Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare ○ TLP:WHITE Alert ID : 9885a570 Nov 17, 2023, 08:45 AM

This week, *Hacking Healthcare*TM welcomes a guest essay which offers an extended examination of the recent Biden administration Executive Order that was published to address a wide range of Artificial Intelligence (AI) issues. We provide some general context, an overview of the scope of the document, and then dive into some of the healthcare specific aspects of the EO, their implications, and what Health-ISAC members may wish to consider doing in response.

Welcome back to *Hacking Healthcare*TM.

Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

Guest Essay by Heather West

Rapid advancements in the capabilities and sophistication of AI alongside a growing desire to integrate AI into an ever-expanding list of use cases, including in the Health Sector, has increasingly made policymakers and the public concerned over a lack of sufficient guardrails and oversight. On October 30th, the Biden administration took a significant step towards outlining how the U.S. would attempt to manage the risks posed by AI with the publication of the *Executive Order 14110: Safe, Secure, and Trustworthy Artificial Intelligence* (AI EO).[i] While the lengthy AI EO is too substantial to be comprehensively covered in its entirety, this week's edition of Hacking Healthcare will include some general thoughts and will highlight a few healthcare specific aspects.

Overview

Before we dive into the substance, it's important to level set as to what an Executive Order is for those not as familiar with the policy mechanism. An Executive Order (EO) is a document, from the President, that manages the operations of the Federal Government and often collects policy priorities and actions on a particular theme across agencies. An EO may instruct, or direct U.S. government entities or outline policy positions, but it is not legislation, requires no approval from Congress, and can be overturned at any time by the President, current or future. The use of an EO to achieve policy objectives has increased in recent years as partisan disagreements have slowed more traditional policy and lawmaking processes.

The AI EO has directed many government agencies to focus on specific AI priorities across the government, within their jurisdiction and authorities, and in their own use of AI. The EO seeks to find consensus and common equities across agencies, develop shared understanding, and identify where new approaches are needed on a host of AI issues. The AI EO is cognizant of AI's tremendous potential and directs agencies to undergo a number of efforts to manage risk inherent in using advanced AI systems. The Biden administration believes that unlocking its potential while mitigating its risks will require a "society-wide effort that includes government, the private sector, academia, and civil society."[ii] Accordingly, the AI EO's scope is understandably broad and contains eight guiding principles and priorities:

- AI must be safe and secure
- AI policies should promote responsible innovation, competition, and collaboration
- AI policies should lead to responsible AI development that supports American workers
- AI policies must promote equity and civil rights
- The protection of American citizens / Consumer protection is critically important
- The protection of privacy and civil liberties is critically important
- An AI competent workforce is critically important
- The U.S. must take on a global leadership role on AI

Why now?

Conversation - in government and otherwise - around AI has been at a fevered pitch. Governments around the world are looking to ensure that AI is adequately governed and regulated as the technology evolves, and as its use booms. The Biden administration has highlighted the AI EO as the largest and most significant government action on AI thus far, and its broad scope gives that claim credence. It joins actions in the European Union, the G7[iii], and a multi-national effort out of the United Kingdom, with goals to ensure that international AI governance reflects global and American priorities.

Why healthcare?

Healthcare, human services, and biologic use of AI are significant elements in the EO. There has been focus on both malicious use of AI to up-level the ability of bad actors to create biological threats or weapons, as well as ensuring nondiscriminatory and safe use of AI in healthcare and human services. The AI EO recognizes that AI is advancing research, drug and device safety, healthcare delivery and finance, and public health generally.

What's in there?

The AI EO has a significant focus on processes to evaluate and manage risk from AI throughout, as well as a section on safety and security (Section 4). These actions impact agency use of AI, further develop NIST and OMB standards, practices, and evaluation criteria, and seek to internationalize the voluntary safety commitments from AI companies. It also calls for guidelines on safety and security for AI used in critical infrastructure and proposes new reporting obligations for cloud computing providers who may provide capabilities to train advanced AI.

There are a number of actions that direct the Department of Health and Human Services (HHS) to establish a task force to develop a plan, policies, frameworks, and potential regulation of AI systems in health and human services, including AI oversight, safety, equity, and privacy. There are also actions to determine whether AI technologies in health and human services are of appropriate quality, whether there is adequate understanding and compliance with Federal nondiscrimination laws, and a specific call for a strategy for the use of AI in drug development, including future rulemaking and consideration of security.

The AI EO calls on HHS to collaborate with private sector actors through existing HHS programs, and to prioritize awards and grants to support the responsible development of AI tools.

The AI EO also considers whether AI could be used to create biological threats, or be used to create and spread misinformation, and how government agencies should understand and mitigate these risks.

What's next?

Over the next year, there are a number of actions for HHS and other agencies. There may be opportunity for private sector engagement around cybersecurity and risk management, both generally and in the health and human services sector.

Action & Analysis
****Included with Health-ISAC Membership****

Congress
Tuesday, November 14
No relevant meetings

Wednesday, November 15
No relevant meetings

Thursday, November 16
No relevant meetings

International Hearings/Meetings
-No relevant Meetings

[i] 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/
[ii] 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/

[iii] The G7 is described by the European Union's European Commission "as an informal forum bringing together the heads of government and ministers of the world's leading industrial nations." It is made up of Canada, France, Germany, Italy, Japan, the United Kingdom, the United States, and the European Union.

[iv] https://www.nist.gov/itl/ai-risk-management-framework

[v] https://csrc.nist.gov/projects/ssdf

[vi] The AI EO Defines the term "omics" as "means biomolecules, including nucleic acids, proteins, and metabolites, that make up a cell or cellular system."

[vii] 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/

[viii] 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/

[ix] 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/

[x] https://alliancefortrustinai.org/

Report Source(s)

Health-ISAC

Reference | References

NIST-CSF
NIST-CSF
alliancefortrustinai
Whitehouse

Tags

Executive Order, Regulatory, Hacking Healthcare, AI, Artificial Intelligence

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:
Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare™:
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council’s efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council’s Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC’s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC’s monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org