BREAKOUT EXERCISE

Build the Policy: Workplace AI Governance in Healthcare

Nathaniel Glasser, Epstein Becker & Green | Gurkan Ay, Resolution Economics

INSTRUCTIONS

Please review the below skeleton AI governance policy for a healthcare organization. You have approximately 10 minutes. Please work through the following tasks and be prepared to share your group's top findings with the full group.

Your tasks:

- Identify the 3 biggest gaps in the policy — what is missing or underdeveloped?
- Flag the 2 provisions that would be hardest for your organization to implement, and explain why.
- Note any provisions that you think are legally required versus merely best practice.

SKELETON AI GOVERNANCE POLICY — "MERIDIAN HEALTH SYSTEM"

Policy Provision	Current Policy Language (Skeleton)
1. Scope & Covered Tools	This policy applies to AI tools used in employment decisions, including hiring and scheduling.
2. Vendor Due Diligence	Before procurement, the HR department will review vendor documentation for AI tools.
3. Bias Auditing	The organization will conduct periodic audits of AI hiring tools for potential bias.
4. Human Review & Override	A human reviewer will be involved in final employment decisions where AI is used.
5. Employee Notice & Transparency	Employees will be notified when AI tools are used in certain decisions affecting their employment.
6. Data Governance & Retention	Data used by AI tools will be stored and retained in accordance with applicable law.
7. Accountability & Governance	The CHRO is responsible for oversight of this policy.

DISCUSSION

Use these prompts to guide your group's analysis of the skeleton policy:

- Does "periodic audits" meet the standard under NYC Local Law 144 or something else? What frequency and methodology would satisfy regulators?
- Who owns vendor contract compliance when a third-party AI tool causes a discriminatory outcome? Is that addressed here?
- The policy covers "hiring and scheduling." Does it need to cover AI tools used in performance management, discipline, or termination decisions?
- Is "applicable law" specific enough for data governance in a HIPAA-regulated environment? What else belongs here?

QUESTIONS FOR YOUR GROUP

1. **What are the 3 biggest gaps in this policy?**
2. **Which 2 provisions would be hardest to implement at your organization, and why?**
3. **Which provisions in this policy are legally required by existing law, and which are merely best practice? Does that distinction matter for your organization?**