NATIONAL ASSOCIATION OF Community Health Centers

March 14, 2025

Networking and Information Technology Research and Development (NITRD)
National Coordination Office (NCO) & National Science Foundation
Attn: Faisal D'Souza, Technical Coordinator
2415 Eisenhower Avenue
Alexandria, Virginia 22314

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

Dear Mr. D'Souza,

The National Association of Community Health Centers (NACHC) is the leading national membership organization dedicated to promoting Community Health Centers (CHCs) (also known as Federally Qualified Health Centers or health centers) as the Employer, Provider, and Partner of choice in all communities, as well as the foundation of the primary health care system in America.

Community Health Centers are the best, most innovative, and resilient part of our nation's health system. For nearly sixty years, health centers have provided high-quality, comprehensive, affordable primary and preventive care. In addition to medical services, CHCs provide dental, behavioral health, pharmacy, vision, and other essential health services to America's most vulnerable, medically underserved communities in urban, rural, suburban, frontier, and island communities. Today, health centers serve more than 32.5 million people at over 16,000 locations, ensuring patients receive the care they need and pay what they can based on a sliding fee scale.

NACHC maintains its role as the national voice for health centers and believes that high-quality primary health care is essential in creating healthy communities and preventing chronic conditions. The collective mission and mandate of NACHC and the 1,496 health centers nationwide is to close the primary care gap and provide access to high-quality, cost-effective primary and preventative medical care.

NACHC urges the Administration to develop an AI framework that helps health centers and their patients and ensures proper guardrails are in place. CHCs provide high-quality, economically efficient care that results in long-term savings to the healthcare system. Health centers utilize artificial intelligence in various administrative and clinical settings, which can free up staff for higher-value tasks, reduce costs, and improve overall financial and operational performance.

Our response reflects the varied landscape of AI adoption among health centers. Some actively leverage AI for efficiency, while others face significant barriers related to cost, compliance, and staff adoption. There is a strong demand for implementation guidance and technical support to facilitate AI adoption across health centers. Currently, CHCs are using AI to automate insurance eligibility verification to instantly check a patient's insurance coverage and benefits before their appointment, reducing claim denials and improving front-end collections. This technology gives patients a clearer picture of their out-of-pocket costs and leads to fewer surprise bills. Health centers also use AI to analyze provider notes and suggest accurate codes to ensure compliance and reduce coding errors while minimizing administrative burden on providers, thus improving patient care. AI also enhances claims before submissions to catch errors in coding, modifiers, and documentation, increasing clean claim

rates and speeding up reimbursements. Lastly, CHCs use AI to match bank transactions with recorded revenue and expenses to flag discrepancies in real-time. This approach eliminates tedious manual reconciliation and ensures accurate financial reporting, which is essential for CHCs operating on tight financial margins. NACHC believes health centers can use AI in more areas of operations, such as streamlining prior authorizations, improving denial management and appeals, automating patient billing and collections, predicting revenue and cash flow, optimizing workforce management, and utilizing AI chatbots for patient and administrative support. We believe that allowing more health centers to use artificial intelligence will help bring greater efficiencies to our healthcare system while maintaining high-quality care.

Unfortunately, there are several barriers health centers face when adopting AI tools. The monthly costs of some AI-powered scribing tools represent a challenge for health centers to afford. CHCs have also raised concerns about the lack of clear vetting criteria for AI products, making it difficult to determine safe adoption, and other health centers reported default AI integrations (e.g., Microsoft AI, Zoom AI (Read.ai)) that can complicate AI standardization. Additionally, some health centers have reported staff reservations and training needs when adopting AI tools. Providers accustomed to human scribes or traditional dictation methods may resist transitioning to AI-powered tools, and many health centers lack the internal expertise to implement AI effectively. Health centers request the Administration provide training on how to implement AI safely and measure its impact, as well as develop model policies and procedures to support ethical AI use in the clinical setting.

There are two main types of AI utilized: generative AI and predictive AI. Generative AI creates new content using data and can help automate tasks and streamline processes. Predictive AI, on the other hand, analyzes data to prognosticate future systems behaviors or events, identify patterns, and, based on the data, make recommendations and decisions.[1] We will be referring to both of these terms throughout the comment letter depending on the type of AI health centers are deploying to help with workflows within their health center or helping directly serve their patients. This RFI lists our recommendations within three categories: I. Risk of Exacerbating Bias Using Artificial Intelligence, II. Data Privacy and Security, and III. Access to AI-Powered Tools and Resources.

I. Risk of Exacerbating Bias Using Artificial Intelligence

NACHC agrees that artificial intelligence (AI) should be free from bias to ensure that the data being used in AI algorithms is sufficiently sourced and representative of a variety of patient experiences from various backgrounds to mitigate ideological bias. AI has the potential to revolutionize healthcare by enabling sophisticated analysis of vast datasets, transforming patient care, and streamlining administrative processes. However, AI also carries risks, including bias, and action standards are needed to ensure that AI in healthcare is safe, effective, and unbiased. The federal government should focus on building international leadership, fostering awareness, promoting transparency, and monitoring outcomes. Any actions by the federal government should balance the risks and benefits and set guardrails that continue to foster innovation within those guardrails. The federal government should facilitate the availability of more complete data sets. Doing so will lead to algorithms that are trained on data that is representative of more Americans and permit outcomes research by those employing AI. NACHC recommends that the National Science Foundation (NSF) utilize several existing models that have outlined transparency and safety guardrails to prevent AI algorithms from developing and exacerbating these ideological biases.

[1] https://www.ibm.com/think/topics/generative-ai-vs-predictive-ai-whats-the-difference

NACHC recommends the federal government adopt the National Institutes of Health's (NIH's) "FAIR" model for artificial intelligence and consider leveraging the National Institute of Standards and Technology (NIST) AI Risk Management Framework to mitigate bias in AI. The NIH FAIR Model supports good data management and reusability to advance discovery and innovation. The FAIR Guiding Principles (Findability, Accessibility, Interoperability, and Reusability) delineate requirements that allow data sharing for data reuse to be possible.[2] *Findability* requires rich published metadata that is both human and machine-readable and for the metadata to include a persistent unique identifier for the data. *Accessibility* requires that there is a clear protocol for accessing the data. This does not mean that all data must be freely downloadable, only that the process of gaining access to it is transparent. *Interoperability* requires that the data is represented in a formally defined format and can be integrated with other data. The data should also be in a format that can be accessed, modified, or analyzed by common analysis, storage, and processing tools. *Reusability*, the core of the FAIR model, requires that the data are in a domain-relevant data standard, that the conditions for usage are clear, and that the metadata provides sufficient attributes for meaningful reuse. In addition, data should be well-described so that they can be replicated and/or combined in different settings.[3]

These principles aim to guide data producers and publishers as they navigate the obstacles inhibiting good data management, helping maximize the added value gained by contemporary, formal scholarly digital publishing. The principles must apply to 'data' in the conventional sense and to the algorithms, tools, and workflows that led to that data. The current data ecosystem, therefore, appears to be moving away from centralization and becoming more diverse and less integrated, thereby exacerbating the discovery and re-usability problem for both human and computational stakeholders. This means greater data diversity, algorithm transparency, and ongoing monitoring and evaluation, which creates stronger, smarter, and less biased artificial intelligence.

Additionally, in collaboration with the private and public sectors, the National Institute of Standards and Technology (NIST) developed a framework to better manage risks associated with artificial intelligence. The NIST AI Risk Management Framework[4] (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. The framework equips organizations to think about AI and risk differently. It promotes a change in institutional culture, encouraging organizations to approach AI with a new perspective — including how to think about, communicate, measure, and monitor AI risks and its potential positive and negative impacts.

The AI RMF is divided into two parts. The first part discusses how organizations can frame the risks related to AI and outlines the characteristics of trustworthy AI systems. The second part, the framework's core, describes four specific functions — govern, map, measure, and manage — to help organizations address the risks of AI systems in practice. These functions can be applied in context-specific use cases and at any stage of the AI life cycle.[5] The AI RMF includes strategies to diversify training datasets, adjust algorithms, and continuously test models for fairness throughout their lifecycle to ensure trustworthiness in AI systems. The framework offers practical and actionable steps for mitigating AI bias, enabling organizations to build fairer and more inclusive AI models, ensure compliance with ethical and regulatory standards on fairness, foster transparency and accountability in AI decision-making, and promote greater public trust in AI technologies.

---

[2] https://www.go-fair.org/fair-principles/.
[3] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). https://doi.org/10.1038/sdata.2016.18.
[4] https://doi.org/10.6028/NIST.AI.100-1.
[5] https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial.

The private sector has also started to create governance, ethical, and practice standards for organizations developing and deploying AI. For example, in September 2023, CTA released voluntary standards[6] outlining ways to identify and manage AI bias in healthcare. These standards outline types of biases and suggest strategies to mitigate bias throughout the development process. Additionally, the Brookings Institute published the Critical Algorithmic Systems Classification (CASC).[7] The CASC aims to outline a flexible regulatory framework that protects civil and consumer rights and addresses the unique challenges of using AI without changing the structure of the federal government. As private sector AI efforts continue to evolve and mature, the healthcare industry and appropriate federal government agencies need to work together to consolidate and coalesce towards a set of common national standards that can be adopted consistently across organizations.

NACHC also recommends utilizing the Responsible AI Guide[8] published by the Coalition for Health AI (CHAI). This guide aims to ensure that AI technologies used in healthcare are reliable, safe, and effective, combining existing standards into a coherent framework and providing practical considerations for applying these standards in day-to-day operations. The guide emphasizes tangible considerations for all stakeholders involved in the health ecosystem, ensuring that AI implementation is fair, transparent, safe, and beneficial. A significant component of the guide is its lifecycle approach to AI development and deployment in healthcare. This approach begins with defining the problem and planning AI solutions, followed by the ethical and effective design of AI systems. Practical engineering and development phases ensure reliability and safety, which are comprehensively evaluated before deployment. A critical element of the Responsible AI Guide is the emphasis on independent review. This ensures that AI solutions undergo rigorous evaluation by external experts to maintain high safety standards, effectiveness, and ethical compliance. The independent review process is designed to build trust and credibility in AI solutions used in healthcare, fostering broader acceptance and adoption. The guide also includes a detailed focus on privacy and cybersecurity. It integrates the NIST Privacy Framework and Cybersecurity Framework to help organizations manage privacy and security risks effectively.

NACHC supports efforts to implement bias auditing tools and urges the Administration to consider using standards to ensure that AI technologies used in healthcare are reliable, safe, and effective. It is well known that AI systems trained on biased historical data can perpetuate and even amplify existing health gaps. There are several methods to train AI systems, including:

- In supervised learning, the AI learns from labeled data, while in unsupervised learning, the model identifies patterns in unlabeled data. This allows the model to identify anomalies to help us discover patterns that have been hidden from us. For example, an AI model trained through unsupervised learning might identify unusual patterns in health center patient data that indicate potential disease or health issues, aiding early diagnosis and personalized treatment planning.
- Another method, "Garbage In, Garbage Out" (GIGO), refers to the idea that the quality of an AI system's output depends on the quality of its input data. In healthcare, AI can be used to diagnose diseases from medical images, such as X-rays or MRI scans. Still, if the data the algorithm was

[6] https://www.cta.tech/Resources/Newsroom/Media-Releases/2023/September/CTA-Tackles-Bias-in-Health-Care-AI.
[7] https://www.brookings.edu/articles/a-comprehensive-and-distributed-approach-to-ai-regulation/#:~:text=The%20CASC%20enables%20a%20comprehensive,oversight%20regime%20for%20algorithmic%20systems.
[8] https://chai.org/responsible-ai-guide/.

trained on is poor or lacks variety, the system can easily misdiagnose the condition. This can have direct, adverse effects on health center patient care and outcomes.[9]

No data set will ever be complete or free of potential biases. Healthcare data can be particularly challenging, given the lack of integration across systems. Being transparent about potential bias in the data used to train AI, methods, and applications is an important step in mitigating unintended consequences. It is also possible to "tune" machine learning ("ML") models to have good bias so they work for specific communities that need intervention or support. While regulations may aim to prohibit algorithmic bias, these same types of rules could unintentionally limit the ability of health centers to use AI to identify health interventions needed for specific groups. Good bias is important in healthcare when targeting specific populations for care based on accepted standards. Medical decisions often need to be biased towards certain groups, such as age or gender, for appropriate treatments or screening. We advise against any regulations that could hinder this. **As the Administration considers what safeguards to protect underserved communities, they should be mindful of how limiting "good bias" could negatively impact these groups.**

NACHC urges the Administration to ensure that AI used in healthcare settings is trained on a wide array of representative datasets and provide formal guidance on appropriately vetting AI solutions to reduce data bias. For AI to function correctly, the data must be reliable and aligned with its intended function and methodology. Improving demographic data standards and collection will help create AI that serves more people and reduce bias in the data used to train it. If AI is trained on misrepresentative data, the algorithm is prone to reinforcing bias, leading to poor health outcomes, misdiagnoses, and lack of generalization.[10] Robust, accurate, actionable, and standardized demographic patient data is fundamental to advancing quality healthcare. Collecting consistent demographic data allows health centers to better identify differences in care and outcomes as well as understand the societal drivers of health, devise innovative solutions, operationalize telehealth, and measure the effectiveness of interventions for continuous improvement.

NACHC encourages the Administration to advance data interoperability to improve provider collaboration, enhance efficiency, and empower providers to make informed decisions. Having interoperable patient demographic data would allow health centers to collect and share information with other providers, with patient consent, to inform patient care, assist in population health management efforts, and effectively address gaps in care and health outcomes. An aligned data-sharing approach will enable healthcare entities to collaborate on common goals, track progress, and better serve communities. Consistent data standards will help address health factors, improve outcomes, and reduce the burden of collecting data on health centers. This data could also be used to develop and train AI to better identify and address potential gaps in health outcomes.

One of the most prominent examples of AI algorithms exacerbating biases in the healthcare industry is included in a 2022 Office of the Inspector General (OIG) report which found coverage denials during one week in June 2019 and found that, among those prior authorization requests that Medicare Advantage Organizations (MAOs) denied, 13% met Medicare coverage rules.[11] Nearly all Medicare Advantage enrollees are required to obtain prior approval, or authorization, for coverage of some treatments or services — something generally not required in traditional Medicare. The denials were

[9] https://shelf.io/blog/garbage-in-garbage-out-ai-implementation/.
[10] Norori N, Hu Q, Aellen FM, Faraci FD, Tzovara A. Addressing bias in big data and AI for health care: A call for open science. Patterns (N Y). 2021 Oct 8;2(10):100347. doi: 10.1016/j.patter.2021.100347. PMID: 34693373; PMCID: PMC8515002.
[11] https://oig.hhs.gov/oei/reports/OEI-09-18-00260.pdf

inappropriate because these services likely would have been approved under traditional Medicare rules.[12] Additionally, according to the same report, these denials can delay or prevent beneficiary access to medically necessary care, lead beneficiaries to pay out of pocket for services that are covered by Medicare, or create an administrative burden for beneficiaries or their providers who choose to appeal the denial.[13] For elderly health center patients, prior authorization denials present significant obstacles, compounding the challenges they already face in managing their health. For these patients, timely access to prescribed medications and treatments is crucial for effectively managing their conditions and maintaining their quality of life. However, when prior authorization requests are denied, elderly patients may experience disruptions in their treatment plans, leading to lapses in medication regimens or delays in accessing essential therapies. Such interruptions can exacerbate their chronic conditions, potentially resulting in disease progression, increased symptom severity, and a higher risk of complications. In fact, health center patients are growing increasingly complex, with nearly 32% of health center patients reporting that they suffer from a chronic condition.[14]

NACHC encourages the Administration to enforce guidelines to ensure that insurers consider relevant factors for each patient when making coverage decisions through artificial intelligence, which will significantly benefit MA patients. While we appreciate that CMS' Contract Year 2024 Policy and Technical Changes to the Medicare Advantage and Medicare Prescription Drug Benefit Programs final rule provides MA patients with certain protections regarding coverage denials based on the use of AI and algorithms, the rule still permits MCOs to use algorithms, AI, and related technologies to assist in making coverage determinations if certain factors are considered for each patient.[15] These include all medical necessity determination requirements[16] and circumstances based on the specific individual, including the patient's medical history, physician recommendations, and clinical notes. NACHC requests further progress be made to ensure MA patients are not being improperly denied care. Health center patients ages 65 and older are the fastest-growing age group – 11% of our patients – and are growing increasingly complex, with higher rates of chronic conditions. For this group of health center patients, denials can result in worsening health outcomes, increased pain and discomfort, unnecessary hospitalizations, and decreased quality of life. With nearly two million prior authorization requests for healthcare services being denied in 2021,[17] it is unclear if these factors were ever considered or if they will be in the future. For this reason, since MCOs are permitted to use AI algorithms, NACHC requests that the Administration take additional steps to ensure insurers consider the relevant patient-specific factors outlined above when making coverage determinations, thereby preventing any bias.

NACHC urges the Administration to develop frameworks or guidance that maintain transparency and explainability when using any type of AI for decision-support interventions. The Assistant Secretary for Technology Policy (ASTP), in the 2024 HTI-1 Final Rule,[18] established new "Algorithm Transparency" requirements[19] for AI and other predictive algorithms that are mandatory for all healthcare providers using certified electronic health record (EHR) technology (CEHRT) in delivering patient care. The Final Rule also established a regulatory approach requiring

[12] https://oig.hhs.gov/oei/reports/OEI-09-18-00260.asp
[13] Ibid.
[14] https://bphc.hrsa.gov/sites/default/files/bphc/data-reporting/2022-uds-manual.pdf
[15] https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07115.pdf
[16] 42 CFR § 422.101(c)
[17] https://www.kff.org/medicare/press-release/medicare-advantage-plans-denied-2-million-prior-authorization-requests-in-2021-about-6-of-such-requests/
[18] https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and.
[19] https://www.healthit.gov/sites/default/files/page/2023-12/HTI-1_Gen-Overview_factsheet_508.pdf.

transparency in the training data used in a model used for decision support interventions (DSI). This promotes responsible AI and enables clinical users to access a consistent baseline set of information about the algorithms and models they use for clinical decision-making and to assess them for bias, fairness, appropriateness, validity, effectiveness, and safety. ONC-certified health IT supports the care delivered by more than 96% of hospitals and 78% of office-based physicians around the country.[20] The changes will improve interoperability through more modern standards and newer versions of existing standards; assist partner agencies such as CMS and the CDC in fulfilling their missions through certified health IT; improve care delivery for clinicians and care experience for individuals by improving access to more interoperable data – consistently and reliably – for patient care and individual access; require greater transparency regarding the decision support interventions included in certified health IT.

II. Data Privacy and Security

NACHC supports many of the gold-standard technical and regulatory requirements in data privacy and security for implementing AI systems. However, we remained concerned about increasing vendor costs that CHCs will incur due to additional software and hardware security development requirements. We advocate for security standards that are internationally vetted and aligned with the Community Health Center mission, including the following:

- **Frameworks** come at no cost, unless it is explicitly stated as mandatory. We support several data security frameworks, including the FDA's Good Machine Learning Practice (GMLP) principles for developing and deploying safe, effective, and high-quality AI/ML models in healthcare[21] and the NIST Cybersecurity Framework. We also support the adoption of the HITRUST CSF (Common Security Framework), which is a widely adopted security and privacy framework in the United States healthcare industry that builds upon HIPAA and incorporates elements of other standards, including ISO 27001[22]; and zero trust architecture (ZTA), a security framework that assumes users and devices are untrusted by default.[23]
- **Encryption standards** are used every day and at no additional cost to the health centers. These encryption standards are all being used by most, if not all, certified electronic health record systems (CEHRTs) in the United States as required by the ONC/ASTP's 2015 Edition Cures Update and 2022 Cures Act Final Rule. NACHC supports the Advanced Encryption Standard (AES) with a 256-bit key length as the de facto encryption algorithm used for data at rest (stored in on-premises or in cloud servers)[24]; and Transport Layer Security (TLS) version 1.3 or higher for data in transit (used to encrypt data during transmission across networks) providing enhanced security and performance during transmission.[25]
- **Application Programming Interfaces (API) Interoperability Standards** are mandatory requirements for certified EHR products in the US before the end of 2025. The burden is on the vendor's side and generally does not impact health center costs because it is an industry and regulatory standard. NACHC supports Fast Healthcare Interoperability Resources (FHIR) based

[20] https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program.
[21] https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles
[22] https://hitrustalliance.net/hitrust-framework
[23] https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
[24] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf
[25] https://datatracker.ietf.org/doc/html/rfc8446

APIs with OAuth 2.0 for secure data exchange[26]; SMART App Launch 2.1.0, based on OAuth 2.0 for client applications to authorize, authenticate, and integrate with FHIR-based data systems.[27]

NACHC recognizes that data breaches in healthcare disproportionately affect low-income populations, leading to financial harm, identity theft, and erosion of trust, and recommends the Administration continue to bolster cybersecurity measures. A descriptive analysis of healthcare-related cyber breaches in the United States from 2011 to 2021 found that there were 3,822 breaches affecting 283,335,803 individuals, with 41.7% being hacking/IT incidents, the most common type of breach.[28] These individuals, including those served by CHCs, are particularly at risk due to limited resources for robust cybersecurity measures. A mixed-methods study highlighted that despite federal and state regulations, including HIPAA, the frequency and impact of data breaches have not significantly decreased. This study identified hacking or IT incidents as having the most significant impact on the number of individuals affected.[29] The financial harm from these breaches can be substantial, as evidenced by a case where a solo practice faced a $5.1 million ransom demand.[30] The erosion of trust is also a critical issue, as patients may become reluctant to share sensitive information, potentially impacting the quality of care. This evidence underscores the need for enhanced cybersecurity measures and policies tailored to protect these at-risk groups.

NACHC recommends that the Administration review requirements that will place extensive financial, administrative, and time-intensive burdens on health centers. Almost half of health centers use more than one electronic health record (EHR) system across their organizations. The vast majority use health information technology (HIT) and EHR data beyond direct patient care to provide quality improvement (99%), population health management (87%), program evaluation (77%), or research activities (27%).[31] CHCs do not utilize HIT or EHR data beyond direct patient care.[32] Health centers are committed to protecting our patients' sensitive data and have made strides towards improving our EHR and HIT systems to enhance service delivery. While health centers are dedicated to enhancing patient care through advanced technologies, they often face challenges such as financial constraints, limited training opportunities, and the complexities of integrating new systems.[33] CHCs are already doing everything they can to keep their data systems HIPAA-compliant while operating on razor-thin margins and fulfilling the specific obligations required by their Section 330 grant. Health centers should be allowed to protect ePHI and their networks using good data privacy practices that meet the needs of the complexity of their EHR systems without falling out of compliance due to unattainable requirements. CHCs have limited IT and cybersecurity full-time staff, mainly outsourcing their IT operations to third party vendors or organizations. About 58.5% of CHCs report having between one and five active HIT vendors under contract to help protect their patient data.[34] NACHC has concerns that rigid guidance from the Administration regarding data privacy using AI tools could cause undue financial and administrative burdens on health centers, hindering their efficiency.

NACHC recommends the Administration consider the financial, workforce, and technical challenges implementing an artificial intelligence plan with strict data security requirements will

[26] https://openid.net/specs/openid-heart-fhir-oauth2-1_0.html
[27] https://build.fhir.org/ig/HL7/smart-app-launch/app-launch.html
[28] https://pubmed.ncbi.nlm.nih.gov/37061434/
[29] https://pubmed.ncbi.nlm.nih.gov/39504550/
[30] https://pmc.ncbi.nlm.nih.gov/articles/PMC9870634/
[31] HRSA, UDS Data 2023.
[32] HRSA, UDS Data 2023.
[33] Ibid.
[34] Ibid.

have on safety-net providers. As we have mentioned throughout this letter, CHCs operate on thin financial margins, making large investments in data security infrastructure a challenge. The upfront cost to purchase, or sometimes co-lease, hardware supporting the latest security patches and encryption tools is not always attainable for health centers. Additionally, software that performs sophisticated security logging, audit analysis, and data encryption tools that are mostly "Software as a Service" (SaaS), making this a recurring cost that adds to the financial burden, potentially diverting funds and staff away from medical services or social programs health centers are already providing.

Additionally, only two-thirds of health centers report having a cybersecurity committee or leader, and 78.9% reported having 1-10 full-time equivalents (FTEs) supporting health IT. While CHCs maintain a dedicated staff, these IT teams are small and usually wear multiple hats, meaning health centers rely on third-party vendors and organizations to assist them in maintaining HIPAA compliance and securing their data. CHCs also lack the time, resources, and budget for regular, engaging training for all staff members. IT departments at CHCs rarely have the budgets to implement strong cloud-based backup and data contingency plans in-house. NACHC has concerns that stringent data security requirements could contribute to high IT staff turnover rates, further complicating access controls, interrupting consistent staff training, and potentially affecting contingency plans in case of a data breach.

III. Access to AI-Powered Tools and Resources

NACHC recommends that the Administration prioritize strategies that ensure access to AI-powered tools. There is currently a "digital divide" at risk of widening if AI innovations are primarily concentrated in well-resourced healthcare settings. The digital divide can be defined as a stark difference between people with access to technologies and the digital literacy to work with them and those without. This manifests in the healthcare landscape as differences in patient portal adoption, telehealth care access, or ability to use patient-facing practice management software, such as online appointment schedulers. This digital divide has led to splitting patient engagement strategies into those for older and younger patients. Yet, more research has illuminated that the digital divide is more nuanced. Some older adults may be excited and able to utilize telehealth, while a younger, potentially low-income, patient might not have the infrastructure to access it.[35] As the AI Framework is developed, NACHC encourages the administration to ensure that AI tools are placed in the hands of health centers that can help bridge the digital divide gap so that we can continue to help patients manage their health conditions.

NACHC recommends continued support for Health Center-Controlled Networks (HCCNs), which can help advance AI usage for health centers. HCCNs are groups of health centers working together to use health information technology (health IT) to improve operational and clinical practices. HCCNs help health centers leverage health IT to increase participation in value-based care by enhancing the patient and provider experience, advancing interoperability, and using data to enhance value. They provide specialized training and technical assistance to take advantage of economies of scale, including group purchasing power, shared training, and data analytics. In 2021, approximately 83% of federally funded health centers participate in an HCCN, an increase from approximately 73% over the past 3 years. That number is likely to be higher in 2025.

HCCNs also provide support services for sharing data through health information exchanges (HIEs) and APIs, as well as support services for data privacy and security. HCCNs have a long and successful

[35] https://www.techtarget.com/patientengagement/news/366585058/Is-the-Digital-Divide-the-Newest-Social-Determinant-of-Health#:~:text=The%20digital%20divide%20is%20the,inequities%20and%20ultimately%20health%20disparities.

track record for improving health center operations. They have developed infrastructures and expertise needed to support their mission-driven health center members in improving population health while reducing costs and prioritizing patient experience and care team well-being. HCCNs are a critical component to health center interoperability and to the successful, meaningful sharing and utilization of health center patient data. They know health centers' needs best, and that support will help them further refine their AI needs by providing training and technical assistance on new AI opportunities. NACHC appreciates HRSA's continued investment in HCCNs.[36]

We also ask the Administration to invest in the development and deployment of AI solutions specifically designed to address the needs of CHCs and their patients, including funding for pilot projects, infrastructure upgrades, and workforce training. To remain competitive and keep up with ever-changing technology, CHCs welcome opportunities to partner with agencies in the AI space. Pilot projects could be developed for CHCs along a continuum with different approaches for those that are advanced in their use and understanding of AI and those that are just beginning to use AI to bolster patient care. There have been many documented success stories of health centers using AI. For example, San Ysidro chose Kore.ai to deliver HealthAssist – an automated approach to call-center conversations for health providers. With the right training data from HRSA's Uniform Data System (UDS), their Electronic Health Records, and language learning sources in English and Spanish, the San Ysidro team felt Kore.ai could help them reduce operational costs and improve call-center response rates, patient scheduling, and appointment reminders. They also used recorded call center data to identify themes and create a "rules engine" to train Kore.ai. The abandonment rate and number of unassigned patients have dropped substantially, and now they're exploring how AI can help increase patient compliance. While the technology can still be refined, overall, San Ysidro has been happy with the ways AI supports their call center operations.[37] Pilot programs coupled with funding could help increase overall uptake of AI systems.

With rising technology costs, helping health centers acquire more advanced infrastructure will allow them to keep pace with the ever-advancing AI landscape. We also value any training programs that different agencies can offer health centers on AI. Specific workforce training programs offered by agencies on various AI tools would be helpful in growing our health center workforce AI-savviness. While health centers are dedicated to enhancing patient care through advanced technologies, they often face challenges such as financial constraints, limited training opportunities, and the complexities of integrating new systems.[38] Nearly 80% reported having 1-10 full-time equivalents (FTEs) supporting health IT. While CHCs maintain a dedicated staff, these IT teams are small and usually have multiple responsibilities. As part of the AI framework, we hope the Administration includes plans for training in AI systems to allow health centers to better grow in this space and more quickly adopt AI products to benefit our patients.

NACHC recommends that the Administration help foster partnerships between AI developers, academic institutions, and health centers to co-create solutions tailored to the unique challenges and opportunities of CHCs. As AI has become more ubiquitous, best practices have come out from AI developers and academic researchers. Health centers are eager to work closely with key AI developers to share best practices they have learned when utilizing different AI products. Furthermore, utilizing academic institutions to gather institutional knowledge about the impact AI has had on low-

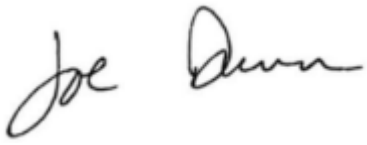
[36] https://bphc.hrsa.gov/funding/funding-opportunities/health-center-controlled-networks-hccn#:~:text=Get%20key%20funding%20details,Patient%2DLevel%20(UDS+)%20data
[37] https://www.nachc.org/rapid-expansion-of-ai-and-tech-tools-serve-health-center-communications/
[38] https://www.nachc.org/nachc-content/uploads/2025/02/NTTAP-HIT-Needs_Assesment_Report-01.28.25.pdf

income populations will ensure developers keep specific patient populations in mind. As mentioned earlier, HCCNs are a wealth of knowledge that AI developers and academic institutions could lean on to better understand the health center experience with AI. We appreciate whatever partnerships, formal or informal, the Administration could create to ensure tools are easily accessible and usable by health centers, and to mitigate any impacts on health center patients.

NACHC recommends the Administration promote the development of affordable and accessible AI technologies, including those that can operate in low-bandwidth environments and on low-cost devices. Many health center patients live in rural areas – health centers serve one in five rural residents across the country[39] – and many of those residents may not have access to high-speed Internet or Wi-Fi. Households in rural areas were less likely to use high-speed internet services and costs can make internet access unaffordable for individuals with lower household incomes. Limited access to reliable technology (e.g., internet and computers), as well as low health and digital literacy, may restrict a health center patient's ability to engage meaningfully.[40] Health centers serve one in three people in poverty, who also are impacted by lack of reliable, stable internet access.[41] The American Health Information Management Association Foundation found that "while over 8 in 10 households with incomes above $100,000 used wired high-speed internet service at home[42], only about 5 in 10 households with incomes below $25,000 did in 2021."

Thank you for your consideration of these comments. We urge the Administration to develop a national artificial intelligence framework that helps health centers and the patients that they serve, with proper guardrails in place. If you have any questions, please contact Elizabeth Linderbaum, Deputy Director of Regulatory Affairs, at elinderbaum@nachc.org.

Sincerely,



Joe Dunn
Chief Policy Officer

[39] 2023 UDS data (HRSA)
[40] https://www.samhsa.gov/blog/digital-access-super-determinant-health#4
[41] 2023 UDS data (HRSA)
[42] https://www.ntia.doc.gov/data/explorer#sel=wiredHighSpeedAtHome&demo=income&pc=prop&disp=chart.