



HR Meets AI: Friend, Foe or Lawsuit?



Kimberly J. Korando
November 5, 2025

EXPECT EXCELLENCE®

Things AI can do for HR



Recruiting and Selection

- Recruiting, resume screening, candidate sourcing, matching
- Test candidate aptitude and cognitive ability
- Conduct interviews

Employee Support and Service

- Virtual assistants (chatbots): hiring and onboarding new employees, employee support & service to answer frequently asked questions
- Learning/development/coaching: personalized learning recommendations, content generation, coaching aids, plan employee career paths, succession planning

Operational

- Monitoring employee productivity
- Improving employee productivity using GenAI

HR Must Understand What and How the AI Tool Makes Assessments

If the AI tool determines the factors and their weights, obtain the following information from the vendor **in writing**:

1. Description of each factor and its assigned weight.
 2. Is the weight assigned by the vendor, the company, or the AI tool itself?
 3. Are the factors and the weights disclosed to the user?
 4. Does the AI tool identify the inputs or fields, or does a human determine them?
5. Is the company allowed to remove a factor or change a factor's assigned weight or otherwise modify the algorithm?
6. How often does the algorithm change? Does it change automatically?
 7. Does the algorithm improve over time?
 8. Does the vendor notify the company of any changes and the reasons for the changes?

Compliance Pitfalls and Bias Concerns

Compliance Pitfalls

Failure to Meet Legal Standards
(employment, AI, data privacy and security)

Insufficient Transparency

Neglecting Human Oversight

Vendor Reliance Without Due Diligence

Bias Concerns

Biased Training Data

Proxy Discrimination

Accessibility

Algorithmic Drift

Compliance Pitfalls

Failure to Meet Legal Standards

Federal employment: Title VII, ADA, ADEA still apply. If AI screens out protected classes disproportionately, employer, not vendor, is liable.

State and local laws governing AI, include:

- Illinois Artificial Intelligence Video Interview Act: Notice, consent, and other requirements for video interviews using AI
- Maryland Facial Recognition Law: Restricts facial recognition and other biometric information in the employment application process
- New York City Automated Employment Decision Tool (AEDT) Law: Prohibits use of AEDT in hiring or promotion decisions unless the tool has been the subject of an independent audit, a summary of the audit results is publicly available, and employer provides advance notice to employees or applicants about the tool's use
- California: Civil Rights Division approved regulations regarding discrimination as a result of the use of AI (eff. Oct. 1, 2025); Automated Decision-Making Technology regulation (proposed): Pre-use notice, privacy disclosures, risk assessment requirements, opt-out notices, vendor contract requirements, functionality and discrimination provisions
- Colorado Senate Bill 24-205 (eff. February 1, 2026): Implements regulation for use of AI in employment
- Texas HB 149 (eff. January 1, 2026): Prohibits development or implementation of AI that intentionally discriminates on the basis of a protected characteristic and eliminates disparate impact as a recognized cause of action
- Utah AI consumer protection requirements (Utah Code § 13-32-12) and the Utah AI policy Act (Utah Code § 13-72-101 to 13-72-305; Utah Admin. Code R166-72-1 to R166-72-7): May impact employer use of AI

Data Privacy and Security laws: Collecting and processing personal data through AI systems may run afoul of data protection laws (GDPR, CCPA, state privacy statutes) if proper safeguards and disclosures are not in place.

Failure to Meet Legal Standards (cont'd)

TIPS

- 
- 1 Keep updated on the expanding state and local laws on use of AI
 - 2 AI tools must be designed, selected, and monitored to prevent discrimination or disparate impact on the basis of protected characteristics (e.g., race, color, sex, national origin, religion, age, disability, or other status protected by law)
 - 3 Obtain bias audits and fairness testing reports before deployment and, after deployment, conduct them at least annually under an attorney-client privilege
 - 4 Obtain EPLI coverage for AI-related risks
 - 5 Configure application process to require execution of an arbitration provision with class action waiver

Insufficient Transparency

AI systems operate as “black boxes,” making it difficult to explain why a candidate was rejected or chosen.

Lack of explainability can violate legal requirements for providing reasons for employment decisions.

TIPS

Provide notice when an AI tool is used to evaluate or assist making employment decisions:

- Purpose of the tool and type of data analyzed
- How outputs are used
- Rights to request human review or appeal

Maintain documentation of all AI tools used, how it is used, what data it processed and how the employment decision is made

Neglecting Human Oversight

Overreliance on AI without meaningful human review may lead to unlawful outcomes, especially if the tool makes errors that go unchecked.

TIPS

- AI is a tool, not a decision-maker
- Use AI to assist, not replace, human judgement
- Keep a human-in-the-loop (a qualified person) for review and approval of all employment decisions before action is taken

Vendor Reliance Without Due Diligence

Employers may assume third-party AI tools are compliant, but liability typically falls on the employer.

Due diligence, audits, and contracts must explicitly address compliance responsibilities.

TIPS

- Don't trust, verify
- Require vendors to provide documentation of bias audits, validation studies, and explainability reports
- Require contractual obligations for compliance and cooperation with audits
- Use the AI Vendor Due Diligence Checklist

Bias Concerns

Bias Concerns



Biased
Training Data

Proxy
Discrimination

Accessibility

Algorithmic
Drift

Biased Training Data



If historical hiring data used to train AI reflects discrimination, AI will replicate and even amplify those patterns.

Tips:

Ensure the tool has undergone a bias audit and obtain a full copy of the report from the vendor

Proxy Discrimination

AI may use neutral-seeming factors (e.g, zip code, college, or employment gaps) that act as proxies for protected characteristics, leading to disparate impact.

AI may seek to remove bias by omitting protected-class data (e.g., gender or race), but algorithm relies on indirect indicators of those traits.

Tips:

Review AI tool outputs for disparate impact, accuracy, and reliability annually under an attorney-client privilege

Algorithmic Drift

Over time, AI models can “drift” and evolve in ways that create new unintended biases, requiring ongoing monitoring and revalidation.

Tips:

Review AI tool outputs for disparate impact, accuracy, and reliability annually under an attorney-client privilege

If disparate impact or other issues are identified, suspend use until corrective actions can be evaluated

Accessibility

AI-driven assessments (e.g., gamified testing or voice analysis) may disadvantage people with disabilities, non-native speakers, or those from underrepresented groups.

Tips:

Determine the disability accommodation and accessibility options available from the vendor by asking:

Is the tool compliant with the most current version of the Web Content Accessibility Guidelines (WCAG) at the highest levels? Require documentation verifying this representation.

What accommodations can the tool make for individuals who have:

- Visual impairments?
- Hearing impairments?
- Physical impairments?
- Cognitive or seizure impairments?

What processes are available for applicants and employees to request disability accommodations? How are individuals notified of these processes?

Who determines whether accommodation requests should be granted?

AI Vendor Due Diligence Checklist

AI Vendor Due Diligence Checklist



Audit History

Litigation
History

AI Tool
Validity Study

Job Analysis

Vendor's Data
Processing
and Storage

Biometric
Privacy
Implications

AI Vendor Due Diligence Checklist

Audit History

Has a bias audit been done on the tool?

- When last performed, who conducted it (independent third party), will vendor provide a full copy of the bias audit report?

As part of the bias audit or otherwise, have selection rates, scorings and impact ratios been assessed by sex (male or female) and race/ethnicity?

If so:

- Was actual or sample data used for the assessments?
- Will the vendor share the selection rates, scoring rates, and impact ratios?

Will the vendor assist the company or an independent third-party auditor (or both) to perform a bias audit before launch and on an ongoing basis?

AI Vendor Due Diligence Checklist (cont'd)



Litigation History

Has the vendor or the AI tool been subject to litigation or administrative charges?

- If so, when, what were the claims, and what is the status of the litigation or charges?

What assistance does the vendor provide to defend discrimination claims or indemnify the company against legal claims?

Can the company access the algorithm or underlying data if necessary to defend against a legal dispute, such as before the EEOC, the OFCCP, or a state or local administrative agency, or in federal or state court litigation?

AI Vendor Due Diligence Checklist (cont'd)

AI Tool Validity Study

Has the vendor validated or otherwise tested the algorithm to determine whether accurate inferences can be made from the results for the company's intended use?

- If so, when was the last time it did so, how often does it do so, who performs the validity study?

Obtain written description of the validation methodology.

How does the vendor conclude whether the results reveal cause for concern about any potential bias?

Is there a potential for false positives?

Does the vendor exercise any bias mitigation efforts in creating the model or monitor the algorithm to ensure that it is performing as intended and accurately?

- If so, obtain a description of the efforts and/or monitoring.

AI Vendor Due Diligence Checklist (con't)

Job Analysis

Does the vendor conduct a job analysis in connection with the tool?

If so:

- How does the vendor to analyze the jobs for which the company is hiring or managing?
- What resources and information does the vendor need from the company to conduct a job analysis?
- Who conducts the job analysis? What are their qualifications?

AI Vendor Due Diligence Checklist (cont'd)

Vendor's Data Processing and Storage

How and where is the data recorded?

What precautions are taken to safeguard data?

For how long is the company's data stored?

Will the vendor modify retention dates:

- as individuals' status change from applicants to employees?
- to reflect requirements in federal, state, or local law or regulation?
- if notified that relevant data is subject to a litigation hold notice?

Does the vendor archive or maintain records showing when it altered an algorithm?

What is the vendor's process for anonymizing individuals' information?

What are the algorithm's data-searching capabilities?

Can the vendor export its information into a spreadsheet aggregating candidate information? If not, at a minimum, can the vendor permit separate access to each candidate's information?

AI Vendor Due Diligence Checklist (cont'd)

Biometric Privacy Implications

Does the tool collect any biometric identifiers (e.g., voiceprints or other unique biological patterns or characteristics used to identify a specific individual)?

If so:

- Does it provide notice about the biometric identifiers being collected, and what steps it is taking to protect the privacy of the information?
- How does it get the individual's consent to collect the biometric identifiers?
- How is the biometric information used? Stored? How and when is it destroyed?
- What steps are taken to safeguard the biometric information?
- Do these procedures comply with applicable biometric privacy laws (e.g., requirements regarding notice, collection, use, storage, and destruction)?

FOE?

AI Deep Fakes and Job Seeker Cheats



4Q24 Gartner survey of 3,290 job candidates: 4 in 10 candidates admitted using AI during the application process to generate text for:

- Résumé/CV (54%)
- Cover letter (50%)
- Writing sample (36%)
- Answers to assessment questions (29%)

2Q25 Gartner survey of 3,000 job candidates: 6% admitted to participating in interview fraud – either posing as someone else or having someone else pose as them in an interview.

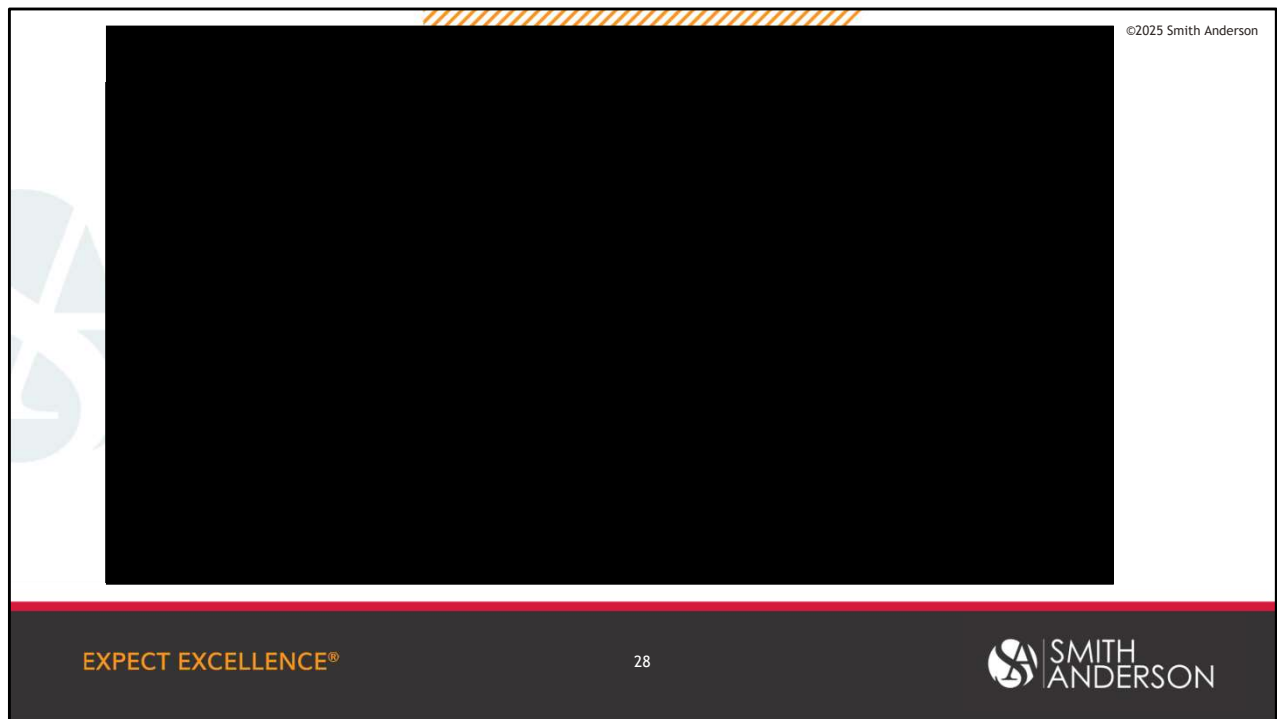
Gartner predicts that by 2028, one in four candidate profiles worldwide will be fake.

Gartner, Inc. NYSE: IT

Other Means of Deceit



- Deep Fake videos
- Voice manipulation
- Fabricated resumes
- Real-time AI assistants to answer technical questions



CBS Morning, How scammers are using AI to create fake job applicants, June 16, 2025

Red Flags



Interviews and
Virtual
Connections

Social Media
Profiles and
Resume

Background
Check

New Employee

Technical

Red Flags—Social Media Profiles and Resume



- Biographical information does not appear to match candidate
- Sparse social media profiles
- Newly created LinkedIn profile or one that doesn't match experience
- No LinkedIn photo, stock AI image or stock photo
- LinkedIn profile no longer available or links to a different person
- Virtual or VOIP phone number
- Near perfect resume with every skill for job
- Multiple location education/work histories
- Inconsistencies in location, employment and education history
- Multiple emails, different names, misspelled name

D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Red Flags—Interviews and Virtual Connections



- Sounds scripted, reading answers
- Unusual communication patterns or interaction
- Robotic difficulty answering questions about city they live in, zip code
- Candidate asks for questions to be repeated multiple times
- Only gives high level answers to questions without details
- Does not ask questions about the company or role
- Goes on/off camera or does not turn camera on
- Uses virtual background
- Connection problems
- Wears headphones

D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Red Flags—Background Check



D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Red Flags—New Employee

New employee looks different than interviewee

Does not work on camera

No show to in-person events

Time of day in background does not match location

Lots of “people noise” in the background

D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Red Flags—Technical

Foreign IP address

Non-sanctioned VPN use

Request for different type of device (Mac v. Windows)

Request for/use of remote access tools (e.g., AnyDesk, Jump Desktop Connect)

Request for/use of tools to prevent laptop from sleeping

Immediate change of address after hire

Laptop's physical location does not match employee's stated location

D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Prevention Tips

Virtual interviews

- Request candidate to hold up photo ID in front of face
- Do not allow candidate to be off-camera
- Do not allow candidate to wear headphones/earbuds
- Ask candidates for details about the cities in which they have lived and projects on which they have worked

IT/Security

- Use strong identity and access management controls
- Use enhanced monitoring and logging for remote IT worker activities
- Maintain log of all network activities
- Lock down USB, restrict use of keyboard/video/mouse switches
- Use endpoint detection and response (EDR) software to detect Remote Desktop Protocol (RDP) and VPN use or logins from multiple locations in a short time
- Retain ability to track laptop location and keep record of shipping addresses

In-person Interactions

In-person Interview
In-person I-9 verification
In-person on-boarding
In-person attendance at a company event (confirm person who attends matches the photos of the interviewee)

Onboarding

Ensure name on direct deposit account matches employee name

D. Drummond, N. Glasser, E. Sullivan, D. Walton, The Imposter Problem: Deep Fake Employees in the World of AI and Remote Work (Oct. 14, 2025)

Final Thoughts Recap

- Identify and inventory currently used technology tools used to make employment decisions
- Stay current with federal and state AI-related employment laws
- Obtain/ensure that EPLI covers AI risk
- Conduct due diligence on AI tools before purchasing; require bias audits or fairness testing from vendors; purchase/license agreement should be reviewed by legal counsel for appropriate representations, warranties, indemnification
- Obtain employee/candidate consent when required and provide a clear explanation of how AI will be used
- Require qualified human review (trained to identify and respond to AI flags) of AI-generated outputs before final decisions are made
- Conduct adverse impact and other assessments of AI tool at least annually under attorney-client privilege
- Keep vigilant for fake candidates and cheaters



HR Meets AI: Friend, Foe or Lawsuit?



Kimberly J. Korando
November 5, 2025

EXPECT EXCELLENCE®