks Associated with Applicant AI Use.** The use of AI interview tools is not only limited to employers; organizations are now confronted with how to address applicants' use of AI during the interview process. Applicant-facing AI tools, such as interview coaching, response assistance, or real-time prompting technologies, are often seen as "cheating," leading some organizations to outright ban their use on the applicant side. Restricting applicant AI use while employers rely on AI interviewers to evaluate candidates has, in some cases, led to negative perceptions of employers and raised questions about fairness. This is particularly important for employers to keep in mind, as interviews are traditionally viewed as a two-way assessment, where not only employers assess potential candidates, but candidates also assess their potential employers.

5 Steps You Can Take to Mitigate Risks

If your organization uses or is considering AI interview tools, the following five steps can help proactively manage risk.

1. Develop Comprehensive AI Policies. While many organizations rely on a single, high-level AI policy, a more effective governance framework typically includes multiple, complementary policies tailored to different aspects of AI use. At a minimum, you should establish a comprehensive program to address three areas: organizational AI governance, ethical use of AI, and tool-specific acceptable use policies. If you are not sure where to begin, our *AI Governance 101 Guide provides* a helpful starting point and can be found here.

2. Ensure Ongoing Vendor Oversight. You should treat AI interview vendors as an extension of the hiring process rather than as standalone technology providers. Managing risk requires clear contractual guardrails, transparency into how tools function, and ongoing monitoring to ensure compliance and fairness. For guidance on key considerations to consider during your vendor selection process, review our *AI Vendor Resource* here.

3. Adopt Measures to Identity and Prevent Deepfakes. Adopting identity verification measures for candidates, particularly in asynchronous interviews, and establishing review protocols to flag irregular or suspicious interview behavior can help mitigate the use of deepfakes. For video interviews in particular, you should implement tools that support human review and train

employees to recognize indicators of manipulated or synthetic content. For guidance about practical steps to take, review our *Hiring with Confidence in the AI Era Insight* here.

4. Audit AI Interview Tools and Systems. You should regularly audit AI interview tools to assess whether they rely on signals such as speech patterns, accents, tone, facial expressions, or eye contact, and limit or disable features that may disadvantage candidates with disabilities, neurodivergent traits, or culturally distinct communication styles. You should also ensure that alternative interview formats are available to help prevent qualified candidates from being screened out based on how AI systems interpret communication rather than job-related qualifications. FP has partnered with analytics firm BLDS and AI fairness software provider SolasAI to deliver an integrated suite of bias audit services – learn more here.

5. Establish Clear and Balanced Policies on Applicant AI Use. Your approach to applicant use of AI during interviews can present reputational risk if perceived as inconsistent, overly restrictive, or misaligned with the employer's own use of AI tools. Prohibiting applicant AI use while deploying AI interviewers may be viewed as a double standard, potentially affecting employer brand, candidate trust, and overall recruitment outcomes. Accordingly, you should address applicant use of AI during interviews through transparent, balanced policies rather than blanket prohibitions. This includes clearly communicating what types of AI use are acceptable, such as accessibility tools or interview preparation support, and what uses are not permitted, such as real-time response generation intended to misrepresent a candidate's abilities.

Conclusion

Fisher Phillips' AI Team provides end-to-end solutions for employers to help them adapt, develop practical solutions, and mitigate risk. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group. We will continue to provide the most up-to-date information on AI-related developments, so make sure you are subscribed to Fisher Phillips' Insight System.

Related People

Vivian Isaboke, CIPP/US, CIPM
Associate
908.516.1028
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

AI, Data, and Analytics

Employment Discrimination and Harassment

Counseling and Advice