

From Tools to Digital Workers

Organizations need new approaches to manage AI that performs accountable work

Fabio A. Thiers, MD, PhD

ConverGen AI, New York, NY, USA

ABSTRACT

Healthcare organizations are beginning to assign operational work to AI systems while continuing to manage them primarily as software. The mismatch becomes consequential when an AI-enabled system uses organizational identity, operates systems of record, communicates with people, or changes workflow state. This article aims to guide the industry through this transition by introducing the Digital Worker as the bounded, role-bearing unit through which AI-enabled capability performs work under organizational authority. The term does not confer personhood or employment status; it creates a persistent management object to which scope, identity, permissions, supervision, performance, evidence, incident history, operational memory, and lifecycle decisions can be attached. Used precisely, the designation separates technical agency from organizational role and supports integration with workflow, identity, quality, accountability, and risk-financing systems.

Keywords: healthcare AI; AI agents; Digital Workers; Digital Labor; Digital Operations; operational identity; organizational memory; non-human identity; risk financing

Key points

- **AI performing work creates a new management problem.** Once AI systems perform accountable work on behalf of an organization, they require management processes that extend beyond traditional software lifecycle management.
- **Digital Workers become the managed operational unit.** Organizations need a persistent role through which identity, authority, supervision, operational history, performance, and lifecycle can be managed consistently.
- **Persistent operational memory enables continuous improvement.** Maintaining explicit operational history supports supervision, organizational learning, auditability, and evidence-based autonomy gating.
- **Digital Operations is the discipline that manages Digital Labor.** It provides the operational framework needed to supervise Digital Workers, integrate them into accountable workflows, and generate evidence that supports governance, quality management, financial planning, risk management, and insurance underwriting.

Healthcare organizations are assigning work before defining the worker

Healthcare organizations are moving beyond AI that only summarizes, predicts, or advises. Emerging agentic AI systems can retrieve patient and payer information, navigate software, prepare documentation, update queues, draft communications, and coordinate multi-step activity on behalf of the organization. In these settings, the central management problem is no longer only whether the software functions properly. It is whether the organization can identify, authorize, supervise, continuously evaluate, and reconstruct work performed through the system.

The mismatch is familiar from earlier waves of enterprise technology. Information technology produced durable gains when organizations redesigned work, coordination, decision rights, and control around it rather than treating the technology as a self-contained artifact.¹⁻⁴ Sociotechnical and healthcare work-system research similarly shows that performance and safety emerge from the interaction of people, technology, tasks, environment, and organizational conditions.⁵⁻⁷ Agentic AI makes this requirement more explicit because the system may become the

immediate operator of defined workflow steps while residual accountability remains with the healthcare organization.

The vocabulary used to manage the system therefore matters. A model is a technical component. A tool assists a user. An automation executes a specified sequence. An agent perceives, plans, and acts in an environment. None of those terms, by itself, identifies the organizational role through which work is assigned, supervised, measured, and retained. The Digital Worker concept is intended to fill that gap for managers of healthcare operations.

Agent is a technical term; Digital Worker is a management term

The AI literature has long used agent to describe systems that perceive an environment and take actions toward objectives.^{8,9} Recent healthcare commentary extends that framing to agentic AI teammates, emphasizing systems that can move from passive assistance toward active participation in care-related work.¹⁰ This terminology is useful for describing architecture and behavior. It is insufficient for specifying how an accountable institution should manage the resulting work.

A Digital Worker is a locally configured, role-bearing unit through which AI-enabled capability performs bounded work under organizational authority. The term does not imply consciousness, legal personhood, employment status, or equivalence to a human worker. It identifies the unit to which the organization attaches a purpose, owner, supervisor, scope, prohibited actions, operational identity, access profile, context requirements, performance standards, evidence obligations, autonomy limits, incident history, and lifecycle.

This distinction reduces rather than increases confusion when used precisely. Agent remains the technical category. Digital Worker becomes the operating designation used only when an AI-enabled system performs a defined role. Many agents will never be Digital Workers: a research assistant used episodically by an individual, a general chatbot, or a demonstration agent may remain a tool. Conversely, one Digital Worker may be implemented through several models, rules, retrieval services, and specialized agents. The Digital Worker is therefore not another name for the model. It is the bounded organizational role assembled from those components.

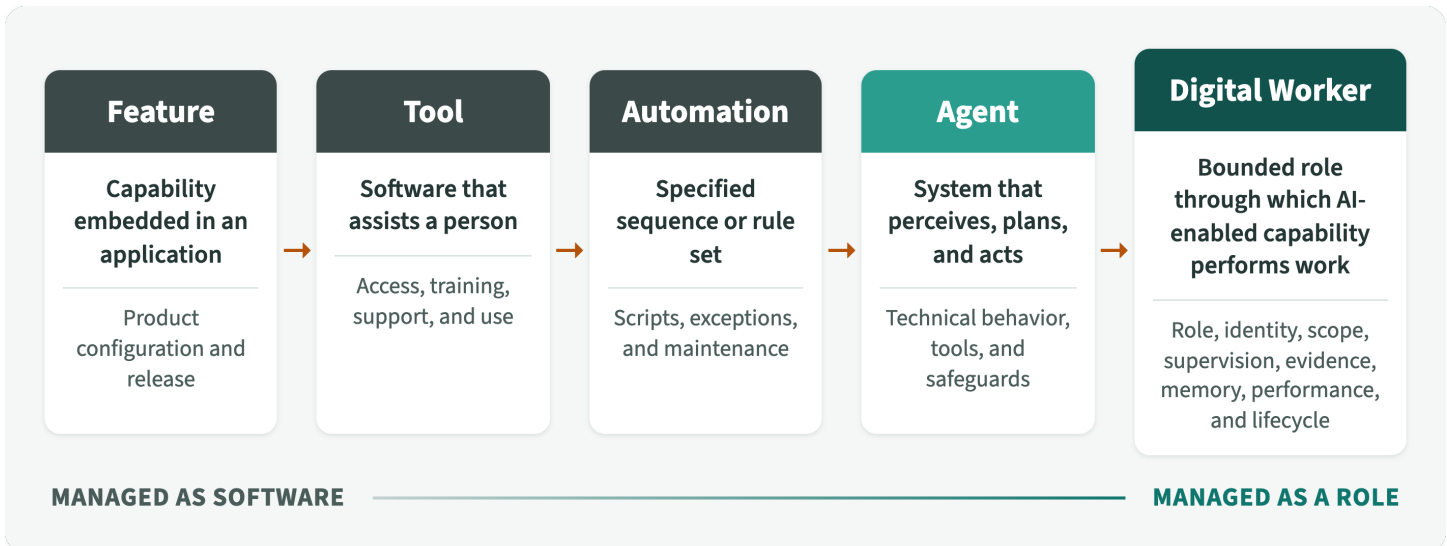


FIGURE 1 - From software categories to a Digital Worker. The categories are related but not interchangeable. Digital Worker is reserved for a bounded organizational role, not for every model, tool, automation, or agent.

Value is derived from the persistence of the management object

The main value of the Digital Worker framing is not rhetorical. It creates a persistent institutional object that can be integrated with systems the organization already uses to manage accountable work of its human workforce. A workflow platform can assign cases to a named Digital Worker. Identity systems can provision a distinct non-human identity. Quality systems can attach deviations and corrective actions to the role. Performance systems can aggregate outcomes across cases. Incident management can link a failure to the worker, configuration, source version, and authority state that existed at the time.

This matters because *ad hoc* tools are often session-bound and user-bound. A prompt may be reused without a registered owner. A browser agent may act through a shared service account. A model update may change behavior without a role-level change record. Logs may show API calls but not the institutional purpose, supervisor, or outcome. The Digital Worker designation requires those fragments to be joined around a role that persists across software versions and individual transactions.

The framing also makes accountability more precise. It does not transfer accountability from the organization to the machine. It identifies where authority was delegated, what controls applied, which human role retained supervision, and whether the work remained within its approved boundary. In this sense, the Digital Worker is a unit of delegated operational authority, not a substitute for institutional responsibility.

Operational identity connects action to authority

Once an AI-enabled system performs work, identity becomes operational. The organization should be able to answer which Digital Worker performed an action, for which case, using which credential, under which role definition, with what authority, and under whose supervision. A generic service account or vendor-level identifier does not provide that chain of attribution.

The cybersecurity industry is also converging on the importance of non-human identities. Service accounts, workload identities, and machine credentials create risks when they are overprivileged, shared, poorly monitored, or not revoked when their purpose

ends.¹¹⁻¹³ The Digital Worker framing adds the operational layer that security controls alone do not provide: why the identity exists, which work it may perform, which sources and systems it may use, and what evidence must accompany its actions.

Access should therefore follow role scope and least privilege. A worker that retrieves claim status does not require authority to submit an appeal. A worker that drafts a patient message may be prohibited from sending it. A worker that assembles a prior-authorization packet may read designated clinical documents but lack authority to alter the clinical record. Operational identity allows permissions to be granted, observed, narrowed, suspended, and revoked at the level of the role.

A Digital Worker accumulates memory

The strongest distinction from an *ad hoc* tool is that Digital Workers can carry longitudinal history indefinitely. A managed Digital Worker should be supported by three related forms of memory. **Execution memory** preserves the current case state needed to complete a workflow across steps, systems, people, and time. **Operational memory** preserves evidence of work performed: source documents and versions, retrieved facts, tool calls, intermediate decisions, uncertainty signals, approvals, overrides, escalations, outcomes, corrections, incidents, and changes in authority. **Organizational memory** converts validated patterns from that history into institution-controlled knowledge that can improve procedures, retrieval rules, evaluation cases, escalation thresholds, and role design.

These forms of memory are not equivalent to a tool's context window or generic conversational memory. Tool memory may be transient, provider-controlled, incomplete, or optimized solely for generating the next response. Digital Worker memory is retained for operational continuity, traceability, supervision, and learning. It must distinguish validated knowledge from unreviewed interactions, preserve provenance, comply with privacy and retention requirements, and remain available when the underlying model, configuration, or vendor changes.

The practical value is cumulative. Execution memory prevents the worker from treating a long-horizon workflow as disconnected prompts. Operational memory enables the organization to reconstruct why an action occurred, which conditions applied,

how humans intervened, and whether performance supports the authority granted. Organizational memory ensures that resolved exceptions and supervisor corrections become reusable institutional knowledge rather than disappearing across sessions. The organization can therefore maintain an explicit, accumulated history for the Digital Worker without attributing personhood to it. This history is an organizational asset, governed by the institution and separable from any particular model.

Documentation frameworks such as model cards, datasheets, supplier factsheets, and internal algorithmic audits established the importance of structured records for models, datasets, services, and accountability processes.¹⁴⁻¹⁷ A Digital Worker Record extends that logic to the operating role. It records not only what the component is, but what the role is authorized to do here, how it has performed, which validated corrections and operational lessons have been incorporated, and how its authority has changed.

Digital Worker is part of the organization

A Digital Worker becomes organizationally consequential through repeated interactions with people. Staff assign cases, review proposed actions, correct mistakes, provide missing context, resolve escalations, and adapt their work around the worker.

Supervisors develop expectations about where it is dependable and where it requires review. Teams may redistribute tasks, change handoffs, and redesign queues because the Digital Worker is present.

These interactions make the Digital Worker an intrinsic part of the AI-enabled work system, even though it remains a technical system and not a person. The work of humans and the behavior of the Digital Worker become interdependent. Human-factors research has long shown that automation changes human workload, attention, trust, and function allocation; effective human-AI systems must make it possible to understand, correct, override, and appropriately rely on automated behavior.¹⁸⁻²⁰ The relevant unit is therefore the combined work system, not the agent or human in isolation.

This is also why the role cannot be treated as fully portable. The same technical agent configured elsewhere may not be the same Digital Worker. Local policies, supervisors, source hierarchies, access rights, escalation practices, patient populations, and accumulated history shape the role. A Digital Worker is partly constituted by its organizational relationships and operating history. Removing that context may preserve software capability while eliminating the role that made the work dependable.

The Digital Worker Record

01 Role and ownership Purpose, workflow, department, accountable owner, supervisor, and job family	02 Scope and prohibitions Permitted functions, prohibited actions, material boundaries, and escalation conditions
03 Operational identity and access Machine identity, credentials, authorized systems, least-privilege permissions, and revocation status	04 Context and source hierarchy Required organizational context, governing sources, freshness requirements, and reconciliation rules
05 Authority and autonomy Authority by function, approval requirements, evidence thresholds, and conditions for narrowing or expansion	06 Evidence and history Inputs, source versions, tool calls, decisions, approvals, overrides, outcomes, corrections, incidents, and changes
07 Performance and validation Shadow results, local evaluation, operational measures, drift signals, and revalidation schedule	08 Lifecycle Onboarding, configuration changes, suspension, redesign, retirement criteria, and retained organizational memory

One record follows the role across design, validation, operation, improvement, revalidation, suspension, and retirement

FIGURE 2 - The Digital Worker Record. The record is the minimum institutional object needed to connect role, identity, authority, supervision, evidence, accumulated history, and lifecycle.

Distinct from governance and digital health

Digital Operations is the management discipline for designing, supervising, measuring, governing, and improving Digital Labor. It begins where AI governance becomes operational. Governance determines whether an AI use is acceptable, who has decision rights, which policies apply, and the risk posture the organization will adopt. Digital Operations manages the role after and between those decisions: current context, task allocation, identity, permissions, supervision, evidence, incidents, performance, change, and autonomy.

Digital Operations is also not a synonym for digital health. Digital health is a broad field encompassing technologies, data, services, research, care models, and policy. It does not identify the management discipline required when AI systems perform organizational work. Nor does Digital Operations replace IT operations, information security, privacy, clinical quality, human resources, or enterprise risk management. It provides the operating layer that connects those disciplines around Digital Workers and AI-enabled work systems.

This distinction is compatible with contemporary management frameworks. NIST AI RMF and ISO/IEC 42001 establish risk-management and management-system requirements across the AI lifecycle.^{21,22} Healthcare governance models emphasize accountability, oversight, and lifecycle management.^{23,24} These frameworks establish necessary institutional conditions. Digital Operations addresses the continuing execution problem: how the organization knows what each Digital Worker is doing, whether its authority remains justified, how humans are interacting with it, and what must change when performance or context changes.

The framing can support insurance underwriting

Insurance underwriting requires a defined exposure. A generic claim that an organization uses AI is too broad to support precise risk assessment. The Digital Worker framing creates a more tractable unit because the role can be described through identity, scope, authority, workflow, volume, supervision, controls, performance, incident history, and change management. These attributes do not make a Digital Worker automatically safe or insurable but make the exposure more observable.

A Digital Worker Record can support underwriting questions that are otherwise difficult to answer: What work is performed? Which actions can create material consequence? How much authority is granted? Which controls prevent or detect error? Who supervises exceptions? Can the organization reconstruct incidents? Has authority changed after near misses or environmental change? The same evidence can support contracting, audit, liability analysis, and risk financing, although each use requires its own legal and actuarial judgment.^{25,26}

The practical effect is to move discussion from abstract model risk toward role-specific operational exposure. Insurers can

distinguish a worker that retrieves non-clinical status information under narrow permissions from one that sends patient-specific communications or changes clinical workflow state. Organizations can also show whether authority is evidence-gated and reversible. This does not eliminate uncertainty, but it creates the evidence base needed to price, limit, exclude, or progressively cover specific forms of Digital Labor.

The market is converging on workforce language

The proposed healthcare use of Digital Worker and Digital Labor does not arise in isolation. Business and research organizations increasingly describe agentic AI through workforce, teammate, and organizational-design language. Microsoft's 2025 Work Trend Index reported that many leaders expected to use "digital labor" to expand workforce capacity and described organizations combining human employees and agents.²⁷ Stanford researchers have examined how workers want AI agents to automate or augment occupational tasks and introduced a Human Agency Scale to express preferred human involvement.²⁸ Stanford HAI and Google DeepMind have also framed AI adoption as an organizational-design challenge.²⁹

These uses are not identical. Digital labor has also long referred to human labor mediated through digital platforms, and that literature should not be collapsed into machine-performed work.³⁰ The healthcare contribution proposed here is narrower and operational: Digital Labor is the work performed by Digital Workers; a Digital Worker is the bounded role-bearing unit; Digital Operations is the discipline that manages the work; and a Digital Operations System (DOPs) is the infrastructure that applies the discipline consistently. Precision is necessary if the terminology is to clarify rather than obscure.

Executive Test for the Digital Worker Designation

Seven questions the organization must answer in writing — and the evidence each answer requires

- 1 **CLASSIFICATION** Is the system assisting a person, or performing a bounded role?
EVIDENCE Written designation as feature, tool, automation, agent, or Digital Worker
- 2 **ROLE** What work is assigned and who owns the role?
EVIDENCE Role definition, workflow, accountable owner, and supervisor
- 3 **IDENTITY & ACCESS** Which persistent identity and permissions are attached?
EVIDENCE Non-human identity, least-privilege access, credential controls, and audit trail
- 4 **SUPERVISION** What is reviewed, escalated, corrected, or prohibited?
EVIDENCE Review points, escalation rules, prohibited actions, and override process
- 5 **MEMORY & TRACEABILITY** Can the organization reconstruct and learn from the worker's history?
EVIDENCE Sources, actions, human interactions, outcomes, corrections, incidents, and change history
- 6 **AUTHORITY** What evidence expands, narrows, suspends, or revokes authority?
EVIDENCE Local thresholds, autonomy state, incident criteria, and documented decisions
- 7 **LIFECYCLE** How is the role onboarded, revalidated, redesigned, and retired?
EVIDENCE Lifecycle plan, change log, revalidation schedule, and retirement criteria



Ready to operate only when every question is answered in writing and supported by evidence

FIGURE 3 - Executive test for the Digital Worker designation. The term should identify an operating architecture, not merely a preferred description of an agent.

When to use and not use the terminology

The Digital Worker designation should be applied only when five conditions are present. **1)** The system performs defined work rather than merely providing general assistance. **2)** It acts under organizational authority. **3)** It has a persistent operational identity. **4)** Its scope, supervision, evidence, and lifecycle are explicitly managed. **5)** Its actions and outcomes can be attached to an institutional record. Without these conditions, the system should continue to be described as a model, tool, automation, or agent.

This threshold prevents anthropomorphic overreach and terminology inflation. It also makes the designation testable. Calling every chatbot a Digital Worker would increase confusion. Reserving the term for managed, role-bearing work reduces confusion by signaling that a specific operational architecture and accountability structure exist. The designation carries weight only when the organization accepts the corresponding obligations.

Close: the managed unit is the role, not the model

Healthcare organizations are beginning to assign work to AI systems faster than they are building the management infrastructure around that work. Continuing to describe every system only as software, a tool, or an agent leaves important questions unresolved: which role is performing the work, under what authority, with which identity, through what human relationships, and with what accumulated evidence and history?

The Digital Worker concept answers those questions by defining a bounded organizational role rather than a new class of model. Its practical value comes from the management obligations it creates. The role must be registered, scoped, supervised, measured, traceable, capable of learning from structured corrections, and subject to revalidation, narrowing, suspension, and retirement. Its operational memory belongs to the organization and should persist beyond individual sessions, model versions, and vendors.

Digital Operations is the discipline required to manage this role-bearing work. A Digital Operations System (DOPs) provides the persistent records and controls through which Digital Workers can be integrated into workflows, identity systems, quality processes, risk management, and, where appropriate, insurance underwriting. Used with precision, the terminology does not anthropomorphize AI or replace established disciplines. It clarifies the management unit that emerges when AI capability begins performing accountable work.

Glossary of key concepts

- **AI-enabled work system.** The complete sociotechnical arrangement through which AI-enabled work is performed, including Digital Workers, human roles, workflows, organizational context, tools, controls, and the operating environment.
- **Digital Worker.** The bounded, role-bearing unit through which AI-enabled capability performs defined work under organizational authority.
- **Digital Labor.** Work performed by Digital Workers under organizational authority, with defined purpose, scope, supervision, evidence obligations, and lifecycle management.
- **Digital Operations.** The management discipline for designing, supervising, measuring, governing, and improving Digital Labor.

- **Digital Operations System (DOPs).** The organizational and technical infrastructure through which Digital Operations is implemented across Digital Workers and AI-enabled work systems.
- **Operational identity.** A persistent identity that connects a Digital Worker's access, actions, evidence, incidents, and lifecycle to a managed role.
- **Digital Worker Record.** The institutional record that defines and tracks role, scope, authority, identity, supervision, evidence, accumulated history, performance, and lifecycle.
- **Organizational memory.** Institution-controlled, provenance-preserving history derived from work, human interactions, corrections, outcomes, incidents, and approved changes.

Live Article information

This PDF is a dated snapshot of a continuously maintained Live Article. Material updates undergo editorial review, and substantive public revisions are released when warranted.

The current maintained article and evidence base are available through the ConverGen Digital Operations Advisor: www.convergen.ai/advisor/

Peer-review status: This public edition has not undergone external peer review.

Competing interests: The author is the founder and CEO of ConverGen AI, which develops and commercializes a Digital Operations System (DOPs) for healthcare organizations.

AI-assisted tools: AI-assisted tools supported research synthesis, drafting, editing, and figure production. The author reviewed and takes responsibility for all content.

Author ORCID: 0009-0008-1814-1983.

References

1. Chandler, A. D. Jr. *The Visible Hand: The Managerial Revolution in American Business*. Harvard University Press (1977).
2. Beniger, J. R. *The Control Revolution: Technological and Economic Origins of the Information Society*. Harvard University Press (1986).
3. Brynjolfsson, E. & Hitt, L. M. Beyond computation: information technology, organizational transformation and business performance. *J. Econ. Perspect.* 14, 23-48 (2000). <https://doi.org/10.1257/jep.14.4.23>.
4. Bresnahan, T. F., Brynjolfsson, E. & Hitt, L. M. Information technology, workplace organization, and the demand for skilled labor: firm-level evidence. *Q. J. Econ.* 117, 339-376 (2002). <https://doi.org/10.1162/003355302753399526>.
5. Carayon, P. et al. Work system design for patient safety: the SEIPS model. *Qual. Saf. Health Care* 15 Suppl. 1, i50-i58 (2006). <https://doi.org/10.1136/qshc.2005.015842>.
6. Holden, R. J. & Carayon, P. SEIPS 101 and seven simple SEIPS tools. *BMJ Qual. Saf.* 30, 901-910 (2021). <https://doi.org/10.1136/bmjqs-2020-012538>.
7. Salwei, M. E. & Carayon, P. A sociotechnical systems framework for the application of artificial intelligence in health care delivery. *J. Cogn. Eng. Decis. Mak.* 16, 194-206 (2022). <https://doi.org/10.1177/15553434221097357>.
8. Wooldridge, M. & Jennings, N. R. Intelligent agents: theory and practice. *Knowl. Eng. Rev.* 10, 115-152 (1995). <https://doi.org/10.1017/S0269888900008122>.
9. Russell, S. & Norvig, P. *Artificial Intelligence: A Modern Approach*. 4th edn. Pearson (2020).
10. Zou, J. & Topol, E. J. The rise of agentic AI teammates in medicine. *Lancet* 405, 457 (2025). [https://doi.org/10.1016/S0140-6736\(25\)00202-8](https://doi.org/10.1016/S0140-6736(25)00202-8).

11. Open Worldwide Application Security Project. OWASP Non-Human Identities Top 10 (2025). <https://owasp.org/www-project-non-human-identities-top-10/>. Accessed 21 Jul 2026.
12. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29 (2024). <https://doi.org/10.6028/NIST.CSWP.29>.
13. U.S. Department of Health and Human Services. Summary of the HIPAA Security Rule (2024). <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>. Accessed 21 Jul 2026.
14. Mitchell, M. et al. Model cards for model reporting. *Proc. Conf. Fairness Accountability Transparency* 220-229 (2019). <https://doi.org/10.1145/3287560.3287596>.
15. Gebru, T. et al. Datasheets for datasets. *Commun. ACM* 64, 86-92 (2021). <https://doi.org/10.1145/3458723>.
16. Arnold, M. et al. FactSheets: increasing trust in AI services through supplier declarations of conformity. *IBM J. Res. Dev.* 63, 6:1-6:13 (2019). <https://doi.org/10.1147/JRD.2019.2942288>.
17. Raji, I. D. et al. Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. *Proc. 2020 Conf. Fairness Accountability Transparency* 33-44 (2020). <https://doi.org/10.1145/3351095.3372873>.
18. Parasuraman, R., Sheridan, T. B. & Wickens, C. D. A model for types and levels of human interaction with automation. *IEEE Trans. Syst. Man Cybern. A* 30, 286-297 (2000). <https://doi.org/10.1109/3468.844354>.
19. Lee, J. D. & See, K. A. Trust in automation: designing for appropriate reliance. *Hum. Factors* 46, 50-80 (2004). https://doi.org/10.1518/hfes.46.1.50_30392.
20. Amershi, S. et al. Guidelines for human-AI interaction. *Proc. 2019 CHI Conf. Hum. Factors Comput. Syst.* 1-13 (2019). <https://doi.org/10.1145/3290605.3300233>.
21. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1 (2023). <https://doi.org/10.6028/NIST.AI.100-1>.
22. International Organization for Standardization. ISO/IEC 42001:2023 Artificial intelligence - Management system (2023). <https://www.iso.org/standard/81230.html>. Accessed 21 Jul 2026.
23. Reddy, S., Allan, S., Coghlan, S. & Cooper, P. A governance model for the application of AI in health care. *J. Am. Med. Inform. Assoc.* 27, 491-497 (2020). <https://doi.org/10.1093/jamia/ocz192>.
24. Bodnari, A. & Travis, J. Scaling enterprise AI in healthcare: the role of governance in risk mitigation frameworks. *npj Digit. Med.* 8, 272 (2025). <https://doi.org/10.1038/s41746-025-01700-4>.
25. Mello, M. M. & Guha, N. Understanding liability risk from using health care artificial intelligence tools. *N. Engl. J. Med.* 390, 271-278 (2024). <https://doi.org/10.1056/NEJMhle2308901>.
26. Stern, A. D., Goldfarb, A., Minssen, T. & Price, W. N. II. AI insurance: how liability insurance can drive the responsible adoption of artificial intelligence in health care. *NEJM Catal. Innov. Care Deliv.* 3 (2022). <https://doi.org/10.1056/CAT.21.0242>.
27. Microsoft. The 2025 Annual Work Trend Index: The Frontier Firm is born (2025). <https://www.microsoft.com/en-us/worklab/work-trend-index/2025-the-frontier-firm-is-born>. Accessed 21 Jul 2026.
28. Shao, Y. et al. Future of work with AI agents: auditing automation and augmentation potential across the U.S. workforce. Preprint at <https://arxiv.org/abs/2506.06576> (2025).
29. Stanford Institute for Human-Centered Artificial Intelligence. AI for Organizations Grand Challenge (2025). <https://hai.stanford.edu/industry/ai-for-organizations-grand-challenge>. Accessed 21 Jul 2026.
30. Rahman, A. T. M. M. & Sultana, S. Digital labor: challenges, ethical insights, and implications. Preprint at <https://arxiv.org/abs/2506.11788> (2025).