

# Biden Executive Order on Artificial Intelligence Highlights Breadth, Challenges, and More Activity to Come

Brian Lee (Alston & Bird LLP)  
Jane Lucas (Alston & Bird LLP)

*This article is brought to you by AHLA's Health Information and Technology Practice Group.*

On October 30, 2023, President Joe Biden signed the *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (EO).<sup>1</sup> The wide-ranging EO covers many sectors of the economy and corresponding federal agencies from labor and workforce to national security. While attempting to establish key foundational principles and definitions, the EO also takes aim at the safe, appropriate, and responsible development of artificial intelligence (AI) used in the delivery and oversight of health care services.

The EO follows previous Biden administration activity, including an October 2022 blueprint for an AI Bill of Rights,<sup>2</sup> which outlines guidelines for the design, use, and deployment of automated systems to protect consumers; numerous administration and congressional meetings with stakeholders; and growing attention and activity at the federal and state levels. With the rapid expansion and availability of AI tools, notably generative AI models, the EO reflects multiple overarching priorities and directives to establish broad guidance and standards as well as targeted directives for specific industries, including health care.

## **Biden Administration Principles, Priorities, and Key Definitions**

The EO articulates the following eight principles and priorities that will be used to advance and govern the development and use of AI:

1. Ensuring AI is safe and secure;
2. Promoting responsible innovation, competition, and collaboration to unlock potential and solve difficult challenges;
3. Committing to support American workers;
4. Ensuring AI policies are consistent with advancing equity and civil rights;
5. Protecting the interests of Americans who use, interact with, or purchase AI and AI-enabled products;
6. Protecting Americans' privacy and civil liberties;
7. Managing the risks from the federal government's use of AI and increasing its internal capacity to regulate, govern, and support responsible use of AI; and
8. Positioning the federal government to lead global societal, economic, and technological progress in AI.

In addition, the EO defines multiple important terms that either do not have a specific federal definition or rely on definitions that have been established in non-health care statutes. For example, the EO defines AI using the meaning 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.

An "AI system" is defined in the EO as "any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI." Based on this definition, an AI system could include virtually all the various AI and AI-enabled tools that are increasingly available and prevalent in the delivery of health care. This is somewhat of a thread across the EO—broad policies and requirements that would appear more applicable to other sectors will be imputed to AI in health care.

### **Overarching Directives to Develop Standards and Guidelines for AI**

As a requirement for establishing guidelines and best practices for AI systems, the EO directs the Director of the National Institute of Standards and Technology, in coordination with the Secretaries of Energy and Homeland Security, to, within 270 days:

- 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 for generative AI;<sup>3</sup>
  - Developing a companion resource to the Secure Software Development Framework<sup>4</sup> to incorporate secure development practices; and
  - 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.
- Establish appropriate guidelines to enable developers of AI to conduct structured testing to find flaws and vulnerabilities in AI systems to enable deployment of safe, secure, and trustworthy systems. These efforts must include:
  - Coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of certain AI models; and
  - In coordination with the Secretary of Energy and the Director of the National Science Foundation, developing and helping to ensure the availability of testing environments to support the development of safe, secure, and trustworthy AI technologies, as well as to support the design, development, and deployment of associated privacy-enhancing technology.

Other broad directives in the EO relate to the requirements for companies developing or intending to develop certain AI models to provide various information about the AI models to the federal government, particularly as they relate to cybersecurity and as these technologies may be used by owners and operators of critical infrastructure.

### **Directives to the Department of Health and Human Services (HHS)**

The EO directs HHS to undertake the following activities:

- Within 90 days, establish an HHS AI Task Force (Task Force).

- Within 365 days of its creation, the Task Force shall develop a strategic plan that includes policies, frameworks, and regulatory action on the responsible deployment and use of AI and AI-enabled technologies in health care, including but not limited to:
  - development, maintenance, and use of predictive and generative AI-enabled technologies in health care delivery and financing;
  - long-term safety and real-world performance monitoring of AI-enabled technologies;
  - incorporation of equity principles in AI-enabled technologies; and
  - incorporation of safety, privacy, and security standards into the software-development lifecycle for protection of personally identifiable information.
- Within 180 days, develop a strategy to determine whether AI-enabled technologies maintain appropriate levels of quality, including the development of an AI assurance policy and infrastructure needs for enabling a pre-market assessment and post-market oversight of AI-enabled health care technologies.
- Within 180 days, consider how federal nondiscrimination and privacy laws relate to AI and issue guidance or take action in response to complaints or reported noncompliance as they relate to AI.
- Within 180 days, publish a plan addressing the use of automated or algorithmic systems in the implementation of public benefits and services administered by HHS.
- Within 365 days, establish an AI safety program that:
  - Creates a common framework for approaches to identifying and capturing clinical errors resulting from AI used in health care settings;
  - Utilizes captured data to develop recommendations, best practices, or other informal guidelines; and
  - Disseminates the recommendations, best practices, or informal guidance to appropriate stakeholders.
- Within 365 days, develop a strategy for regulating the use of AI or AI-enabled tools in drug development processes.

### Where Do We Go from Here?

As Congress continues its work to better understand the threats and opportunities associated with AI into 2024, states are likely to continue their trend of adopting standards or enacting legislation regulating various segments of AI. This could lead to a patchwork of state-based requirements, much like what occurs with the regulation of data privacy. For AI developers, compliance with different state-based standards and requirements could prove difficult and costly.

From a federal health care standpoint, agencies like the Food and Drug Administration and the Centers for Medicare & Medicaid Services are already using existing regulatory tools and frameworks to address AI technologies and AI-enabled services. A big question is whether Congress will recognize that unlike other industries, health care has these existing frameworks to address AI and legislate accordingly. Additionally, will the EO spur or halt legislation that stymies innovation in health care, and will developers and manufacturers see new opportunities from future legislative or regulatory frameworks as AI continues to change the health care delivery system.

---

<sup>1</sup> <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>.

<sup>2</sup> <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

<sup>3</sup> <https://www.nist.gov/itl/ai-risk-management-framework>.

<sup>4</sup> <https://csrc.nist.gov/Projects/ssdf>.