DMEC

POLICY BRIEF

Artificial Intelligence in Workplace Leave and Accommodation Management

Artificial Intelligence in Workplace Leave and Accommodation Management

Artificial intelligence (AI) is a collective term used to describe machine-based technologies that can, when given a set of objectives, generate outputs such as predictions, recommendations, or decisions with applicability in real or virtual environments. In essence, AI performs tasks previously only possible with human intelligence, and it has significant implications across society, including the workplace.

In the context of workplace leave and accommodation management, employers are increasingly adopting AI-driven tools to provide customized training to employees, assess benefits eligibility, support claims management, flag compliance concerns, verify medical information, facilitate accommodations, and predict leave periods or absenteeism trends. While AI tools can optimize these operations, they also carry risks for both individuals and organizations. For example, automated leave denials without explanation can create confusion or lead to legal disputes if employees don't understand the rationale behind decisions. Further, because AI-based leave systems are more likely to utilize a third-party vendor, breaches in security or unauthorized use of sensitive data can risk employee privacy.

Policymakers can play a role in protecting constituent interests when it comes to AI and workplace leave and accommodation management by providing companies using AI with guardrails that ensure privacy, prevent bias, promote transparency, set consistent standards, and encourage responsible innovation. Policymakers can also guide how AI is used by the state. States may want to consider policy options related to the following areas:

- **AI Governance at the State Level:** Create an AI Governance Committee to oversee ethical use, conduct impact assessments, and guide policy development related to AI.
- **Guidelines for Responsible, Ethical, and Transparent AI Use:** Direct developers and deployers of AI systems to act in compliance with ethical AI standards.
- **Consumer Protections for Algorithmic Bias and Discrimination:** Apply algorithmic fairness and anti-discrimination policies to AI in high-risk systems such as benefits, health care, and employment.
- **Human Oversight of Employment-Related Decisions:** Require periodic human review of decisions generated by AI systems.
- **Disclosure of AI Use:** Require disclosure to individuals regarding the use of AI in employment contexts, including its function in decision-making and data collected.
- **Data Security Requirements:** Set standards to ensure data utilized for and input into high-risk systems is minimal, protected, and only used for articulated purposes.

AI Governance at the State Level

According to the National Conference of State Legislatures, state legislators considered more than 150 bills relating to government use of AI during the 2024 legislative session. Topics included inventories to track the use of AI, impact assessments, AI use guidelines, procurement standards, and government oversight bodies. Additionally, governors in more than 10 states, including Alabama, Maryland, Massachusetts, Oklahoma, Oregon and Washington, D.C., issued executive orders to study AI use in running government operations and providing government services and benefits.

While many states are considering regulations around the use of AI in topics tangential to leave and accommodation management (ex. data security, transparency, bias, and algorithmic discrimination, etc.) a 2025 DMEC study found that little to no guidance or regulation exists around the use of AI in HR, benefits and leave administration, and claims processing. State policymakers can create governance structures or committees to oversee ethical use, conduct impact assessments, and guide policy development related to AI in workforce and leave systems.

While the policies below do not specifically focus on leave management, opportunity exists to include individuals, experts, or employers who can speak to the importance of providing guardrails to its use in workplace leave and accommodation management.

Examples in Action:

Delaware HB 333 (2024) created the Delaware AI Commission. This commission was tasked with making recommendations to the General Assembly and Department of Technology and Information on AI utilization and safety within the State of Delaware. The bill also tasked the commission with creating an inventory of all Generative AI usage within Delaware's executive, legislative, and judicial agencies and identifying high risk areas for the implementation of Generative AI.

Maryland SB 818 (2024) established a Governor's AI Subcabinet to strengthen coordination across state agencies and promote collaboration with academic institutions and AI-driven industries. The Subcabinet is responsible for developing statewide strategies, policies, and oversight mechanisms to guide the responsible and effective use of AI and related data.

New Jersey AB 4888 (2025) established a commission dedicated to studying the impact of AI on the labor market. This commission will analyze both the potential threats and opportunities that AI presents, with a particular focus on job displacement and the emergence of new roles.

Utah established a first-in-the-nation Office for AI Policy, Regulation & Innovation. The office consults with businesses, academic institutions, and other stakeholders to facilitate dialogue on regulatory proposals to foster innovation and safeguard public safety.

Establishing Guidelines for Responsible, Ethical, and Transparent AI Use

As states establish AI commissions or agencies to guide the roll out of AI in their communities, they may consider establishing or adopting AI guardrails or ethics principles. Ethical AI principles can include accountability, non-discrimination, human agency and oversight, privacy and data governance, technical robustness and safety, transparency, and social and environmental well-being. A well-designed framework will reflect state values, build constituent trust, prevent unintended harm, guide decision-making, and ensure accountability. AI guardrails can also ensure that the use of AI to manage leave or benefits administration complies with relevant regulations, such as the Americans with Disabilities Act, the Health Insurance Portability and Accountability Act, and the Family and Medical Leave Act, among others.

States may also want to consider defining the concept of high-risk systems and adopting more stringent regulations on AI applications use within them. Such regulations can allow for flexibility and innovation while also ensuring protections around systems that may significantly affect people's health, safety, or fundamental rights; affect areas like employment, education, law enforcement, or access to public services; or operate without full human oversight, especially when profiling individuals or automating decisions.

There are numerous examples and templates states can use, for example:

EU AI Act

Proposal for a

Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

2021/0106 (COD)

European
Commission

→ The EU Artificial Intelligence Act and AI Ethics Guidelines

→ National Institute of Science and Technology AI Risk Management Framework

→ Organization for Economic Co-operation and Development AI Principles

→ United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of Artificial Intelligence

Regardless of formal policies set by the state, for the purposes of managing risk around AI in workplace leave and accommodation management, states may want to consider the following principles:

→ Ensure AI models have comprehensive and complete documentation that is available for review and inspection;

→ Require audits and validation for bias, unintended consequences, and correctness for all outcomes from generative and high-risk (those affecting health, safety, or civil rights) AI systems; and

→ Ensure the use of generative AI and high-risk AI systems is accountable and explainable.

Examples in Action:

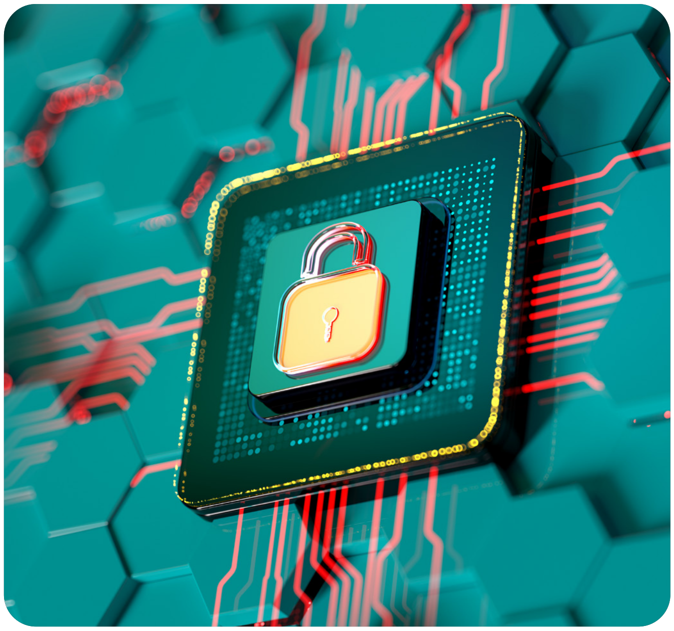
California AB 2013 (2024) mandates that by January 1, 2026, AI developers must post documentation on their websites regarding the data used to train AI systems before each release or substantial modification. This documentation should include a high-level summary of datasets, their sources, the number of data points, and any presence of copyrighted or personal information.

Delaware HJR 7 (2025) directs the state AI Commission to collaborate with the Secretary of State to create a regulatory sandbox framework for testing innovative technologies that utilize agentic AI.

Texas SB 1964 (2025) outlines amendments to the Government Code of Texas concerning the regulation and use of AI systems by governmental entities. It mandates state agencies inventory their AI systems, particularly those classified as heightened scrutiny, and assess their impact on public services. Local governments are also required to review their use of such systems and report findings to the relevant department. It also introduces a new code of ethics for AI systems, which aligns with the National Institute of Standards and Technology’s AI Risk Management Framework.

Though ultimately vetoed, the 2025 **Virginia** High-Risk AI Developer and Deployer Act (HB 2094) defined high-risk AI system, algorithmic discrimination, and generative AI, among other critical components of AI implementation.

Consumer Protections for Algorithmic Bias and Discrimination



Algorithmic bias refers to systematic and repeatable errors in a computer system that create unfair outcomes, often benefiting one group over another. These biases can stem from various factors, including biased or incomplete training data, flawed assumptions in algorithm design, bias reflecting values of those designing the program, or reliance on data that may not represent individuals from varying backgrounds.

Courts and agencies in the United States have already recognized that algorithms with discriminatory effects are subject to existing civil rights and employment laws. Still, stronger and clearer safeguards are needed. Without principled rules and oversight, automated systems may wrongly deny leave or benefits, deepen inequities, and erode trust. By establishing clear standards for fairness in algorithmic tools, policymakers can protect workers' rights while ensuring technology is used responsibly. States that already have rules on algorithmic fairness or anti-discrimination in AI should ensure that these protections extend to high-risk systems, such as public benefits, health care, employment and retention.

Examples in Action:

California Governor Newsom issued Executive Order 12 (2023), which tasked the Government Operations Agency, California Department of Technology, California Department of Human Resources, and Labor and Workforce Development Agency with providing trainings for state government worker use of state-approved generative AI (GenAI) tools to achieve equitable outcomes, and to identity and mitigate potential output inaccuracies, fabricated text, hallucinations, and biases, while enforcing public privacy and applicable state laws and policies.

Human Oversight of Employment-Related Decisions

Addressing bias is only part of the equation; robust oversight mechanisms are essential to ensure accountability and safeguard against unintended harm for both employer and employee. Human auditing of AI systems can watch for and rectify potential biases and mitigate unfair discrimination based on demographic factors. This oversight can also take external factors into account and infuse empathy and flexibility as needed. Moreover, it can provide accountability for the choices made by AI, allowing for appeals, intervention, and remediation when necessary.

While constant oversight of AI systems may not be possible or practical, policymakers can encourage employers to provide for periodic human review of decisions generated by AI systems, require review of contested employment and leave-related outcomes, and establish clear processes for challenging those decisions. Annual audits can further safeguard against systemic bias and reinforce trust in AI-driven systems. While the policies below do not specifically focus on leave management, states have embedded human oversight processes into AI systems broadly.

Examples in Action:

Kentucky enacted SB 4 (2025) establishes an AI Governance Committee tasked with developing policy standards and technology protocols to protect data privacy and mitigate risks associated with AI applications. Key provisions of the bill include the requirement for transparency in AI decision-making processes, where entities must disclose the use of AI and the extent of human oversight. High-risk AI systems must adhere to risk management policies that identify and mitigate potential biases.

Montana HB 178 (2025) seeks to restrict the use of AI systems by state and local government entities. It specifically prohibits the use of AI for cognitive behavioral manipulation, classifying individuals in ways that could lead to discrimination, engaging in deceptive practices, and conducting surveillance in public spaces, with limited exceptions for certain situations. Additionally, the legislation mandates that any material generated by AI that has not been reviewed by a qualified human must include a disclosure indicating its AI origin.

Disclosure of AI Use

Transparency complements oversight. Without clear disclosure requirements, stakeholders—including workers and employers—may be left in the dark about how AI systems impact decisions. Requiring disclosures when AI is used in high-risk areas is an important step toward protecting the public and strengthening trust in AI systems. Clear disclosure rules help people understand how AI systems work, what information they use, and what risks may be involved. This transparency not only reassures individuals that their personal data is being handled responsibly but also protects governments and organizations from legal and reputational harm. By setting clear standards for disclosures and transparency in high-risk AI applications, policymakers can protect individual rights, ensure fairness in decision-making, and foster innovation and efficiency within a framework of accountability.

Examples in Action:

Colorado SB 205 (2024) outlines new consumer protection regulations for high-risk AI systems. These regulations aim to enhance accountability and transparency in the deployment of AI technologies, particularly in sectors such as education, finance, health care, and legal services, where AI systems may make consequential decisions affecting consumers. Developers of high-risk AI systems are required to provide comprehensive documentation to deployers, including evaluations of performance, data governance measures, and known risks of algorithmic discrimination. Deployers must implement risk management policies, conduct impact assessments, and notify consumers when AI systems are used to make significant decisions. They are also obligated to disclose reasons for adverse decisions and provide opportunities for consumers to correct data or appeal decisions.

New York AB 433/S 822 (2025) outlines amendments to New York's technology and civil service laws, focusing on the regulation and disclosure of automated employment decision-making tools and AI systems used by state agencies. State agencies utilizing automated decision-making tools are required to publish a list of these tools on their websites by the end of the year following the amendments' effective date. This list must include descriptions of the tools, their start dates, purposes, and any other pertinent information to ensure transparency.

Data Security Requirements

In addition to understanding what AI programs are used and how, it is important that individuals understand what data is being collected by AI systems, where that data is stored, and how the data is protected. AI systems often process sensitive personal information that may impact an individual's health, civil rights, and/or livelihood. For example, in the context of leave management, the system may store important health records necessary to receive bonding leave or FMLA. For high-risk AI, robust data security not only protects individuals but also enables organizations to maintain accountability, comply with legal and ethical obligations, and preserve confidence in AI-driven decisions. Policymakers can develop policy standards regarding use of data in AI systems to ensure data input into high-risk systems is minimal, protected through encryption, and only utilized for articulated purposes.

Examples in Action:

The **Hawaii** State Data Office established a set of Data and AI Guiding Principles to drive trust, transparency, citizen satisfaction, and innovation by improving security, quality, accessibility, and accountability of data and AI. The principles set specific statewide rules and responsibilities at the state, county, and division levels.

Maryland SB 818 (2024) establishes a Governor's AI Subcabinet to develop policies and procedures for AI use across various sectors, including health care, cybersecurity, and education. This Subcabinet will collaborate with state agencies to enhance job creation, workforce development, and the management of critical infrastructure risks. The legislation introduces competitive proof of concept procurement methods for acquiring AI-related products and services, streamlining the procurement process while maintaining oversight.

Conclusion

As AI becomes increasingly embedded in workforce systems, state policymakers have a critical opportunity to shape its use in ways that protect workers, promote equity, and foster innovation. While AI offers powerful tools to streamline workplace leave and accommodation management, its application must be guided by ethical principles, legal compliance, robust oversight, and clear accountability. By establishing governance structures, enforcing transparency, and ensuring human review of high-risk decisions, states can build trust in AI systems while safeguarding constituent rights.

About DMEC

This document was developed by DMEC, the only national nonprofit association dedicated to advancing effective leave and accommodation management. DMEC serves more than 20,000 professionals representing 1,400+ employers nationwide—from private companies to government agencies—who manage millions of leave and accommodation cases annually.

This brief is part of the DMEC Policy Blueprint, the first national, nonpartisan policy initiative grounded in the real-world experience of employers navigating workplace leave and accommodation management. The Blueprint identifies four priority areas where policymakers can lead with impact: Inter-State Leave Coordination, Artificial Intelligence, Mental Health, and Stay-at-Work/Return-to-Work. It is not a legislative agenda, but a collaborative resource designed to equip legislators, regulators, and administrators with field-tested strategies to modernize systems, reduce complexity, and strengthen workforce participation.

DMEC is a mission-driven organization that values partnership. We invite you to work with us to shape the future of leave and accommodation management. To get started, create a free policymaker account at **dmec.org/dmec-state-policy** or contact us at **partners@dmec.org**.

This brief does not indicate DMEC's endorsement of any specific policies and practices established by states. This document is intended to proactively educate state policymakers on issues relevant to workplace leave and accommodation management which may impact their employers and constituents.

DMEC

November 2025