CHIME

DIGITAL HEALTH LEADERS

CHIME AI PRINCIPLES

JULY 2024

EXECUTIVE SUMMARY

The deployment of artificial intelligence (AI) in healthcare is brimming with promise, heralding in a transformative era in patient care. However, this potential can only be realized with thoughtful implementation and robust safeguards to ensure trust among patients and providers. The federal government plays a crucial role in creating an environment that enhances patient care and supports healthcare providers.

With over 5,000 members across 60 countries, the College of Healthcare Information Management Executives (CHIME) is the premier professional organization for senior-level digital health leaders worldwide. We empower our members and industry partners to collaborate, grow professionally, and advocate for effective information management. Together, we are advancing the future of health and care for all.

As AI accelerates changes in the healthcare system, CHIME members are on the frontlines navigating this dynamic landscape. CHIME is uniquely posed to lend our voice and thought leadership by supporting policymakers as they chart a responsible path forward that supports care delivery while fostering innovation.

Patient safety remains paramount, necessitating vigilant oversight to prevent AI from inadvertently compromising care. Simultaneously, AI's potential to reduce provider burnout and improve efficiency promises substantial savings, both in time and financial resources. However, regulatory frameworks must avoid exacerbating the administrative load on healthcare professionals.

Innovation must be allowed to thrive with a culture that values research and high-quality patient care. Monitoring AI to eliminate bias and discrimination is crucial for equitable healthcare delivery. Key policy changes are needed to support patient privacy and federal funding for cybersecurity will help maintain trust in these technologies and protect against emerging threats.

Enacting lasting and flexible telehealth and high-speed broadband policies across the entire country is essential to harness AI's full potential without exacerbating the digital divide. Lastly, collaboration among providers, clinicians, technology giants, educators, policymakers, and other critical stakeholders is vital to navigate the evolving landscape of AI tools and labor demands, ensuring affordability and education keep pace with innovation.

Following months of input by our members, we have laid out ten principles combined with multiple recommendations that, if adopted, will ensure the appropriate level of oversight and support for providers and patients is met in this era of transformation.

1. **Patient Safety:** Patient safety must remain a top concern, and it is crucial that the use of AI does not lead to worse health outcomes than if it were not used.
2. **Administrative Efficiencies:** Investments in AI tools designed to improve our sector's efficiency could result in significant savings in time and cost.
3. **Regulatory Oversight:** Regulatory oversight is needed; however, it should not result in duplicative mandates or worsen administrative burdens on providers and clinicians.
4. **Innovation & Research:** AI tools and applications that help reduce provider burnout, including both administrative and clinical, foster a culture of innovation, and uphold high standards for patient care must be prioritized.
5. **Discrimination, Bias & Equity:** Monitoring of AI performance to prevent discriminatory outcomes and enhance fairness in healthcare delivery is needed.
6. **Affordability:** The federal government should help ensure that the use of AI does not result in a larger divide between the digital haves and have-nots.
7. **Privacy:** Patient data privacy and security are paramount in healthcare, and the burden for protecting patient data must be a shared one.
8. **Cybersecurity:** AI holds significant promise insofar as it will help providers take a more proactive posture against cyber threats. However, it bears a significant financial cost; national investments in cybersecurity for providers is needed. Unfunded mandates will only set providers back further.
9. **High-Speed Broadband:** Expanding nationwide high-speed broadband is crucial for harnessing AI tools and reducing healthcare disparities across the U.S.
10. **Education & Workforce:** Support by large technology companies, educators and policymakers is needed to manage the use of these new tools and the changing labor demand.

DETAILED RECOMMENDATIONS

1. PATIENT SAFETY

Everyone is a patient, and every patient deserves to receive care that best supports their individual healthcare needs. A "one-size fits all" policy approach to AI which is entirely sector agnostic is unlikely to best support patient needs. Its use in healthcare settings requires an added level of expertise and consideration, as patient care outcomes and lives are at stake.

Patient safety must remain a top concern, and it is crucial that the use of AI does not lead to worse health outcomes than if it were not used. If AI is appropriately developed and applied, it holds the potential to personalize and enhance the delivery of patient care and potentially improve patient outcomes.

Recommendations:

- An added level of deliberation by policymakers is needed when it comes to AI in the healthcare sector, given the potential to negatively impact patient care outcomes and lives.
- A "one-size-fits-all" law and/or policies and oversight that fail to consider the uniqueness of the healthcare sector should be avoided. Policymakers must avoid enacting redundant, industry-agnostic legislation and regulations that unduly hinder American AI innovation.

- Several healthcare delivery organizations (HDOs) have AI Councils, acceptable use, and/or governance policies established within their organizations. These existing frameworks are intended to enable responsible, ethical, and effective advancements in health AI on behalf of the patients and communities they serve. Any new federal policies must consider that these frameworks – created to protect patients – are often already in place and should be sufficiently nimble to accommodate unique HDO needs.
- AI tools must prioritize safety for the betterment of patient care and should only be used to augment clinical decision-making processes, not replace human judgment. They are not a substitute for a healthcare professional's judgment, or patient's values and preferences.
- Federal agencies must pass rules that ensure appropriate, safe and certified use of AI algorithms ensuring removal of data bias within the algorithms and equitable care for all.

2. ADMINISTRATIVE EFFICIENCIES

According to the National Health Expenditure Accounts (NHEA), the share of gross domestic product (GDP) devoted to healthcare was 17.3 percent in 2022 and is estimated to increase by more than 5% between 2022-2031. The average growth in NHEA is projected to outpace the average GDP growth (4.6%) resulting in an increase of the health spending share of GDP from 18.3% in 2021 to 19.6% in 2031.

Several experts have posited that significant savings can be achieved in healthcare by addressing administrative and often labor-intensive processes. McKinsey has studied the issue of administrative simplification and found that a quarter of healthcare costs – or $265 billion - could be saved annually with greater efficiencies. Specific to administrative use of AI, McKinsey concluded AI-enabled prior authorization (PA) "can automate 50 to 75 percent of manual tasks, boosting efficiency, reducing costs, and freeing clinicians at both payers and providers to focus on complex cases and actual care delivery and coordination."

Whereas clinical tools can take years for clinicians to adopt into practice, uptake of administrative AI tools often don't require clinical acceptance suggesting a shorter period in which these tools will be widely used by HDOs. CHIME's own 2023 Digital Health Most Wired (DHMW) survey for example, found the majority of HCOs report having some level of experience in using AI for clinical workflow purposes, though most present as just "dipping their toes" in the AI waters at this point in time. It stands to reason that investments in AI tools designed to improve our sector's efficiency could result in significant savings in time and cost.

Recommendations:

- Regulators should explore ways to leverage AI to increase administrative efficiencies among providers.
- Policymakers should consult with healthcare stakeholders including chief information officers (CIOs), chief information security officers (CISOs), and other senior health IT leaders in HDOs that are purchasing, deploying and using these tools in care settings to support efficiencies in healthcare delivery. This will help ensure that new and future changes to federal laws and regulations are feasible and do not worsen administrative burden on providers and clinicians.
- Lawmakers should appropriate funds to support investment in AI tools designed to improve efficiencies in the healthcare sector and support providers across the entire continuum of care.
- Additional attention is needed to support adoption of AI tools among safety-net and under-resourced providers.

- Federal agencies should consider development of safe and free "public good" AI algorithms (example: AI algorithms to expedite CMS Medicare reimbursement in order to facilitate the reduction of burden for healthcare organizations).

3. REGULATORY OVERSIGHT

Regulatory oversight is needed. However, it should not result in duplicative mandates or unnecessarily increasing administrative burdens on providers and clinicians. Healthcare providers are struggling to stay afloat in the current economic climate, a situation that is made more dire by unprecedented challenges related to a shrinking workforce and service and payment interruptions stemming from cyberattacks.

As AI evolves in the way it is applied in healthcare, liability concerns are growing surrounding what responsibility providers and clinicians should have to shoulder when they augment care delivery with the use of AI tools, and there is an adverse patient outcome. Further, if the use of AI is unrelated to an adverse outcome, it is unclear how this will be mitigated; there is no protection or case law offering guidance to assist healthcare providers regarding legal liability, especially individual clinicians.

Recommendations:

- All efforts must be made to minimize duplicative mandates when addressing the use of AI for purposes of health and care.
- Oversight over AI by the Food and Drug Administration (FDA) and the Office of the National Coordinator (ONC) use must be tightly coordinated. Tools that are already regulated and that are in widespread use today – including those under the FDA's "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions" Draft Guidance, "Clinical Decision Support Software" Final Guidance, and "Software as a Medical Device (SAMD): Clinical Evaluation" Final Guidance," should not be subjected to additional oversight without more research, or at the very minimum pilot testing.
- The FDA publishes and provides a list and insights of AI/ML-enabled medical devices marketed in the U.S. as a resource to the public about these devices and the FDA's work in this area. As of May 2024, the FDA has reviewed and authorized nearly 880 devices with AI/ML across many different fields of medicine (marketed via 510(k) clearance, granted De Novo request, or premarket approval) – and expects this trend to continue.
- ONC oversight around predictive decision support interventions (predictive DSIs) should be tested before being mandated across all providers and certified EHRs, otherwise investment and innovation could be stymied. Congressional oversight surrounding these policies is needed.
- ONC should create a new, semi-permanent subcommittee under the HITAC to focus on implementation of predictive DSIs.
- Until key issues are resolved around FDA and ONC oversight, is premature to tie Medicare payment policies to the use of predictive DSIs in certified EHRs.
- Adequate timeframes for implementing any AI mandates (i.e., those included in ONC's HTI-1 final rule) must take into consideration competing mandates and allow sufficient time for vendor development and provider implementation.
- Algorithmic transparency is needed for commercially developed and sold products.

- The burden for adverse outcomes stemming from the use of AI should not be unilaterally borne by clinicians and providers.
- New policies should not hinder HDOs' ability to leverage significant IT investments – including AI tools – which can support safer and higher quality care.

4. INNOVATION & RESEARCH

AI technology is rapidly evolving, and the clinical evidence base is still emerging. Comprehensive research, shared via peer-reviewed journals, and made widely available to providers is needed. Common definitions are needed to foster a shared understanding across diverse applications within the healthcare sector to support research and promote consistency.

Additional innovation partnerships between industry and federal partners are needed – and they must be fostered. For example, the Industry–University Cooperative Research Centers (IUCRC) program accelerates the impact of basic research through close relationships between industry innovators, world-class academic teams, and government leaders.

AI tools and applications that help reduce clinical burnout, foster a culture of innovation, and address high-priority use cases are needed. This work could be built on HHS' own AI use cases. Before widespread federal policies and mandates are placed on healthcare providers around the use of AI, more research is needed. Algorithms must also be validated, tracked and cataloged for reference by providers and the processes for this must not fall entirely to providers.

Recommendations:

- HHS should work collaboratively with the industry to foster a culture of innovation and safety.
- The HHS AI Safety Taskforce should consult with a wide array of healthcare stakeholders including clinicians and healthcare providers. HHS should work with healthcare stakeholders to establish use cases for AI that can be pilot tested by providers.
- Use cases should focus on high-priority areas that address clinician burnout, administrative efficiencies, common disease states (i.e., opioid use disorder), improve care outcomes (i.e., transitions of care), and advance the cybersecurity posture of providers.
- Federal agencies must work with healthcare stakeholders – specifically, users of AI – to establish collaborative efforts aimed at developing and disseminating standardized definitions of AI and ML.
- Lawmakers should fund comprehensive research and development resulting in open source or low-cost AI technology that can be deployed by providers.
- Existing programs like IUCRC should be leveraged and further funded in order to cultivate and conduct the crucial, high-impact research to meet shared and critical needs regarding the use of AI in healthcare.
- A validation process is needed for vendor-developed algorithms which have been approved. The burden for validating algorithms should not fall unilaterally on providers.
- A central repository to track validated / approved algorithms (i.e. registry or clearinghouse) should be stood up and in place for at least three years which can be referenced by HCOs.
- Additional federal support will be needed to ensure all patients – no matter where they live – have access to high-quality care supported by AI.

5. DISCRIMINATION, BIAS, EQUITY

Addressing bias is easier said than done, and providers are learning. Bias is often "baked into" underlying systems like electronic health records (EHRs) and technologies like pulse oximeters, infrared thermometers, x-ray radiation, and other medical devices and are calibrated using populations that were not diverse. Providers, medical specialty groups, patient groups and others are actively working to address these biases.

Ongoing efforts to identify and address bias in AI algorithms and ensure that these systems are trained on diverse and representative datasets are needed. The implementation of AI in healthcare should not be a one-time event but rather an iterative process. Continuous monitoring of AI performance to prevent discriminatory outcomes and enhance fairness in healthcare delivery is needed.

Recommendations:

- Efforts to root out bias in AI and address equity concerns should be done in collaboration with healthcare providers, researchers, patient community advocates, and developers to share and maximize transparency, share learnings, and foster continuous improvement.
- Patient care needs should drive the use of AI, not the reverse.
- AI systems should be trained on diverse and representative datasets.
- AI tools and solutions must be audited to ensure they are performing as intended and can be validated.
- Audits must be performed by independent auditors or third-parties.
- HHS must ensure the Trusted Exchange Framework and Common Agreement (TEFCA) facilitates responsible and secure data sharing across the country in order to allow for representative datasets.

6. AFFORDABILITY

Most providers do not have the vast resources to purchase and deploy cutting edge AI tools and applications. Many remain financially stretched and are still wrestling with workforce shortages – especially for health IT employees. Small and under-resourced providers will need additional support adopting AI to prevent widening the digital divide.

Federal support is needed to help encourage and expand treatment options for patients residing in underserved areas, and those cared for by resource-strapped providers. CHIME's 2023 DHMW survey data clearly finds that the use of AI varies by size of the organization. Arguably facilitated in part by the presence of dedicated, specialized data analytics leaders in larger HCOs, the DHMW findings suggest the AI divide in HCOs may grow exponentially as the divide in analytic leaders grows.

Recommendations:

- The cost of using AI solutions should be built into the cost of doing business for healthcare providers and clinicians and should be supported by reimbursement policies and should not increase the cost of delivery of care to the patient.
- The federal government should lead on establishing reimbursement which supports the use of AI that is designed to enhance efficiencies, improve patient care and, protect patient data.
- Federal support will be needed to help neutralize treatment options for patients residing in underserved areas and those cared for by resource-strapped providers.
- Policymakers should explore reforming the Stark and Anti-kickback laws and policies to accommodate donations of AI tools to improve access and reduce the potential for a growing digital divide.
- Larger healthcare organizations that donate AI should receive credit for doing so and it should count towards meeting their not-for-profit status.

7. PRIVACY

Patient data privacy and security are paramount in healthcare and the burden for protecting patient data must be a shared one. The amount of healthcare data is increasing with each passing year. One estimate has pegged the compound annual growth rate (CAGR) for healthcare data as reaching 36% by 2025, a rate higher than the manufacturing, finance, and media sectors. The existence of more data means more data is at risk. A significant amount of data now lives outside of the protections of the Health Insurance Portability and Accountability Act (HIPAA) however, risks exist to the privacy of data whether it is governed by HIPAA or not.

Even when health data is de-identified, when it is aggregated with other data identity can be easily reestablished. AI products using de-identified data in an attempt to reduce bias have the potential to inadvertently create privacy risks such as reverse-engineering data to re-identify individuals.

Recommendations:

- The U.S. needs a comprehensive national data privacy law to better protect consumers' sensitive health information and inform consumers of how their data is being permissibly used.
- The Federal Trade Commission (FTC) is the primary federal agency responsible for protecting consumers' privacy and security and their funding should not be predicated on the passage of a national privacy law. The Commission should be adequately funded to help ensure that health data not governed by HIPAA is protected.
- Any AI tools and applications used in healthcare settings must comply with all relevant privacy and security regulations and guidelines.
- Ongoing review is needed to ensure de-identified data used to train AI models are not creating privacy risks.
- Developers and vendors must develop tools with a privacy and security-first mindset and implement robust data protection measures, data anonymization techniques, and access controls to safeguard patient information from unauthorized access and breaches.

8. CYBERSECURITY

Privacy of healthcare data is not possible without security. Cybersecurity attacks are on the rise for providers of all sizes, which pose a direct threat to patient safety and to national security. The overall privacy and cybersecurity landscape has become infinitely more complex for the entire healthcare ecosystem. Even the most sophisticated and well-funded healthcare entities are not impervious to cyber-attacks financed by hostile nation-states and supply chain attacks have disastrous outcomes. Patients need to trust the technology they are using. The only way to do that is through an investment in cybersecurity.

AI holds significant promise insofar as it will help us take a more proactive posture against cyber threats. However, we are aware that cyber criminals are also using these tools to their advantage. HHS' Cyber Command Center, HC3, outlined how AI can be weaponized. In their 2023 Healthcare Cybersecurity Year-in-Review and 2024 Lookahead they explain that generative AI and large language models (LLMs) will rapidly change and continue to impact healthcare cybersecurity. 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. The National Institute of Standards and Technology (NIST) has also warned that AI/ML systems can be manipulated by malicious actors who can confuse or "poison" AI systems to make them malfunction and that several attacks have against healthcare applications have already been demonstrated.

Third-party risk remains an enormous weak spot for the healthcare sector and cannot be solved by imposing costly mandates on providers. Third parties that store, process and/or transmit protected health information on behalf of HIPAA covered entities are critical to the healthcare sector; yet they routinely shift millions of dollars of liability for a cybersecurity breach back to HDOs during contract negotiations. If we are to make meaningful improvements in our sector, this responsibility must be equally shared and cannot be born alone by providers.

Efforts to improve the posture of our sector will take a concerted effort by all. As we navigate emerging technologies like AI, lessons can be learned from partnerships our sector has fostered under the public-private partnership of the Health Sector Coordinating Council's (HSCC) Joint Cybersecurity Working Group. CHIME continues to strongly support the best practices jointly developed under this partnership which stems from a mandate in the Cybersecurity Information Sharing Act of 2015 under Section 405(d).

Recommendations:

- Given the interconnected nature of the healthcare system, the risk cyber-attacks already pose to patient safety, and the totality of the impact a cyber-attack could have on algorithms used in healthcare settings, investments are needed to foster both defensive and offensive postures.
- Congress should appropriate funding to help providers improve their cybersecurity posture, support their adoption of the cybersecurity best practices, and increase HHS funding to support cybersecurity education and outreach to providers on emerging technologies.

- Congress should immediately appropriate grants to HDOs to help offset the costs of purchasing the hardware, software, licensing and expertise needed to secure their environments and protect their patients from the theft of their data stemming from rising cyber-attacks. Providers who are under-resourced ones and those caring for underserved communities who are in dire need of federal grants should be prioritized.
- A longer-term incentive program for all providers is needed to help them make greater investments in cybersecurity and to adopt cybersecurity best practices including the Cybersecurity Performance Goals (CPGs) announced by HHS. Any federal provider mandates related to meeting cybersecurity standards and practices must occur in lockstep with the federal funding so as not to further burden an already deeply-workforce strained system or be unduly punitive. Unfunded mandates will only serve to punish patients as HDOs will be further inhibited in their ability to make needed cybersecurity investments.
- Policymakers should require minimum cyber standards for all third-party entities providing any services in healthcare (i.e., EHRs, medical devices and applications).

9. HIGH-SPEED BROADBAND

As the pace of AI innovation and expansion increases, the appropriate infrastructure will be needed to support it. There are still pockets of the U.S. without broadband access. Almost 90 percent of rural broadband provider members of NTCA - The Rural Broadband Association reported locations missing in the Federal Communication Commission's (FCC) broadband database.

While there have been recent breakthroughs related to accessing AI without broadband, many models still demand it. AI cloud storage needs are pervasive requiring access to high-speed internet. AI applications around telehealth are also increasing and remote patient monitoring and hospital and home demand broadband connections.

Continuing to expand nationwide high-speed broadband is crucial for harnessing AI tools and reducing healthcare disparities. To the degree that there are broadband access gaps, this will further impede use of AI and worsen the digital divide.

Recommendations:

- Congress should continue their efforts monitoring and addressing areas of the country still lacking broadband access.
- Congress should reauthorize the Affordable Connectivity Program.
- Lawmakers should permanently extend the Medicare telehealth flexibilities established during the pandemic.
- Policymakers should carefully monitor the impact of AI use and its impact on digital divide and care outcomes.
- Providers, federal authorities, broadband carriers and satellite internet providers should be convened to collaboratively address and rectify persisting broadband gaps to improve access to AI for all patients nationwide.

10. EDUCATION & WORKFORCE

Hospitals create 50 petabytes of data annually but only a small fraction of it is used, according to the World Economic Forum. Tapping into this trove of data could help improve patient outcomes and leverage workflow and administrative efficiencies. AI holds enormous potential to synthesize this data into actionable intelligence, yet, education and an adequately trained workforce is needed to support this new era of augmentation and automation. There are vague estimates around the impact AI will have on workforce and present day workforce shortages continue to create challenges for HDOs. Workforce shortages in rural and underserved areas can be even more pronounced.

Positioning the healthcare sector - the largest employer in the U.S. - and our nation as an AI leader requires a well-trained and upskilled workforce. This must, however, be balanced against the need for a strong employment rate and economy, avoiding significant job displacement, and exacerbating existing inequities. Support by large technology companies, educators and policymakers is also needed to manage this disruption and the changing labor demand.

The goal of AI should not be to eliminate human involvement in healthcare delivery. Rather, AI should be leveraged to enhance the care provided by clinicians. This will require education so that patients are aware of how AI is being used in care delivery. Additionally, the need for education and training must be a shared one between HDOs and AI companies; once again the burden should not rest solely on providers.

Recommendations:

- Industry, educators and policymakers must work together to ensure the American healthcare workforce and education system is well-positioned to absorb the changes surrounding AI.
- Congress should mandate a national strategy be established to outline a roadmap for AI needs in the healthcare sector.
- The focus of AI training and retraining related to patient care should focus on helping clinicians augment care delivery, not replace the clinician entirely.
- Transparency is needed to allow for patient understanding related to how AI is being used to help facilitate their care.
- Subsectors within the healthcare system that are already behind in IT adoption (i.e. small, under-resourced, and those that did not qualify for HITECH funding for electronic health records) should receive additional support.
- Large technology companies should be encouraged to invest in and launch new education programs to help feed a steady supply of IT savvy workers.
- Federal support is needed to help providers reskill their workforce.
- Novel retraining programs funded by the federal government should be pilot tested at hospitals and other healthcare settings that could serve as national models.

CHIME PUBLIC POLICY

WORKING FOR YOU IN WASHINGTON

The CHIME Public Policy team serves as the collective voice for our members, advocating on their behalf for digital health policies that improve the health and care in the communities they serve, and the patients they care for. With a strong presence in Washington, the team collaborates closely with members to offer educational and technical policy leadership to Congress, the White House, and federal agencies. Leveraging their extensive expertise in digital health and health IT policies, the team actively champions our members' interests, ensuring they are well-represented and informed on critical legislative and regulatory developments.

If you have any questions, comments, or would like to discuss the principles further, please contact CHIME's Public Policy team at policy@chimecentral.org.