

Landmark Executive Order on AI: What Does it Mean for Healthcare?

Article By:

Kristen O'Brien

Rachel Stauffer

On October 30, 2023, the White House released a long-awaited Executive Order (EO) on the “[Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#).” The EO acknowledges the transformative potential of AI while highlighting many known risks of AI tools and systems. It directs a broad range of actions around new standards for AI that will impact many sectors, and it articulates eight guiding principles and priorities to govern the development and use of AI (outlined below). This summary highlights directives in the EO that impact the use of AI in healthcare.

IN DEPTH

All stakeholders across the AI lifecycle (developers, deployers, users, auditors, etc.) should review the directives in the EO. While several directives significantly impact technology companies developing “foundation models,” along with government contractors and others developing advanced AI systems, the EO also directs action, reevaluation and potential changes in existing regulatory and enforcement schemes that could affect a variety of organizations. Additionally, the EO highlights a range of opportunities for formal and informal engagement to shape AI policy and standards, including through new task forces.

EO'S EIGHT GUIDING PRINCIPLES AND PRIORITIES FOR DEVELOPMENT AND USE OF AI

1. **Safety and Security:** AI must be safe and secure, which will require rigorous testing, evaluation and monitoring of AI systems, along with labeling and content provenance mechanisms to foster transparency and trust.
2. **Innovation and Competition:** Promoting responsible innovation, competition and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges.
3. **Commitment to Workforce:** The responsible development and use of AI requires a commitment to supporting American workers.
4. **Equity and Civil Rights:** AI should not deepen discrimination and must comply with federal

laws to advance civil rights.

5. **Consumer Protection:** The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected.
6. **Privacy:** Americans' privacy and civil liberties must be protected as AI continues advancing. AI is making it easier to extract, re-identify, link, infer and act on sensitive information about people's identities, locations, habits and desires.
7. **Government Use of AI:** It is important to manage the risks from the federal government's own use of AI and increase its internal capacity to regulate, govern and support responsible use of AI to deliver better results for Americans.
8. **Global Leadership:** The federal government should lead the way to global societal, economic and technological progress, as the United States has in previous eras of disruptive innovation and change.

HEALTHCARE-SPECIFIC DIRECTIVES IN THE EO

Section 8. Protecting Consumers, Patients, Passengers and Students

Section 8.b.i. Within 90 days of the EO's publication, the secretary of the US Department of Health and Human Services (HHS), in consultation with the secretary of defense and the secretary of veterans affairs, is required to establish an **HHS AI Task Force**. Within one year of establishment, the task force is required to develop a strategic plan that includes policies and frameworks—**possibly including regulatory action, as appropriate—on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health)**, and identify appropriate guidance and resources to promote such deployment, including in the following areas:

- **Developing, maintaining and using predictive and generative AI-enabled technologies in healthcare delivery and financing**—including quality measurement, performance improvement, program integrity, benefits administration and patient experience—taking into account considerations such as appropriate human oversight of the application of AI-generated output
- **Long-term safety and real-world performance monitoring of AI-enabled technologies in the health and human services sector**, including clinically relevant or significant modifications and performance across population groups, with a means to communicate product updates to regulators, developers and users
- **Incorporating equity principles into AI-enabled technologies used in the health and human services sector**, using disaggregated data on affected populations and representative population data sets when developing new models, monitoring algorithmic performance against discrimination and bias in existing models, and helping to identify and mitigate discrimination and bias in current systems
- **Incorporating safety, privacy and security standards** into the software-development lifecycle for protection of personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector
- **Determining appropriate and safe uses of AI** by developing, maintaining and making available documentation to help users in local settings in the health and human services sector
- **Advancing positive use cases and best practices for use of AI in local settings** by working with state, local, tribal, and territorial health and human services agencies
- **Identifying uses of AI to promote workplace efficiency and satisfaction** in the health and

human services sector, including reducing administrative burdens

Section 8.b.ii. Within 180 days of the EO's publication, the secretary of HHS is required to **develop a strategy**, in consultation with relevant agencies, to determine whether AI-enabled technologies in the health and human services sector **maintain appropriate levels of quality**. This work is to include **developing AI assurance policy**—to evaluate important aspects AI-enabled healthcare tools' performance—and infrastructure needs for enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.

Section 8.b.iii. Within 180 days of the EO's publication, the secretary of HHS, in consultation with relevant agencies as the secretary of HHS deems appropriate, is required to consider appropriate actions to advance the **prompt understanding of, and compliance with, federal nondiscrimination laws** by health and human services providers that receive federal financial assistance, as well as how those laws relate to AI. Such actions may include:

- Convening and providing technical assistance to health and human services providers and payers about their obligations under federal nondiscrimination and privacy laws as they relate to AI and the potential consequences of noncompliance
- Issuing guidance, or taking other action as appropriate, in response to any complaints or other reports of noncompliance with federal nondiscrimination and privacy laws as they relate to AI

Section 8.b.iv. Within 365 days of the date of this order, the secretary of HHS, in consultation with the secretary of defense and the secretary of veterans affairs, is required to establish an **AI safety program** that, in partnership with voluntary federally listed patient safety organizations:

- Establishes a **common framework for approaches to identifying and capturing clinical errors resulting from AI** deployed in healthcare settings, as well as specifications for a central tracking repository for associated incidents that cause harm, including through bias or discrimination, to patients, caregivers or other parties
- Analyzes captured data and generated evidence to develop, wherever appropriate, recommendations, best practices or other informal guidelines aimed at avoiding these harms
- Disseminates those recommendations, best practices or other informal guidance to appropriate stakeholders, including healthcare providers

Section 8.b.v. Within 365 days of the date of this order, the secretary of HHS is required to develop a **strategy for regulating the use of AI or AI-enabled tools in drug-development processes**. The strategy must, at a minimum:

- Define the objectives, goals and high-level principles required for appropriate regulation throughout each phase of drug development
- Identify areas where future rulemaking, guidance or additional statutory authority may be necessary to implement such a regulatory system
- Identify the existing budget, resources, personnel and potential for new public/private partnerships necessary for such a regulatory system

Section 5.2 Promoting Innovation

Section 5.2.a.i. Within 90 days of the EO's publication, in coordination with the heads of agencies

that the director of the US National Science Foundation (NSF) deems appropriate, **launch a pilot program implementing the National AI Research Resource (NAIRR)**, consistent with past recommendations of the NAIRR Task Force.

Section 5.2.a.iii. Within 540 days of the EO's publication, the director of NSF should establish at least **four new national AI research institutes**, in addition to the 25 that are currently funded.

Section 5.2.e. To advance responsible AI innovation by a wide range of healthcare technology developers that promotes the welfare of patients and workers in the healthcare sector, the EO requires the secretary of HHS to **identify and prioritize grantmaking and other awards, as well as undertake related efforts, to support responsible AI development and use**, including:

- Collaborating with appropriate private sector actors through HHS programs that may support the advancement of AI-enabled tools that develop personalized immune-response profiles for patients
- Prioritizing the allocation of 2024 Leading Edge Acceleration Project (LEAP) cooperative agreement awards to initiatives that explore ways to improve healthcare-data quality to support the responsible development of AI tools for clinical care, real-world-evidence programs, population health, public health and related research
- Accelerating grants awarded through the National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity (AIM-AHEAD) program and showcasing current AIM-AHEAD activities in underserved communities

NON-HEALTHCARE-SPECIFIC DIRECTIVES IN THE EO

Section 4. Ensuring the Safety and Security of AI Technology

Section 4.1.a. Within 270 days of the EO's publication, the secretary of commerce is required to **develop guidelines, standards and best practices for AI safety and security**. Specifically, the secretary of commerce is required to work through the director of the National Institute of Standards and Technology (NIST), and in coordination with the secretary of energy, the secretary of homeland security and the heads of other relevant agencies as the secretary of commerce may deem appropriate, to:

- Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure and trustworthy AI systems, including:
 - Developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI
 - Developing a companion resource to the Secure Software Development Framework to incorporate secure development practices for generative AI and for dual-use foundation models
 - Launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity

Section 4.2.a. Within 90 days of the EO's publication, to **ensure and verify the continuous availability of safe, reliable and effective AI in accordance with the Defense Production Act**, the secretary of commerce will require:

-
- Companies developing or demonstrating an intent to develop potential dual-use foundation models to **provide the federal government, on an ongoing basis, with information, reports or records** regarding the following:
 - Any ongoing or planned activities related to training, developing or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats
 - The ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights
 - The results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security
 - Companies, individuals or other organizations or entities that acquire, develop or possess a potential large-scale computing cluster to report any such acquisition, development or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster

Section 4.5.a. Within 240 days of the date of this order, the secretary of commerce, in consultation with the heads of other relevant agencies as the secretary of commerce may deem appropriate, is required to submit a report to the director of the Office of Management and Budget (OMB) and the assistant to the president for National Security Affairs identifying the **existing standards, tools, methods and practices, as well as the potential development of further science-backed standards and techniques**, for:

- Authenticating content and tracking its provenance
- Labeling synthetic content, such as using watermarking
- Detecting synthetic content
- Preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual)
- Testing software used for the above purposes
- Auditing and maintaining synthetic content

Section 4.5.b. Within 180 days of submitting the abovementioned report, the secretary of commerce, in coordination with the director of OMB, will **develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures**.

Section 4.6.a. Within 270 days, the secretary of commerce, in consultation with the secretary of state, is required to solicit input from the private sector, academia, civil society and other stakeholders through a public consultation process on potential risks, benefits, other implications, and appropriate policy and regulatory approaches related to dual-use foundation models for which the model weights are widely available.

Section 6. Supporting Workers

Section 6.b.i. Within 180 day of the EO's publication s, the secretary of labor, in consultation with other agencies and with outside entities (including labor unions and workers) as the secretary of labor deems appropriate, is required to **develop and publish principles and best practices for**

employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits. The principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover, at a minimum:

- Job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers
- **Labor standards and job quality, including issues related to the equity, protected-activity, compensation, health and safety implications of AI in the workplace**
- Implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management and activity protected under worker-protection laws

Section 12. Implementation

Section 12.a. The EO creates the **White House Artificial Intelligence Council**, which will coordinate the activities of agencies across the Federal Government to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in this EO.

IMPORTANT DEFINITIONS IN THE EO

- **Artificial intelligence (AI)** (defined in 15 U.S.C. 9401(3)): A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
- **Generative AI:** The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text and other digital content.
- **Machine learning:** A set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

CONCLUSION

The order is a consequential landmark document that sets the stage for the responsible governance of AI in the United States. By laying down guiding principles and a broad range of policy directives, the administration has created a roadmap for a coordinated, multi-stakeholder approach to AI across numerous industry sectors. This is a pivotal moment for AI governance, and while this EO is historic in its approach, the execution of its many directives depends heavily on the agencies and companies that have been called to action. Many of the key, material details and AI governance standards will be developed during the next six months to one year. For organizations interested in developing or using AI or machine learning tools in healthcare, there will be far-reaching implications as new standards, compliance expectations and other guidelines emerge.

Notably, this EO comes on the heels of increased attention on AI by senior lawmakers in the House and Senate. Senate Majority Leader Chuck Schumer (D-NY) is leading a bipartisan group in holding a series of roundtables and listening sessions to help educate members and staff on the benefits and risks of AI across various sectors. Similarly, a primary committee of jurisdiction on the House side, the Energy and Commerce Committee, has begun a series of hearings on AI to help inform

policymakers of potential legislative and regulatory needs around the use of AI. For the administration's part, there is a recognition that Congress may be slow to act and meaningful federal agency action is needed in the meantime. There is also an eagerness to make progress heading into an election year.

We will continue to unpack and provide analysis on the directives in the EO, including as federal agencies work to implement the policies described in the EO. Note that the administration also published a [fact sheet](#) about the EO. If you have questions about the EO or other AI regulatory, legal or policy developments, reach out to one of the authors below or your regular McDermott lawyer.

© 2025 McDermott Will & Emery

National Law Review, Volume XIII, Number 305

Source URL: <https://natlawreview.com/article/landmark-executive-order-ai-what-does-it-mean-healthcare>