FAQ: Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

Updated: 11/10/2023

The Biden-Harris Administration released the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence on Monday, October 30, 2023, aiming to use the extent of the Executive Branch's current authorities to regulate the use of artificial intelligence (AI) both within and outside of the US Federal Government. A fact sheet was released by the White House indicating the Executive Order aims to establish new standards for AI safety and security, protect Americans' privacy, advance equity and civil rights, stand up for consumers and workers, promote innovation and competition, advance American leadership, and address other key areas of focus.

While the Executive Order is the most aggressive piece of AI policymaking yet, it is noted that direction given to the agencies named within the Executive Order is subject to the availability of appropriations. Areas that need additional authorizations or appropriations to enact the directions contained within the Executive Order will need to rely on Congress to pass those measures. Nearly every Executive Branch Agency is named in the Executive Order and, even though not named explicitly, several provisions allude to work the Office of the National Coordinator for Health Information Technology (ONC) has already undertaken.

The Appendix to this document provides full text for all provisions within the Executive Order the AHIMA Policy and Government Affairs team has identified as impactful to the HI profession. Key highlights of the Executive Order Provisions include:

- Identifying and defining key terms related to AI providing harmony across the agencies;
- Provisions related to ensuring AI that is deployed and utilized is safe and reliable;
- Details on updates and the development of best practices related to the cybersecurity of AI;
- Promoting innovation and competition in the development of healthcare AI;
- Plans related to protecting workers including:
    - Identifying the impact of AI on the US workforce
    - Protecting workers as AI is deployed and utilized
    - Ensuring employee well-being is protected
    - Ensuring employee upskilling education is available
- Healthcare specific AI activities within the Department of Health and Human Services (HHS) including:
    - Creating an AI taskforce within HHS
    - Determining if HHS sub-agencies are able to determine if AI is reliable and safe and creating a plan to address identified issues
    - Creating an action plan to ensure AI is deployed and used in an equitable manner

The AHIMA Policy and Government Affairs team will remain engaged in the implementation of this Executive Order. If you have any questions, please contact us at advocacy@ahima.org.

Appendix

Key Definitions from Executive Order

- **Artificial Intelligence (AI):** Set forth 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.
- **AI Model:** A component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.
- **Dual-use Foundation Model: A**n AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters.
- **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.
- **AI Red-Teaming:** A structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI, most often performed by dedicated "red teams" that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

Relevant Executive Order Text

Sec. 4. Ensuring the Safety and Security of AI Technology

4. Developing Guidelines, Standards, and Best Practices for AI Safety and Security.

(a) Within 270 days NIST 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, shall:

(i) Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including:

(A) developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI;

(C) 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.

(ii) Establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. These efforts shall include:

(A) coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models; and

(B) in coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, 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 Technologies (PETs), consistent with section 9(b) of this order.

4.2. Ensuring Safe and Reliable AI.

(a) Within 90 days of the date of this order, to ensure and verify the continuous availability of safe, reliable, and effective AI in accordance with the Defense Production Act, as amended, 50 U.S.C. 4501 et seq., including for the national defense and the protection of critical infrastructure, the Secretary of Commerce shall require:

(i) 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:

(A) 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;

(B) 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; and

(C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST pursuant to

subsection 4.1(a)(ii) of this section, and a description of any associated measures the company has taken to meet safety objectives.

4.3. Managing AI in Critical Infrastructure and in Cybersecurity.

(a) To ensure the protection of critical infrastructure, the following actions shall be taken:

(i) Within 90 days of the date of this order, and at least annually thereafter, the head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant SRMAs, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security for consideration of cross-sector risks, shall evaluate and provide to the Secretary of Homeland Security an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks, and shall consider ways to mitigate these vulnerabilities. Independent regulatory agencies are encouraged, as they deem appropriate, to contribute to sector-specific risk assessments.

Sec. 5. Promoting Innovation and Competition.

5.2. Promoting Innovation.

(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 Secretary of HHS shall identify and, as appropriate and consistent with applicable law and the activities directed in section 8 of this order, prioritize grantmaking and other awards, as well as undertake related efforts, to support responsible AI development and use, including:

(i) 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, consistent with section 4 of this order;

(ii) prioritizing the allocation of 2024 Leading Edge Acceleration Project 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; and

(iii) 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.

Sec. 6. Supporting Workers.

(a) To advance the Government's understanding of AI's implications for workers, the following actions shall be taken within 180 days of the date of this order:

(i) The Chairman of the Council of Economic Advisers shall prepare and submit a report to the President on the labor-market effects of AI.

(ii) To evaluate necessary steps for the Federal Government to address AI-related workforce disruptions, the Secretary of Labor shall submit to of AI in the healthcare, public-health, and human-services sectors: agencies to support workers displaced by the adoption of AI and other technological advancements. The report shall, at a minimum:

(A) assess how current or formerly operational Federal programs designed to assist workers facing job disruptions -- including unemployment insurance and programs authorized by the Workforce Innovation and Opportunity Act (Public Law 113-128) -- could be used to respond to possible future AI-related disruptions; and

(B) identify options, including potential legislative measures, to strengthen or develop additional Federal support for workers displaced by AI and, in consultation with the Secretary of Commerce and the Secretary of Education, strengthen and expand education and training opportunities that provide individuals pathways to occupations related to AI.

(b) To help ensure that AI deployed in the workplace advances employees' well-being:

(i) The Secretary of Labor shall, within 180 days of the date of this order and in consultation with other agencies and with outside entities, including labor unions and workers, as the Secretary of Labor deems appropriate, 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:

(A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers;

(B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and

(C) 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.

(ii) After principles and best practices are developed pursuant to subsection (b)(i) of this section, the heads of agencies shall consider, in consultation with the Secretary of Labor, encouraging the adoption of these guidelines in their programs to the extent appropriate for each program and consistent with applicable law.

(iii) To support employees whose work is monitored or augmented by AI in being compensated appropriately for all of their work time, the Secretary of Labor shall issue guidance to make clear that employers that deploy AI to monitor or augment employees' work must continue to comply with protections that ensure that workers are compensated for their hours worked, as defined under the Fair Labor Standards Act of 1938, 29 U.S.C. 201 et seq., and other legal requirements.

(c) To foster a diverse AI-ready workforce, the Director of NSF shall prioritize available resources to support AI-related education and AI-related workforce development through existing programs. The Director shall additionally consult with agencies, as appropriate, to identify further opportunities for agencies to allocate resources for those purposes. The actions by the Director shall use appropriate fellowship programs and awards for these purposes.

Sec. 8. Protecting Consumers, Patients, Passengers, and Students.

(a) Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.

(b) To help ensure the safe, responsible deployment and use of AI in the healthcare, public-health, and human-services sectors:

(i) Within 90 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an HHS AI Task Force that shall, within 365 days of its creation, 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 that deployment, including in the following areas:

(A) development, maintenance, and use of 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;

(B) 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;

(C) incorporation of equity principles in 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;

(D) incorporation of 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;

(E) development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings in the health and human services sector;

(F) work to be done with State, local, Tribal, and territorial health and human services agencies to advance positive use cases and best practices for use of AI in local settings; and

(G) identification of uses of AI to promote workplace efficiency and satisfaction in the health and human services sector, including reducing administrative burdens.

(ii) Within 180 days of the date of this order, the Secretary of HHS shall direct HHS components, as the Secretary of HHS deems appropriate, 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, including, as appropriate, in the areas described in subsection (b)(i) of this section. This work shall include the development of AI assurance policy -- to evaluate important aspects of the performance of AI-enabled healthcare tools -- and infrastructure needs for enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.

(iii) Within 180 days of the date of this order, the Secretary of HHS shall, in consultation with relevant agencies as the Secretary of HHS deems appropriate, 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:

(A) 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; and

(B) 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.

(iv) Within 365 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an AI safety program that, in partnership with voluntary federally listed Patient Safety Organizations:

(A) 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;

(B) analyzes captured data and generated evidence to develop, wherever appropriate, recommendations, best practices, or other informal guidelines aimed at avoiding these harms; and

(C) disseminates those recommendations, best practices, or other informal guidance to appropriate stakeholders, including healthcare providers.