March 15, 2025

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov and via email to: ostp-ai-rfi@nitrd.gov

Faisal D'Souza
National Coordination Office
National Science Foundation
2415 Eisenhower Avenue
Alexandria, VA 22314

RE: Request for Information on the Development of an Artificial Intelligence (AI) Action Plan

Dear Mr. D'Souza:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Request for Information on the Development of an Artificial Intelligence (AI) Action Plan**,** as published in the *Federal Register* on February 6, 2025 (Vol. 90, No. 24). We look forward to continuing to be a trusted stakeholder and resource to President Trump, his new Administration – and continuing to deepen the long-standing relationship we have shared.

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. With more than 3,000 individual members in 58 countries and two U.S. territories and 200 CHIME Foundation healthcare IT business and professional service firm members, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate for the effective use of information management to improve the health and care in the communities they serve.

Key Recommendations and Takeaways

CHIME applauds President Trump's Executive Order 14179 – Removing Barriers to American Leadership in Artificial Intelligence – to establish U.S. policy for sustaining and enhancing America's AI dominance in order to promote human flourishing, economic competitiveness, and national security. As noted in the Request for

Information (RFI), this Executive Order directs the development of an AI Action Plan to advance America's AI leadership, in a process led by the Assistant to the President for Science and Technology, the White House AI and Crypto Czar, and the National Security Advisor.

CHIME appreciates that the Trump Administration recognizes that with the right government policies, the United States can solidify its position as the leader in AI and secure a brighter future for all Americans. The Office of Science and Technology Policy (OSTP) is seeking input on the highest priority policy actions that should be in the new AI Action Plan.

We commend President Trump's commitment to positioning America as the global leader in AI – ensuring a future of innovation, economic prosperity, and national security. CHIME appreciates that the Administration recognizes the pivotal role that sound government policy plays in unleashing AI's full potential and securing America's leadership in this critical domain. **By fostering direct engagement with key stakeholders through this RFI – particularly experts in healthcare information technology (IT) – the Administration is ensuring that the new AI Action Plan is informed by real-world expertise and aligned with national priorities.**

CHIME members believe that any AI policies under consideration should provide clear and consistent guidance, eliminate redundancies, reduce regulatory burdens on providers, and create an environment that incentivizes responsible AI innovation. These principles are essential to driving confidence, investment, and sustained leadership in AI-powered healthcare solutions.

We recognize that implementing AI at scale through hospitals and healthcare systems will require thoughtful and iterative policymaking, and we are encouraged by the Administration's emphasis on reducing bureaucracy and fostering a pro-innovation regulatory environment. This is a pivotal time, which represents a generational opportunity to modernize healthcare, improve patient outcomes, lower costs, and position America at the forefront of AI-driven advancements in healthcare. CHIME looks forward to continued collaboration to ensure that AI policies reflect these objectives and serve the best interests of patients, providers, and the nation as a whole.

Highest Priority Feedback for President Trump's New AI Action Plan

Healthcare delivery organizations (HDOs) are under significant pressure to meet a growing number of federal and state policies that often are duplicative, unnecessary, and do not add value to their primary mission – which is patient care. There are significant cost-savings – perhaps as much as a quarter of trillion dollars – that could be saved with greater administrative efficiencies. CHIME therefore is pleased that President Trump's "Massive 10-to-1 Deregulation Initiative," as announced through his Executive Order "Unleashing Prosperity Through Deregulation," could unlock some of these efficiencies.

An overarching theme and concern CHIME members are facing right now is regulatory uncertainty. Some are concerned that we may be at a tipping point for healthcare organizations and their ability to meet, maintain and sustain regulatory requirements. Given this, many are extremely hesitant to move forward investing in and purchasing AI tools and solutions without a better understanding of the regulatory landscape, which has been challenging under the Biden administration. Uncertainty in healthcare drives up costs, disrupts our members financial planning, and undermines efforts to improve health and wellness for all Americans.

Navigating an uncertain regulatory and legal landscape makes it significantly more challenging for our members to invest in AI technology which helps America keep pace with innovation and the ever-growing cybersecurity threats from hostile nation states, including the People's Republic of China (PRC). Cybersecurity, data protection, clinician education, initial costs and return on investment, and most importantly – patient safety – are all challenges our members are facing as they approach the responsible use of AI in their hospitals and healthcare systems. **Hospitals and healthcare systems are also facing crucial competing priorities such as cybersecurity needs, expenses that directly support patient care, and operational costs like repairing essential infrastructure. These competing demands make it challenging to allocate resources effectively while still advancing technological innovations.**

Even the largest and most resourced health systems – who have already invested countless hours and hundreds of millions of dollars into AI tools – list concerns with regulatory compliance as a top challenge. One such member noted that navigating rapidly evolving regulations surrounding AI in healthcare is arduous and costly. Further – members must balance high initial investment costs for AI implementation and developing methodologies to quantify the return on investment for AI projects.

CHIME members are currently navigating the complexities of AI adoption amidst an already intricate, complex regulatory landscape in healthcare. The uncertainty surrounding future regulations further complicates their efforts. We are eager to collaborate with the Administration and provide much-needed clarity and stability through the AI Action Plan.

Our members believe that any future policies, frameworks, and the AI Action Plan should be driven by a clear understanding of the purpose (why) and the methods (what) of using AI in healthcare. This approach ensures that AI development is effective and it safeguards patient data, while enabling innovation. In other words, the primary considerations for any future policies should be the intended use and benefits of the AI technology. **Policies should be flexible and adaptive, ensuring they protect patients without stifling technological advancement. This will promote the innovative use of AI, ensuring it can improve healthcare delivery while maintaining patient safety and privacy, as well as data security.**

CHIME members wish to convey that the usage of the term "AI" is extremely broad. AI is a language in itself – varying from natural language processing (NLP) to data

aggregation tools. Importantly, there are differences between “predictive AI” and “generative AI” which must be recognized, as they are two distinct types of AI, each with different functionalities and applications. Additionally, they are used in two very separate and distinct areas of a healthcare organization – administrative and clinical. It is important to ask our members what they are using, and why they are using it.

CHIME members have voiced excitement – and concerns – about the speed and promises of AI tools. They, however, recognize that innovation could quickly devolve into a situation of “haves” and “have nots.” The “have nots” cannot afford to implement AI solutions and will continue to lag behind their more well-resourced counterparts. While the work of “the haves” are, of course, of great import, they will continue to invest in AI tools and are currently doing so in a thoughtful and cautious manner, while staying alert to the inherent risks that accompany AI being introduced into their organization.

Due to the cost of implementing an AI tool within a hospital or healthcare system, many of our members are simply unable to afford them – and the state of AI in hospitals and healthcare systems is currently directly dependent upon the size and type of organization. Larger, more resourced hospitals and health centers are at the forefront of the AI frontier in healthcare, using it in innovative ways to do things we didn’t think were possible a few years ago.

Our members who are currently utilizing or planning to utilize AI tools have or are working to put a level of governance and oversight in place for both the clinical and operational processes. However, this too, brings challenges, including addressing compatibility issues with legacy healthcare IT systems such as their electronic health record (EHR), and overcoming challenges in standardizing data across different systems and departments to be used in AI solutions.

Additionally, our members are deeply committed to ensuring the highest standards of data security in AI model training and development, recognizing the critical role that secure and trustworthy AI plays in the healthcare sector. **Given their extensive expertise and direct operational experience, CHIME members are uniquely positioned to provide valuable, real-world insights into the practical implications of any AI Action Plan. We welcome the opportunity to engage with you throughout the development of this plan, leveraging our members' knowledge to help shape policies that are both effective and implementable.**

We also wish to acknowledge that the work done by President Trump’s Administration and the AI Action Plan can help bridge the digital divide that will grow for providers serving American patients living in rural, small, and under-resourced communities.

Application and Use

AI tools and solutions require our members to contract with vendors as third-parties, which inherently introduces risk into their ecosystem. Often, these third-parties are

unwilling to sign Health Insurance Portability and Accountability Act (HIPAA) business associate agreements (BAAs), and/or resist acceptance of appropriate levels of liability that recognize the great amounts of data and protected health information (PHI) they process and maintain. The current landscape of consumer AI applications remains largely unstructured, creating a highly unpredictable environment with significant data security and sovereignty implications.

In the absence of clear direction from this Administration, there is a substantial risk that consumer data may be stored, processed, or transmitted in jurisdictions with inadequate protections or misaligned regulatory standards. This includes the potential for sensitive data to reside in offshore data centers, including those located in regions such as China, where data access and oversight mechanisms does not align with U.S. privacy and security expectations.

Addressing these vulnerabilities requires a more structured approach to ensure data integrity, security, and compliance with established legal and ethical standards. **If we are to make meaningful improvements in our sector, this responsibility must be equally shared with those selling AI tools and solutions, and cannot be borne alone by providers.**

A primary concern for members is related to where the data goes when a hospital or healthcare system engages the AI engines – does it just stay within the specific process, or does it get captured and included within the algorithm to help improve the models? We have heard that some vendors have tried to use existing language in their contracts to essentially steal our members' data sets to pilot their AI models. The existing legal framework is not sufficiently equipped to address the complexities of AI-driven data security challenges, particularly in cases of data theft and unauthorized access.

As AI technologies continue to evolve, the absence of clear legal parameters creates significant uncertainty regarding liability, enforcement, and redress mechanisms. **Accordingly, an AI Action Plan that provides clarification on the limitations and legal implications of data theft could serve as a critical step toward establishing greater regulatory certainty, enhancing risk mitigation strategies, and ensuring the responsible development and deployment of AI systems.**

Further, when negotiating contracts with AI companies – or restructuring existing contracts – some of our members have found that they have had to undertake substantial risk management, data governance, and data hygiene efforts, and then reexamine existing contracts. Many offerors of AI tools and solutions do not give them the option to "opt-out." This limits innovation by placing unnecessary restrictions on the use of potentially valuable tools, preventing their safe and responsible integration. As a result, it hinders technological progress and the ability to fully leverage these tools to improve outcomes while maintaining security and compliance.

For example, there have been ongoing issues with being unable to completely turn off a chat-powered AI assistant within a hospital because it's part of the overall software

package. They are concerned that if an AI tool is capturing their data, and that data leaves their organization – they have no method of knowing where it is going, how it is being used, and/or if it might be re-released for other (potentially non-HIPAA compliant) purposes. The current regulatory landscape heavily penalizes the provider in these situations that are difficult for them to control.

AI has been an integral component of healthcare technologies for decades, playing a critical role in enhancing clinical decision-making and operational efficiencies. One notable example is its longstanding application in radiology, where AI-driven algorithms assist healthcare professionals and clinicians by augmenting diagnostic accuracy, streamlining workflows, and improving patient outcomes. **These advancements underscore AI's established presence as a supplementary tool that enhances, rather than replaces, the expertise of clinicians and medical practitioners.**

With the advent of large language models (LLMs), there has been a proliferation of new AI tools to the market as well as increased marketing claims and hype. While many organizations do model validation on their own data for vendor supplied tools, we have heard a wide array of concerns from members regarding predatory sales practices of AI vendors' tools and solutions. For example, a common sales tactic/selling point is that the tool will "save 10 minutes of time per patient," or guaranteeing "more clinician time with patients"; often these claims are made without proof of concept.

When it comes to purchasing an individual AI tool, everything is proprietary. Hospitals could simply, as one member stated, "be buying a bill of goods." **There is a considerable gap between companies that claim to have AI capabilities and those that actually show real, AI-powered outcomes.**

CHIME members find that many of the sales and marketing teams of AI tools will not offer demonstrations of the capabilities of their tools, and are often unwilling to bring the engineers into meetings. Further, as one example, a member noted that the "development" sales teams will market to the physicians or others in their organization in an attempt to go around the governance structures that have been created to protect the organization and limit risk.

There are – of course – many pressing issues that CHIME members face as they approach the appropriate use of AI in their hospitals and healthcare systems. Change management involves overcoming resistance to AI adoption among healthcare professionals and managing the cultural shift required for successful AI integration. They encounter significant challenges in ascertaining when modifications to software by vendors may have downstream implications for the responsible deployment of AI—such as instances where a coding tool integrates AI functionality through an update without adequate disclosure.

Furthermore, they face substantial network bandwidth constraints and heightened cybersecurity risks, particularly when AI-enabled tools are introduced into an organization's ecosystem without proper oversight (i.e., when they are used

unknowingly by patients and/or healthcare professionals). Notably, there have been documented cases in which such AI tools have served as the attack vector for cybersecurity incidents, underscoring the necessity of rigorous governance and risk management frameworks.

Our members who are using AI are moving deliberately to establish guardrails to encourage thoughtful evaluation and implementation of AI technology in the appropriate use cases in which they can understand the potential risks and benefits. **CHIME members must continually address concerns surrounding AI decision-making in healthcare and manage patient trust and consent in these AI-assisted care situations.**

Hospitals and healthcare systems at the forefront of AI in healthcare must prioritize use cases, which involves identifying high-impact areas for AI application and balancing clinical and operational AI use cases. Our members are dedicated to developing comprehensive AI education programs, including prompt training, for and with their medical staff, and must balance technical knowledge with practical application in these clinical settings.

Without any significant reduction in burden on clinicians across the care continuum, the current urgent clinician burnout and workforce shortage that our country is facing will continue to grow. Our members are dedicated to best practices in EHR and AI implementation, prioritizing safety and effectiveness. They take their responsibility to protect the privacy, security, and accuracy of patient data – and, most importantly, the overall safety and well-being of their patients – very seriously.

Additional Recommendations

The Centers for Medicare and Medicaid Services (CMS) and Office of Inspector General (OIG) could consider further amending the regulations to the Stark Law and the Anti-Kickback Statute and Beneficiary Inducement Civil Monetary Penalty Law to include permitting donations of AI tools, and further ease the cybersecurity technology and related service donations provisions.

While the Cybersecurity Exception and Safe Harbor and the EHR Exception and Safe Harbor offer hospitals and other donors a valuable pathway to protect their systems through donations to connected recipients – further updating these regulations should be considered to enhance their effectiveness and adaptability. **We believe this would help to bridge the innovation and implementation across the care continuum, and across the "have and have nots."**

The Cybersecurity Landscape and National Security

The Health-ISAC 2025 Health Sector Cyber Threat Landscape[1] highlights a continued escalation of cyberattacks, with the top impact on HDOs reported as: "Disruption in the

[1] Annaloro, J. (2025, February 21). *Health-ISAC 2025 Health sector Cyber threat landscape*. Health-ISAC - Health Information Sharing and Analysis Center. https://health-isac.org/health-isac-2025-health-sector-cyber-threat-landscape/

normal operation of medical technology, including such things as loss of diagnostic technology or loss of access to electronic medical records which may cause delay and disruption to patient care, such as diversion of patients and ambulances, canceled surgeries, or the need to revert to manual procedures."

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. This poses an imminent risk to our national defense. Put simply, cybersecurity is national security. We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals.

Privacy of healthcare data is not possible without security. Hospitals and healthcare systems are spending an increasing amount of time, energy and resources navigating this highly challenging and evolving environment. **Our 2024 Digital Health Most Wired (DHMW) Survey (DHMW) survey shows that over the past several years, security has maintained the position as the highest priority for digital investment – with 99% of respondents stating that "Security" is essential or high priority. The survey encompasses nearly 48,000 facilities, including acute care, ambulatory, and long-term/post-acute care settings. Organizations surveyed are also increasing their financial commitment to IT, with average budget allocations for IT systems and initiatives nearly doubling year over year.**

Therefore, CHIME respectfully requests that the Trump Administration consider the increasingly complex cybersecurity landscape hospitals and health systems must navigate, and we are hopeful that you will keep this in mind when crafting the AI Action Plan. **CHIME members are focused on safeguarding against AI-specific cybersecurity threats. AI holds significant promise in ways it can assist the sector to take a more proactive posture against cyber threats. However, we are aware that cyber criminals are also using these tools to their advantage – and weaponizing AI.**

With these tools, cyber criminals can make phishing attacks look more authentic, and custom malware code will become available to more criminals, expanding their capabilities. We are on notice and have been warned that AI/ML systems can be manipulated by malicious actors who can confuse or "poison" AI systems to make them malfunction and several attacks against healthcare applications have already happened.

Hospitals and healthcare systems are spending an increasing amount of time, energy and resources navigating this highly challenging and evolving environment. Cybersecurity challenges and threats that our members are facing are what those who have been active in the cybersecurity landscape have known for years – healthcare is under constant threat and more resources are needed for healthcare providers.

The budget and resources our members would need to allocate to comply with any new regulations are valuable funds and assets that could otherwise be directed toward critical investments to enhance hospital and healthcare systems'

cybersecurity posture and innovation. Any relief of regulatory burden or investments in cybersecurity and AI, for or by the healthcare sector, will be an investment not just in patient safety – but also national security.

Conclusion

CHIME deeply appreciates the opportunity to respond to this RFI. We are hopeful that the Trump Administration carefully considers the following critical priorities in the development of the AI Action Plan: ensuring patient safety and privacy, reducing regulatory burden, establishing clear and consistent regulatory oversight, fostering responsible innovation, maintaining affordability, strengthening cybersecurity, achieving administrative efficiencies, and advancing workforce education. **Additionally, we emphasize the importance of leveraging the AI Action Plan to bridge the widening digital divide, particularly for providers serving rural, small, and under-resourced communities.**

As the Administration solicits and evaluates public input to shape the AI Action Plan, CHIME and its members stand ready to serve as a strategic resource. Our members—comprised of executives and senior healthcare IT leaders—bring decades of expertise at the intersection of healthcare and technology, including firsthand experience managing the complex implications of AI adoption and responding to cybersecurity threats. Their insights are invaluable in crafting policies that balance innovation with risk mitigation and operational feasibility.

We welcome ongoing collaboration and look forward to serving as a trusted stakeholder and resource to the Administration throughout and beyond the development of the AI Action Plan.

Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME