

# PUBLICATION

---

## Federal AI Framework and Trump America AI Act: Health Care Impacts

Authors: Alisa L. Chestler, Michael J. Halaiko, Alexandra P. Moylan  
April 01, 2026

The federal government is moving toward a unified national approach to AI regulation – and health care and life sciences organizations need to pay attention. There have been two major developments in recent weeks: the Trump administration released its National Policy Framework for Artificial Intelligence (the Framework), outlining seven legislative priorities including child protection, intellectual property, innovation, and federal preemption of state AI laws; and Senator Marsha Blackburn (R-Tenn.) introduced a discussion draft of The Republic Unifying Meritocratic Performance Advancing Machine intelligence by Eliminating Regulatory Interstate Chaos Across American Industry (Trump America) Act (the Act), comprehensive proposed legislation that would codify Executive Order 14179 and establish a single federal rulebook for AI governance. In our companion alert, we review the details of the Framework and the Act.

For health care and life sciences organizations, the implications are significant. AI is already embedded throughout the health care system, from diagnostic imaging and clinical decision support to revenue cycle management, drug discovery, and clinical trial optimization. Both the Framework and the Act would introduce new liability frameworks, mandatory bias audits, copyright-based training data requirements, and transparency obligations that directly affect these high-risk, data-intensive applications. While neither proposal is final, the convergence of executive policy guidance and draft legislation signals that federal AI regulation may no longer be a question of "if" but "when." Organizations should begin assessing how these proposals may reshape their governance programs, compliance obligations, and product development strategies now and consider legislative engagement.

### I. Overview of the Framework's Seven Key Objectives

The Framework, released on March 20, 2026, organizes its legislative recommendations around seven core objectives: (1) child protection through age-assurance requirements and platform safety features; (2) infrastructure and economic growth, including ratepayer protections and streamlined permitting for AI data centers; (3) intellectual property protections, including collective licensing frameworks and digital replica rights; (4) content restrictions preventing government coercion of AI providers; (5) enabling innovation through regulatory sandboxes and sector-specific oversight rather than a new federal rulemaking body; (6) workforce training and education programs; and (7) preemption of state AI laws that impose "undue burdens," while preserving state police powers, zoning authority, and state procurement requirements. Notably, the Framework did not specifically address the use of medical or health care AI, though its provisions could have far-reaching impacts for the health care industry. Health care and life sciences stakeholders should be active participants in shaping how this framework is ultimately legislated – particularly to ensure that patient safety protections are explicitly carved out from any preemption provision, as they are in the child safety context.

### II. The Trump America AI Act

While the Framework articulates the Trump administration's policy goals, the Act attempts to create a statutory mechanism through which those goals would be implemented. The Act is structured around protecting the so-called "4 Cs" – children, creators, conservatives, and communities. Critically, the Act's general preemption provision differs markedly from the Framework's approach. The Framework calls for broad preemption of state AI laws that impose undue burdens; the Act, however, provides that it "shall not preempt any generally

applicable law, such as a body of common law or a scheme of sectoral governance." This distinction is consequential for health care and life sciences organizations, as existing regulatory frameworks—including FDA oversight of AI/ML-enabled medical devices, HIPAA, and state medical and health data privacy laws would remain fully operative under the Act's approach. The Act is broader in scope than the Framework in several important respects, and organizations should be aware of both convergences and divergences between the two.

### III. Implications for Health Care and Life Sciences Organizations

Health care and life sciences are among the highest-stakes sectors for AI deployment. Notably, neither the Framework nor the Act directly addresses how federal AI policy would interact with the FDA's authority over AI-enabled medical devices – a significant gap that stakeholders should work to fill through legislative engagement. The following areas warrant particular attention:

**New Liability Exposure.** The Act's proposed duty of care (Title I) and products liability provisions (Title VII) would create a fundamentally new liability framework for AI deployment. The statutory duty to prevent and mitigate foreseeable harm – paired with federal private rights of action for defective design and failure to warn – would need to be integrated with existing medical malpractice, FDA compliance, and HIPAA risk management programs. Organizations developing, deploying, or substantially modifying clinical AI systems should assess whether existing indemnification, quality management, and risk disclosure documentation is robust enough to defend against AI-related claims. Notably, products liability theories are being pursued in active litigation and warrant attention regardless of how the Act takes shape.

**Digital Replica Protections.** The Act would incorporate the NO FAKES Act (Title XII), establishing rights for individuals to control the use of their digital likeness. Organizations using patient images, voice recordings, or other biometric data in AI development should assess whether their consent frameworks would adequately address these digital replica rights if enacted.

**Mandatory Bias Audits.** The Title VIII (Section 801) bias audit requirement for high-risk AI systems would be directly applicable to health care AI used in treatment recommendations, insurance eligibility, or clinical resource allocation, as well as life sciences AI used in patient selection or diagnostic screening. Section 801 would specifically require audits to "detect any viewpoint discrimination or discrimination based on political affiliation" – a narrower focus than traditional anti-discrimination frameworks under Section 1557 of the ACA, which has been applied by HHS to clinical algorithms. These requirements would layer onto existing FDA expectations for AI/ML device performance across demographic subgroups.

**Section 230 Sunset.** The Act would sunset Section 230 of the Communications Act (Title III), which currently exempts platforms from liability for third-party content. Health information platforms, telehealth providers, and patient-facing AI tools that rely on current liability protections should evaluate how this proposed change would reshape their risk profiles.

**Multi-Jurisdictional Compliance.** The Framework calls for broad federal preemption, but the Act would preserve "generally applicable law" and "sectoral governance schemes." HIPAA and state health data privacy laws would likely survive, and FDA authority over AI/ML-enabled devices would remain intact. Organizations should maintain robust state compliance programs rather than assuming federal legislation will provide preemptive relief.

**Interaction with FDA's AI/ML Regulatory Framework.** The FDA has established an evolving framework for AI/ML-enabled medical devices, including its 2021 Action Plan and guidance on predetermined change control plans. The Act's preservation of "sectoral governance schemes" means FDA's existing authority – including over software as a medical device (SaMD) and clinical decision support software – would remain intact, but the

Act's products liability and bias audit provisions would create a multi-track compliance environment requiring careful integration with FDA's Total Product Life Cycle approach.

**NAIRR as a Research Catalyst for Health Care and Life Sciences.** The Act's proposed National AI Research Resource (Title X) could substantially reduce cost and access barriers for AI-enabled biomedical research. The Act would direct the Center for AI Standards and Innovation to prioritize standards development for biotechnology and health care (Section 911). Organizations with academic research partnerships should monitor NAIRR's governance structure, particularly regarding data sharing, IP ownership, and interaction with FDA regulatory pathways.

#### **IV. Recommended Action Steps for Health Care and Life Sciences Organizations**

In light of the Framework and the Act, health care and life sciences organizations developing, deploying, or using AI systems should consider the following priority actions:

1. **Conduct a comprehensive AI training data audit.** Title XV of the Act would address AI training data issues through copyright law – specifically Section 1501, which would amend fair use provisions to exclude unauthorized use of copyrighted works for AI training. Rather than establishing a standalone "affirmative consent" requirement, the Act's approach would operate through the existing copyright framework to require authorization for training on copyrighted works. Health care and life sciences organizations should immediately audit their data acquisition practices, data licensing agreements, institutional data sharing arrangements, and terms of service to assess whether they establish adequate authorization for AI training purposes, particularly for proprietary research data, biomedical literature, and patient records.
2. **Integrate AI products liability risk into governance and vendor management.** AI-related products liability lawsuits are already proceeding under existing state law theories, making this an area of risk regardless of whether the Act is enacted. The Act's Title VII would create additional federal exposure. Organizations should review AI vendor agreements for adequate indemnification, strengthen product documentation and safety disclosures, and evaluate whether existing quality management system (QMS) infrastructure can be extended to cover AI-specific risks such as algorithmic drift and model validation.
3. **Prepare for high-risk AI bias audit obligations.** Organizations should evaluate whether their clinical AI deployments – including treatment recommendations, diagnostic screening, and clinical trial patient selection – would fall within the Act's high-risk definition and begin planning for audit-ready documentation and ethics training programs.
4. **Maintain state AI and health data compliance programs.** The Act would not preempt generally applicable laws like HIPAA and state health data privacy statutes. Organizations should map their full inventory of state compliance obligations and avoid deprioritizing state-law compliance in anticipation of federal relief that may not materialize.
5. **Engage proactively with regulators and legislators.** Organizations should engage with the FDA, HHS, OCR, CMS, and the FTC as these agencies develop AI-specific guidance. Early engagement creates an opportunity to shape guidance before it becomes binding. Given the extended legislative timeline expected for the Act, health care associations and life sciences organizations should consider direct engagement to ensure their perspectives are represented before the legislative text is finalized.

6. **Leverage the NIST AI RMF as a baseline governance foundation.** The NIST framework's voluntary, outcome-based structure provides a practical compliance foundation consistent with both the Framework and the Act. Alignment also provides a defensible governance record in the event of regulatory examination or litigation.

For more information or for questions on this article, please contact [Alisa L. Chestler](#), [Michael J. Halaiko](#), [Alexandra P. Moylan](#), or any other member of Baker Donelson's [Health Law](#) Group.