Healthcare Trust Institute

Testimony on AI in Healthcare

Wisconsin Legislative Council Study Committee
Healthcare Trust Institute (HTI)
September 2026

Guiding Principles

Every use of AI in healthcare should be built on trust.

HTI represents healthcare organizations across the U.S. committed to using AI responsibly — protecting patients while enabling the benefits AI can deliver.

Transparency — patients should know when they're interacting with AI.

Accountability — organizations answer for how AI is used.

Fairness — AI should benefit patients and populations equitably.

Privacy — individual rights and health data must be protected.

I. Improving Patient Care

AI is transforming care — and every deployment should build trust.

AI covers many different applications, each with its own purpose and its own level of risk — from clinical decision support to everyday administrative tasks.

- **Clinical Care** — sharper imaging, safer treatment plans, fewer medication errors.
- **Population Health** — helps identify patients who could benefit from proactive outreach.
- **Patient Administration** — faster scheduling, claims answers, and plain-language help.

Healthcare Trust Institute

II. A Risk-Based Approach

Using AI, by itself, does not make an application high-risk.

What matters is what the system does, what's at stake, and whether human oversight is involved in the outcome.

- **Highest Safeguards for Highest Risk** — lower-risk uses, like R&D, should be encouraged, not burdened.
- **Humans Stay in Control of clinical decisions** — AI should inform the clinical decisions of health professionals, not replace them.
- **A Meaningful Distinction** — a system that flags information differs from one that decides on its own.

Healthcare Trust Institute

III. Safeguards

A risk-based approach still involves safeguards – the higher the risk, the stronger the safeguards.

Responsible AI deployment should rest on a few core practices — grouped here into four key areas.

Privacy & Security — privacy-by-design, data minimization, strong cybersecurity controls.

Data Quality — training data must be reliable, representative, and complete.

Ongoing Monitoring — watch for bias, model drift, and hallucinations after deployment.

Governance & Transparency — clear oversight, plus upfront disclosure when patients interact with AI.

Harmonize, Then Adapt

New AI rules should reinforce existing oversight — not duplicate or conflict with it.

Legislation should rely on established, risk-based, flexible frameworks rather than rigid, technology-specific mandates that quickly become outdated.

- **Rely on National Frameworks** — such as the NIST AI Risk Management Framework and the NAIC model bulletin, already adopted by 25 states.
- **Avoid Rigid Mandates** — technology-specific rules raise compliance costs and get outdated fast.
- **Support Continuous Improvement** — let clinical AI tools keep improving based on real-world evidence.

Healthcare Trust Institute

Key Points

State legislation should get six issues right — part 1 of 2.

Scope

Focus on high-risk AI — not the many everyday uses that have worked safely for years.

Meaningful Disclosure

Require upfront disclosure that a patient-facing tool is AI — not disclosure of proprietary algorithm details.

Impact Assessments

Compliance with recognized frameworks, like the NIST AI RMF, should satisfy this requirement.

Healthcare Trust Institute

Key Points

State legislation should get six issues right — part 2 of 2.

Meaningful Enforcement

State attorneys general only, with a chance to cure violations — no private right of action.

Consent & Opt-Out

Patient-by-patient consent and/or opt-out for AI use is impractical and could leave every patient worse off.

Consistent Definitions

Shared definitions across states ease compliance and reduce conflicting requirements.

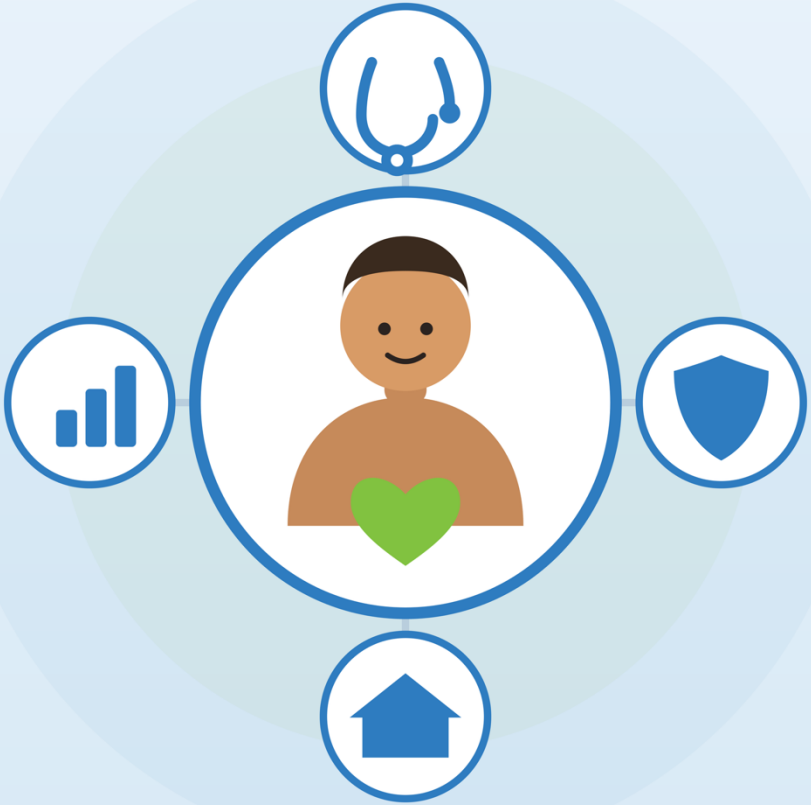
Healthcare Trust Institute

Conclusion

Putting patients at the center

The right framework is risk-based, proportionate, flexible, and coordinated — placing the strongest safeguards around the highest-risk applications while letting lower-risk uses keep improving care.

AI policy should keep AI trustworthy, transparent, and focused on augmenting clinicians — not on adding requirements that deprive patients of its benefits. Thank you for the opportunity to testify.



Appendix: Data Privacy

Health data privacy deserves special attention in the AI policy debate.

Health data privacy is regulated unevenly — by sector at the federal level and unevenly across states — creating gaps that any AI legislation must address directly.

- **Federal Patchwork** — HIPAA covers providers and their partners, but non-health companies handling health data are policed only after the fact, by the FTC.
- **A Growing State Patchwork** — without a comprehensive federal law, states are filling the gap with their own, often inconsistent, privacy laws — and data doesn't know borders.
- **One Standard as the Foundation** — AI legislation should rest on a single, harmonized privacy standard, not a fragmented patchwork that confuses patients and slows innovation.

Healthcare Trust Institute

Thank You

Tina O. Grande, MHS

President and CEO
Healthcare Trust Institute
tina@hctrustinst.com

We welcome your questions and look forward to continued dialogue on these issues.

Healthcare Trust Institute