NATIONAL ASSOCIATION OF Community Health Centers

February 27, 2026

Thomas Keane, MD, MBA
Assistant Secretary for Technology Policy
U.S. Department of Health and Human Services
330 C Street SW, Floor 7
Washington, DC 20201

RE: Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity (HTI-5) Proposed Rule (RIN 0955–AA09)

Dear Assistant Secretary Keane:

For the past 55 years, the National Association of Community Health Centers (NACHC) has been the leading national, nonpartisan organization dedicated to supporting Community Health Centers (CHCs), also known as Federally Qualified Health Centers, as the Employer, Provider, and Partner of choice in all communities. Collectively, CHCs are the largest primary care network in the nation, serving as the medical home for 52 million patients,[1] and employing 326,000 dedicated staff.

For 60 years, CHCs have provided high-quality, affordable, comprehensive care – including primary, preventive, dental, behavioral health, pharmacy, vision, and other essential health services at over 17,000 locations across rural and nonrural communities. This includes 1 in 7 Americans, 1 in 3 rural residents, and 1 in 2 in poverty. As our nation's largest primary care system, there is strong evidence, including from the Congressional Budget Office, that our work saves lives and also saves Medicaid and Medicare billions annually by reducing costly emergency, inpatient, and specialty care.[2] Research shows that every dollar invested in primary care yields a 13-to-1 return in overall health system savings.[3]

At a time when CHCs are facing sustained financial instability and deepening workforce shortages, NACHC appreciates the Administration's goal of reducing regulatory burden through the HTI-5 proposed rule. However, it is imperative that these efforts do not inadvertently remove or weaken the safety and security safeguards that safety net providers like CHCs rely upon.[4] Nearly 90% of CHC patients have incomes at or below 200% of the Federal Poverty Level (FPL). CHCs serve these patients amid rising labor costs, negative operating margins, and constrained reimbursement

[1] Weitzman, 2025.
[2] Volerman A, Carlson B, Wan W, Murugesan M, Asfour N, Bolton J, Chin MH, Sripipatana A, Nocon RS. Utilization, quality, and spending for pediatric Medicaid enrollees with primary care in CHCs vs non-CHCs. BMC Pediatr. 2024 Feb 8;24(1):100. doi: 10.1186/s12887-024-04547-y. PMID: 38331758; PMCID: PMC10851548.
[3] https://www.oregon.gov/oha/HPA/dsi-pcpch/Documents/PCPCH-Program-Implementation-Report-Final-Sept-2016.pdf
[4] Cohen G, Lake T, Hossain M, O'Malley AS, Geonnotti K. Incorporating health IT into primary care transformation. Am J Manag Care. 2024 Jan 1;30(1):e26-e31. doi: 10.37765/ajmc.2024.89491. PMID: 38271571.

growth.[5] In 2024 alone, CHCs provided care to 6.9 million dental health patients, 3.4 million behavioral health patients, and over 28.7 million medical patients. All of this occurred while CHCs faced rising labor costs, negative operating margins, and increasing reports of operating losses and limited cash reserves. These challenges restrict their ability to undertake unfunded technology upgrades.[6,7]

These pressures are compounded by ongoing uncertainty in the 340B Drug Pricing Program, anticipated changes with Medicaid enrollments and eligibility, and higher projected uninsured rates.[8] Simultaneously, CHCs must comply with evolving federal requirements, including information blocking, evolving certification criteria, and enhanced privacy and security requirements, each of which has required years of extensive vendor coordination, policy revision, and workforce training. CHCs rely heavily on Certified Electronic Health Record Technologies (CEHRT) to maintain quality, ensure patient safety, and report on health outcomes. While NACHC supports efforts to streamline the market, we are concerned that removing federal "floors" for certification will shift the burden of verification from the government to resource-constrained health centers, potentially exposing them to security flaws, data breaches, hidden vendor costs, and discriminatory algorithms.

Workforce constraints further exacerbate these challenges. Persistent vacancies across clinical and non-clinical roles, including information technology and cybersecurity positions, have left many CHCs without the internal expertise necessary to implement complex interoperability and data governance requirements.[9] With an estimated shortage of 87,150 full-time equivalent (FTE) primary care physicians and 302,440 FTE nurses by 2037,[10] the CHC workforce is experiencing significant burnout.[11] CHCs frequently rely on external vendors to operationalize federal health IT mandates, and they do not maintain the in-house technical capacity that certain aspects of the proposed rule presume. **Absent sufficient transition time, targeted funding, and clear accountability for certified developers, the HTI-5 proposals risk imposing obligations and liability exposure that CHCs lack the operational and financial capacity to absorb without diverting resources from direct patient care.**

NACHC appreciates the opportunity to comment and looks forward to continued engagement with ASTP/ONC to ensure that final policies are workable for the nation's health care safety net.

I. Supporting Interoperability

---

[5] NACHC, America's CHCs Fact Sheet (2024). https://www.nachc.org/resource/americas-health-centers-by-the-numbers/

[6] 2024 UDS Data

[7] NACHC, Financial Impact Survey Findings (2023). https://www.nachc.org/about-nachc/mission/nachc-annual-report-2023/

[8] https://www.urban.org/research/publication/48-million-people-will-lose-coverage-2026-if-enhanced-premium-tax-credits

[9] NACHC, Health Center Workforce Survey (2023). https://www.nachc.org/wp-content/uploads/2023/09/Health-Center-Workforce-9.2023-FINAL.pdf

[10] https://bhw.hrsa.gov/sites/default/files/bureau-health-workforce/state-of-the-health-workforce-report-2024.pdf

[11] America's Health Centers: By the Numbers - NACHC

NACHC strongly supports the proposed changes to Information Blocking regulations, including the removal of the "Third Party Seeking Modification Use" condition within the Infeasibility Exception at § 170.315(a)(12). This change would help ensure that vendors cannot prevent CHCs from using authorized third-party applications to write data back into the Electronic Health Record (EHR). For CHCs, this functionality is essential to documenting referrals, tracking social risk interventions, and closing the loop on external care coordination activities in a timely and efficient manner.[12]

Current write-back restrictions often require CHC staff to enter referral information into a separate care coordination platform and then manually copy that information into the EHR. Allowing data to flow directly into the patient's chart through standardized APIs, such as Fast Healthcare Interoperability Resources (FHIR), would eliminate duplicate documentation, reduce medical errors, improve workflow efficiency, and reduce administrative burden on medical assistants and care coordinators, allowing staff to focus more on patient care.

NACHC also supports the revised definition of "Access" to explicitly include autonomous artificial intelligence (AI) systems. Clarifying that such agents qualify as permissible users would allow CHCs to automate routine queries, such as monitoring hospital portals for discharge notifications and related care information, tasks that currently require significant manual staff time.[13] Permitting recurring automated queries would streamline care management, facilitate timely post-discharge follow-up and Transitional Care Management (TCM) billing, and better align federal policy with the operational realities facing CHCs. NACHC strongly supports the expanded definitions of Access and the allowance of third-party write-back, provided that ASTP/ONC retains rigorous certification standards for auditability, provenance, and data integrity.

While NACHC supports the proposed advancements in interoperability, we have significant concerns about removing specific certification criteria. We fear these removals will allow vendors to "unbundle" current standard features, including information technology frameworks, into expensive add-ons or remove them entirely, harming our ability to care for vulnerable populations.

II. Cybersecurity & Privacy: A Critical Risk

NACHC opposes the blanket removal of privacy and security certification criteria (§ 170.315(d)(1)-(d)(13)),[14] and instead recommend ASTP/ONC to adopt the Alternative Proposal mentioned in the rule to retain the Audit Log requirements (§ 170.315(d)(2), (3), and (10)) to ensure fraud and abuse can still be detected. This proposal removes the requirement for vendors to demonstrate Multi-Factor Authentication (MFA), audit logs, and

---

[12] Everson J, Healy D, Patel V. Experiences with information blocking in the United States: a national survey of hospitals. J Am Med Inform Assoc. 2023 May 19;30(6):1150-1157. doi: 10.1093/jamia/ocad060. PMID: 37029919; PMCID: PMC10198516.

[13] Mello MM, Roberts JL. Antidiscrimination Law Meets Artificial Intelligence—New Requirements for Health Care Organizations and Insurers. JAMA Health Forum. 2024;5(8):e243397. doi:10.1001/jamahealthforum.2024.3397; Arndt BG, Beasley JW, Watkinson MD, Temte JL, Tuan WJ, Sinsky CA, Gilchrist VJ. Tethered to the EHR: Primary Care Physician Workload Assessment Using EHR Event Log Data and Time-Motion Observations. Ann Fam Med. 2017 Sep;15(5):419-426. doi: 10.1370/afm.2121. PMID: 28893811; PMCID: PMC5593724.

[14] Section III.A.4, p. 60988-60989

encryption during certification. The removal of the privacy and security certification criteria would shift responsibility to providers, including CHCs, to perform additional due diligence to assure alignment with HIPAA privacy and security safeguard requirements, validate and embed specific protections within contractual arrangements, and integrate business associate security assessments into their HIPAA compliance oversight, as appropriate.

CHCs are dedicated to enhancing their security postures and maintaining privacy stewardship, but this proposal will impose undue financial hardship and create significant liability concerns. As safety net providers operating on razor-thin margins, CHCs often face challenges such as financial constraints, limited training opportunities, and the complexities of integrating new systems within the health IT space.[15] 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 many CHCs maintain dedicated staff, these IT teams are small and often wear multiple hats, so CHCs rely on third-party vendors and organizations to help them maintain HIPAA and cybersecurity compliance to secure their sensitive data.

If these privacy and security protection criteria are removed, CHCs will need to test cybersecurity measures in-house or contract with additional vendors. Small to medium-sized CHCs do not have the resources to conduct independent security testing of their software or afford to pay a third party.[16] Health center health IT experts estimate that the cost for penetration testing (PEN tests) would range from $20,000 to $80,000, depending on the size and complexity of a CHC's system. Removing the federal "seal of approval" for security does not remove the HIPAA requirement for CHCs to be secure, but it removes the assurance that their vendor software supports that compliance. This can expose CHCs to massive liabilities regarding data breaches and ransomware.[17]

In 2025, healthcare cybersecurity attacks increased by 21% to 575, up from 476 in 2024.[18] In 2024, CHCs were among the stakeholders impacted by the Change Healthcare breach. Over three-quarters of CHCs were negatively affected by the cybersecurity breach, with an average of 75% of CHC patients directly affected. Over 60% of CHCs had patients affected by delays in access to care due to inability to obtain prior authorization, service interruptions, or going without needed medications, and over 70% of CHCs report that access to discounted medication or health care services has been affected. One in five health centers (20%) had over half (50%) of their revenue impacted by the breach. While the scale and impact of cyberattacks were largely an anomaly, removing these cybersecurity protection requirements from vendors could lead to an increase in cyberattacks. Additionally, this creates a more significant risk for the CHC. If these key cybersecurity measures are removed, there are more instances in which CHCs fail to meet the HIPAA Security Rule requirement for audit controls (45 CFR 164.312(b)), exposing them to Office

---

[15] https://www.nachc.org/nachc-content/uploads/2025/02/NTTAP-HIT-Needs_Assesment_Report-01.28.25.pdf

[16] Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inform. 2013 Jun;46(3):541-62. doi: 10.1016/j.jbi.2012.12.003. Epub 2013 Jan 8. PMID: 23305810.

[17] Suleski T, Ahmed M. A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things. J Med Internet Res. 2023 Aug 29;25:e44114. doi: 10.2196/44114. PMID: 37490633; PMCID: PMC10498322.

[18] https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/healthcare-cyberattacks-up-21-in-2025-5-notes/#:~:text=Advertisement,192.7%20million%20patients%20in%202024.

for Civil Rights (OCR) investigations and fines. Removing the § 170.315(d) criteria effectively decouples Health IT Certification from HIPAA compliance support, creating a regulatory misalignment in which a 'Certified' product may no longer be 'HIPAA-ready.' Additionally, removing these items could erode invaluable patient trust; without them, CHC cannot prove to patients that their data is safe, irreparably damaging community trust.

NACHC warns that the legal medical records could be corrupted by "agentic AI" users without "humans in the loop" having the technical tools, such as audit logs, provenance tags, or AI transparency data, to detect data corruption. The question of accountability for when this happens is concerning because this again shifts the liability to community health centers, and away from AI vendors. **As previously stated, we recommend ASTP/ONC adopt the Alternative Proposal mentioned in the rule to retain the Audit Log requirements (§ 170.315(d)(2), (3), and (10)).** Keeping these items – auditable events and tamper resistance, audit report(s), and auditing actions on health information – will help ensure fraud and abuse can still be detected. This will also help support CHC compliance obligations as providers and aid in internal and external investigations.

III. "Black Box" Algorithms (AI Transparency)

NACHC strongly urges ASTP not to finalize the removal of Decision Support Intervention (DSI) transparency requirements (§ 170.315(b)(11)), specifically the elimination of "source attributes" and risk management. "Model cards" provided by vendors help disclose training data or bias testing for AI. These model cards provide CHCs with clearer insight into the positives and limitations of the DSI tools they use, helping them better judge and understand outcomes from DSIs. Without clear expectations for documentation and disclosure, CHC providers may lack sufficient information to assess the reliability, bias risks, and clinical appropriateness of AI-enabled tools. This could undermine trust, impair informed decision-making, and create variability in how risk is evaluated and mitigated across care settings. CHCs already consistently deliver high-quality, cost-effective care that meets or exceeds national benchmarks, particularly for populations with complex needs. For instance, CHCs provide strong chronic disease management (67% blood pressure control in 2024), increase preventive screenings, and reduce reliance on Emergency departments,[19] all of which help improve patients' quality of life while saving the U.S. healthcare system money. CHCs serve the populations more likely to be harmed by biased algorithms. Without "Model Cards" to disclose training data, CHC clinicians cannot know if a predictive tool is safe for our patient base, which could negatively impact the high-quality care CHCs already provide. Additionally, this removal contradicts the FAVES (Fair, Appropriate, Valid, Effective, Safe) principles previously championed by ASTP/ONC.[20] CHCs serving disproportionately minority populations cannot assess 'Fairness' or 'Safety' without federal mandates requiring vendors to disclose the demographics of their training data.

---

[19] https://www.nachc.org/investing-in-the-quality-clinical-care-community-health-centers-deliver/#:~:text=According%20to%20the%202024%20Uniform%20Data%20System,2024%2C%20outperforming%20the%20Medicaid%20median%20of%2038%25

[20] https://healthit.gov/blog/ai-ml/leveraging-agency-expertise-to-foster-american-ai-leadership-and-innovation/#:~:text=Going%20even%20further%2C%20I'm,validity%2C%20effectiveness%2C%20and%20safety.

For example, a CHC uses a DSI tool to flag "High Risk" patients for care management, a common service. The tool rarely flags patients from a specific zip code (a predominantly low-income area) or flags patients of differing demographic backgrounds at lower rates. Because the AI was trained on commercial insurance claims data (wealthier patients, non-minorities), certain patient populations are now excluded or receive reduced recommendations for care management resources, potentially worsening health disparities. Without the Model Card, providers and end-users cannot see this source bias.[21] The CHC may be paying for and using a discriminatory tool but lacks the transparency data to prove it. Deregulation in this area creates a "black box" that transfers medico-legal liability to the provider.[22]

CHCs are eager to continue to utilize AI, including DSI tools. CHCs use artificial intelligence across administrative and clinical settings, freeing up staff for higher-value tasks, reducing costs, and improving overall financial and operational performance. While we acknowledge that no dataset will ever be free of bias, being transparent about potential bias in the data used to train AI methods and applications is an important step toward mitigating unintended consequences. We understand ASTP's desire to enhance cost savings by eliminating these model cards, this would be at the expense of safety net providers who rely on them to better assess and understand how these AI tools impact the patients we serve.

IV. The UDS Reporting Blind Spot (CQM Filtering)

NACHC opposes the proposed removal of the "Clinical Quality Measures (CQM) – Filter" criterion at § 170.315(c)(4). CHCs are federally required to report clinical quality data through the Uniform Data System (UDS), including measures stratified by race, sex, ethnicity, payer, age, and other demographic factors.[23] The current certification requirement ensures that EHR systems can uniformly filter and generate reports using these data elements. Removing this criterion would shift responsibility for maintaining this essential functionality from vendors to providers who do not control the technology's design.

Without certified filtering capabilities, CHCs could lose the now default automated tools they rely on to identify differences and produce required reports. In practice, CHCs may be forced to return to manual chart reviews, custom report building, or external data extraction processes to meet UDS obligations, a requirement of fulfilling 330 grant requirements. This would increase administrative workload, increase the likelihood of human error, and divert clinical and quality improvement efforts from patient care, all while CHCs are facing significant workforce shortages and burnout.[24] In many cases, the only viable alternative would be for CHCs to contract a third-party population health vendor to replicate the filtering capabilities currently required under certification. This would impose new and unfunded costs on organizations that are already operating on narrow or

---

[21] Chin MH, Afsar-Manesh N, Bierman AS, et al. Guiding Principles to Address the Impact of Algorithm Bias on Racial and Ethnic Disparities in Health and Health Care. JAMA Netw Open. 2023;6(12):e2345050. doi:10.1001/jamanetworkopen.2023.45050

[22] Ferryman K, Mackintosh M, Ghassemi M. Considering Biased Data as Informative Artifacts in AI-Assisted Health Care. N Engl J Med. 2023 Aug 31;389(9):833-838. doi: 10.1056/NEJMra2214964. PMID: 37646680.

[23] https://data.hrsa.gov/topics/health-centers/uds

[24] NACHC, Health Center Workforce Survey (2023). https://www.nachc.org/wp-content/uploads/2023/09/Health-Center-Workforce-9.2023-FINAL.pdf

negative margins.[25] CHCs do not have the capital to procure additional analytics platforms needed to maintain compliance with existing federal reporting mandates. For rural and frontier CHCs, limited vendor availability and interoperability challenges between EHR systems and external analytics platforms would further increase operational and financial complexity.

The removal also creates heightened liability risks for providers. CHCs would remain legally responsible for the accuracy and completeness of their UDS reporting, regardless of whether their vendors provide certified filtering tools. If EHR systems lack reliable stratification functionality, CHCs may face audits, compliance deficiencies, or financial consequences tied to incomplete or inaccurate reporting, which could expose CHCs to malpractice risk if discrimination is later identified and attributed to insufficient monitoring.[26] Shifting the burden of verifying data integrity and maintaining reporting functionality from certified developers to CHCs creates an imbalance in accountability and places disproportionate legal and compliance exposure on providers that neither design nor control the underlying technology. **NACHC urges ASTP/ONC to maintain the existing "Clinical Quality Measures – Filter" criterion to ensure that certified health IT continues to support CHC UDS reporting, regulatory compliance, and safe, efficient care delivery within the health care safety net.**

V. Loss of Structured Family Health History

NACHC is also concerned with the proposed removal of the "Family Health History" criterion at § 170.315(a)(12). Eliminating the functional requirement to capture family health history risks means reverting this critical field to unstructured, free-text documentation. For CHCs, structured family health history data are essential to population health management, preventive care outreach, and clinical decision support. Without these data elements, CHCs' ability to generate reports identifying patients who require earlier or more frequent screenings, such as individuals with a family history of colon cancer or hereditary cardiac conditions, would be significantly impaired. Interoperability with other systems will be affected by non-standardization and the requirement for data entry.

If family health history is no longer required to be captured in structured fields, CHCs may be forced to rely on manual chart reviews or keyword searches within narrative text to identify high-risk patients, which can be inefficient, prone to omission, and resource-intensive. As previously mentioned, CHCs are already experiencing staffing shortages and workforce burnout across care teams. Requiring providers or supporting staff to manually document, review, or validate family history information would add existing workload pressures and divert time from direct patient care and care coordination. Additionally, removing this key criterion raises serious liability concerns for CHCs. Providers rely on structured family health history data to identify patients who may require earlier screening or additional genetic evaluation.[27] If this information is harder to locate, CHCs face an increased risk of missing clinically significant risk factors. For example, failure to identify a patient eligible for earlier colon cancer screening due to inadequate data functionality

---

[25] https://www.nachc.org/community-health-centers-grew-in-2024-but-patient-access-faces-a-tipping-point/

[26] https://www.davidkates.com/blog/2023/december/how-discrimination-can-cause-medical-malpractice/

[27] Ginsburg GS, Wu RR, Orlando LA. Family health history: underused for actionable risk assessment. Lancet. 2019 Aug 17;394(10198):596-603. doi: 10.1016/S0140-6736(19)31275-9. Epub 2019 Aug 5. PMID: 31395442; PMCID: PMC6822265.

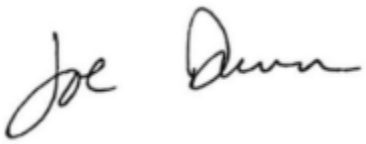
could have grave consequences, including delayed diagnosis and preventable morbidity or mortality.[28]

We anticipate that this change could eventually be implemented using FHIR-based standards. However, CHCs will require sufficient lead time, funding, and technical assistance from ASTP/ONC to implement and operationalize these capabilities effectively. Transitioning to new exchange frameworks without maintaining baseline structured documentation requirements risks creating gaps in functionality during the interim period. **Without clear safeguards and guidance, removing this criterion would increase workforce burden, operational challenges, and legal exposure for CHCs, while undermining preventive care and population health management efforts central to the CHC mission.**

Thank you for the opportunity to comment on these proposals. NACHC appreciates the Administration's goal of unleashing prosperity through innovation. However, for safety net providers, regulation often serves as a necessary protection against cost-shifting and substandard technology. We urge ASTP/ONC to finalize the information blocking improvements while retaining the critical certification criteria that protect patient safety, fairness, and security.

If you have any questions about our comments, please contact Elizabeth Linderbaum, Director of Regulatory Affairs, at elinderbaum@nachc.org.

Sincerely,



Joe Dunn
Chief Policy Officer

[28] Doubeni CA, Fedewa SA, Levin TR, Jensen CD, Saia C, Zebrowski AM, Quinn VP, Rendle KA, Zauber AG, Becerra-Culqui TA, Mehta SJ, Fletcher RH, Schottinger J, Corley DA. Modifiable Failures in the Colorectal Cancer Screening Process and Their Association With Risk of Death. Gastroenterology. 2019 Jan;156(1):63-74.e6. doi: 10.1053/j.gastro.2018.09.040. Epub 2018 Sep 27. PMID: 30268788; PMCID: PMC6309478.