American Health Information Management Association
201 West Lake Street, 226
Chicago, IL 60606

February 25, 2025

Dr. Thomas Keane
Assistant Secretary and National Coordinator
Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology
330 C Street NW
Floor 7, Mary E. Switzer Building
Washington, DC 20201

Dear Dr. Keane:

On behalf of the American Health Information Management Association (AHIMA), I am writing in response to the Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology (ASTP/ONC) Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions To Unleash Prosperity proposed rule published in the December 29, 2025 *Federal Register* (RIN 0955-AA09).

AHIMA is a global nonprofit association of health information (HI) professionals, with over 61,000 members and more than 88,500 credentials in the field. The AHIMA mission of empowering people to impact health® drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and health information professionals. Leaders within AHIMA work at the intersection of healthcare, technology, and business, occupying data integrity and information privacy job functions worldwide.

Overall Recommendations

AHIMA applauds ASTP/ONC for taking a comprehensive review of its compliance programs to determine where regulatory burden could be removed. It is important for agencies to regularly review their suite of regulatory requirements to ensure they still meet the intended goals. While AHIMA supports some of the changes proposed throughout HTI-5, it does caution that others may lead to unintended consequences, shift additional administrative burden to the end-user, or may remove technology that is needed to promote nationwide interoperability.

One area of concern for AHIMA relates to the proposed removal of Health IT Certification Program (Certification Program) criteria related to the standards used to facilitate health data exchange. ASTP/ONC states throughout the HTI-5 proposed rule its desire to shift the Certification Program to a new innovative future focused on the use of HL7® Fast Healthcare Interoperability Resources (FHIR) application programming interfaces (APIs). Many of the proposals related to the Certification Program in this rule prioritize removing criteria that support the use of the Common-Clinical Data Architecture (C-CDA), on which much of the document-based exchange in healthcare interoperability is based today. AHIMA applauds ASTP/ONC's focus on continuing to push the health IT community forward and looking for ways to spur innovation. However, we recommend ASTP/ONC refrain from removing certification criteria that jeopardizes the ability of provider organization and HI professionals to utilize C-CDA based exchange until FHIR is fully developed, tested, and implemented.

Removing C-CDA functionality without understanding the readiness and/or ability of healthcare organizations to support widespread use of FHIR jeopardizes ongoing nationwide interoperability. Finalization of this proposal will prevent patient information from traveling to where it needs to be, when it needs to be there. Due to the cost of FHIR implementation and its lack of widespread adoption, C-CDA is often used by under resourced provider organizations and HI professionals to support participation in nationwide data exchange. If ASTP/ONC were to remove it from the Certification Program, it would open the possibility for health IT developers to charge provider organizations for the use of C-CDA, as well as the new FHIR APIs outlined in this proposed rule. This would further stretch provider organizations by having to pay for already used technology because it would be deemed outside of the Base Electronic Health Record (EHR) definition requirements as outlined by ASTP/ONC in this rule.

ASTP/ONC's mission is to improve the access, exchange, and use of patient health information throughout the US health system. The agency's mission can only be accomplished if the healthcare community has widespread usage of technology. C-CDA today is the technology that maintains the highest adoption rate for providers to enable the sharing of patient health information. While AHIMA agrees with ASTP/ONC that the health system must look to new, innovative technologies for data sharing, innovation cannot happen in a vacuum with no alternate means for patient data to be moved easily in a trusted manner. As such, we recommend ASTP/ONC continue to support the use of C-CDA, and its accompanying transfer modalities moving forward, or until a time when FHIR technology is widely adopted and actively used by healthcare organizations.

III. Health Information Technology Standards, Implementation Specifications, and Certification Criteria and Certification Programs for Health Information Technology (Part 170)

A. Certification Criteria for Health Information Technology

1. Care Coordination Certification Criteria

a. Transitions of Care

ASTP/ONC proposes to remove the "transitions of care" certification criteria at 45 CFR § 170.315(b)(1)(iii) "create" eliminating the only criteria within the Certification Program that designates data to be used to support patient matching. The inclusion of patient matching criteria within the continuity of care document (CCD) improves patient safety and security by reducing instances of patient misidentification. Further, it is the only section within the certification criterion that references patient matching. AHIMA recommends ASTP/ONC refrain from finalizing the removal of these requirements until a time in which patient matching can be more fully addressed within health IT.

Without the ability of HI professionals to correctly connect a patient to their medical record, lives have been lost and medical errors have needlessly occurred. These are situations that could have been avoided had patients been accurately identified and matched to their records. This problem is so dire that one of the nation's leading patient safety organizations, the ECRI Institute, has named patient misidentification as a recurring top ten threat[1] to patient safety.

If ASTP/ONC were to remove the patient matching requirements in the Certification Program, AHIMA recommends adopting provisions found in HR 2002, the Patient Matching and Transparency in Certified Health IT Act of 2025 or

[1]Available at: https://assets.ecri.org/PDF/White-Papers-and-Reports/2020-Top-10-Patient-Safety-Executive-Brief.pdf.

the MATCH IT Act[2] of 2025, which includes a provision to define and adopt a minimum data set needed to reach a 99.9% patient match rate, and directs the creation, updating, or adoption of data standards, (including an established industry standard, if available) to ensure demographic elements are entered in a standardized format. Without a more robust strategy to address patient matching, ASTP/ONC risks further complicating the patient matching landscape, increasing the likelihood of patient data mismatches and jeopardizing patient safety.

e. Decision Support Interventions

AHIMA previously supported the adoption and use of the Decision Support Intervention (DSI) criterion in the Certification Program at 45 CFR § 170.315(b)(11) and recommends ASTP/ONC refrain from finalizing proposals within HTI-5 to remove this criterion at this time. This criterion and its requirements remain a crucial part of helping providers evaluate DSI technologies and other artificial intelligence (AI) tools for purchase and implementation. Helping providers, HI professionals, and other end-users understand what and how patient data is used is crucial in helping to determine what DSI/AI technology is suitable for use for their patient population. Such transparency helps ensure they are not purchasing and implementing unneeded and costly technology and facilitates trust with patients.

The DSI transparency requirements also help providers and HI professionals understand when patient data is used to make a recommendation for care and what data from the United States Core Data for Interoperability (USCDI) is being utilized. This helps providers adjust recommendations from the DSI based on the data used and the type of patient the DSI is providing a care recommendation for. Without the ability to have visibility into what and how the data is used, providers will be limited in their ability to understand how much to factor a DSI recommendation into a patient's care plan. If providers cannot trust the DSIs available to them it will slow the uptake and use of new innovative DSI technologies. ASTP/ONC's stated goal within the HTI-5 proposed rule is to increase the innovation and use of DSIs. Removing this criterion increases the risk of slowing the adoption and implementation of such innovation.

While AHIMA supports the implementation of the DSI criterion, we recognize opportunities exist to improve the criterion. Within the proposed rule, ASTP/ONC states they do not believe this criterion is being used because there is limited evidence of use. Since health IT developers were only required to adopt the criterion beginning January 1, 2025, it is difficult to determine whether uptake and use is low due to delays in reporting. As a result, we recommend ASTP/ONC pursue alternative proposals to improving the DSI criterion requirements. Such alternatives could include building on existing DSI requirements or proposing new criteria to provide transparency in the use of DSI and AI within healthcare. If ASTP/ONC proceeds with removing this criterion we are concerned the nation would be left no regulatory guardrails for DSI/AI tools in the health IT space.

2. Privacy and Security Certification Criteria

AHIMA opposes ASTP/ONC's proposal to remove the privacy and security certification criteria from 45 CFR § 107.315(d) and the associated Privacy and Security Certification Framework from 45 CFR § 170.550 (h). Removing the privacy and security criteria from the Certification Program exposes patients' most sensitive information at a time when healthcare is under constant threat of cyberattack. ASTP/ONC should work to find other alternatives to current privacy and security certification criteria if it seeks to reform the program and then propose those changes as part of another proposed rule before removing the criteria and framework proposed in this rule.

[2]Available at: https://www.congress.gov/bill/119th-congress/house-bill/2002/text.

ASTP/ONC states within HTI-5 that the above referenced certification criteria were created to assist with HIPAA Privacy and Security Rule compliance and that now the criteria no longer meets these needs due to the complexity of the health technology stack within organizations. While it is true the EHR is only one part of the technology landscape within a hospital or provider organization, it is often the largest part managing the largest volume of patient health information. The EHR serves as the main conduit for exchange for patient data, often connected to statewide and nationwide data exchange networks. Even if the privacy and security criteria for the EHR does not ensure compliance for the whole organization it does relieve significant burden from provider organizations and HI professionals by eliminating the need to find bespoke solutions for the EHR in addition to other technology tools.

ASTP/ONC states that the privacy and security criteria within the Certification Program "[diverts] financial resources and effects from innovative, agile, and comprehensive solutions that can address the threats faced by healthcare providers and meet the regulatory obligations under HIPAA." This assumption is based on the belief that the funds tied to the development of the EHR certification criteria are the same as those used to develop comprehensive privacy and security tools. In reality, the developers of CEHRT subject to the Certification Program do not develop broader privacy and security tools. As a result, the costs to develop and implement these technologies are not spent to create more innovative solutions, but are instead passed on to hospitals and provider organizations who will need to purchase additional software developed by different software developers.

Further, HTI-5 grounds many of the proposed changes to the privacy and security criteria in the justification that ASTP/ONC's shift to a FHIR API-based certification structure necessitates this change. The proposed rule text states ASTP/ONC may consider adding further privacy and security constraints as more API-focused certification criteria are implemented. However, human error is still the number one threat to privacy and security according to Chief Information Security Officers (CISOs).[3] These human errors include phishing attacks and social manipulation schemes designed to gain access to human accounts and into a system. These types of attacks are the top vectors of compromise used to access the EHR and gain access to patient data. By removing the privacy and security criteria in the Certification Program, ASTP/ONC will remove protections from the EHR that could help hospitals and provider organizations guard against these types of compromises. Ensuring these requirements, like two-factor authentication, remain in the Certification Program will give hospitals and provider organizations additional layers of security needed to protect themselves in the ever-evolving cyber threat landscape.

ASTP/ONC wrote in the proposed rule that 45 CFR § 170.315(d)(2) and (10) would be retained as the criteria may help with compliance and investigations by relevant entities. AHIMA reminds ASTP/ONC that patients, under HIPAA law, have the right to request an audit report of who has access to their protected health information (PHI). Ensuring this functionality remains part of the Certification Program is crucial to enabling HI professionals within hospitals and provider organizations the ability to comply with these HIPAA requirements. While these criteria may be important due to compliance and investigatory requirements, it is also important that these requirements remain in place to ensure patients maintain some level of control over their health information, something AHIMA recognizes is a priority of this administration.

If ASTP/ONC removes the privacy and security criteria from the Certification Program, AHIMA recommends a robust set of replacement criteria be drafted and proposed for inclusion. AHIMA agrees it is important to develop and implement new innovative privacy and security solutions while ensuring that development and innovation does not jeopardize the healthcare system's current cybersecurity posture. At this time, with no alternative proposal for how to maintain that posture, it would be premature for the proposed privacy and security criteria to be removed from the Certification Program.

[3]Available at: https://www.ibm.com/think/insights/cisos-list-human-error-top-cybersecurity-risk.

5. Patient Engagement Certification Criteria

a. View, Downland, and Transmit to a 3rd Party

AHIMA recommends ASTP/ONC refrain from finalizing the proposal to remove 45 CFR § 170.315(e(1)(i) Web Content Accessibility Guidelines (WCAG 2.0). This portion of the Certification Program is crucial to ensuring accessibility tools remain a part of health IT systems for end-users who utilize these tools without resulting in additional cost to the provider organization. Removing these criteria creates the possibility for health IT developers to charge for these accessibility functions.

Within the justification for the proposed removal, ASTP/ONC states the functionality is widespread throughout health IT technology and that because of other federal laws, this functionality will remain. Specifically, ASTP/ONC cites requirements within the Americans with Disabilities Act (ADA), specifically the provision requiring those who receive federal funding to support ADA compliant accessibility tools. While the ADA does require health IT systems to have this functionality, not every health IT developer under the Certification Program receives federal funding and thus may not be beholden to these accessibility requirements. As a result, removal of this requirement could result in this functionality no longer being included in health IT products and/or allow health IT developers to charge customers to remain compliant with ADA law. While developers may not receive federal funding, their provider organization customers do if they accept Medicare and Medicaid insurance, creating a scenario where the proposed removed criteria are still needed by provider organizations, but developers are now able to charge for the "extra" functionality since it is no longer part of the Certification Program requirements.

If ASTP/ONC were to finalize HTI-5 with the removal of these requirements, additional cost burden may be shifted to provider organizations to ensure they remain in compliance with ADA and maintain the capability for those covered under the ADA, including HI professionals who utilize ADA accessible tools, to use health IT within their facility. While this technology may be widely adopted, ASTP/ONC must ensure it is shielded from being able to be separately charged for as an add-on technology. Failure to do so could be catastrophic to maintaining a low- or no-cost accessible environment in health IT technology.

7. Design and Performance Certification Criteria

c. Safety Enhanced Design and e. Accessibility-Centered Design

ASTP/ONC proposed to remove 45 CFR § 170.315(g)(3) Safety Enhanced Design and 45 CFR § 170.315(g)(5) Accessibility-Centered Design, as well as its references at 45 CFR § 170.550(g)(1) stating that both certification criteria are widely adopted and that removal of these criteria will remove cost burden from developers and increase the ability for innovative design techniques to be pursued in health IT. AHIMA recommends ASTP/ONC refrain from finalizing these proposals as it creates the ability for health IT developers to charge provider organizations for the inclusion of such techniques, shifting cost burden onto the provider community.

HTI-5 states that both of these techniques for design are widely adopted and used throughout modern software design. Additionally, it states that the removal of criteria related to accessibility-centered design should not impact the ability for users to comply with ADA regulations as those that receive federal funding will still be subject to ensuring tools are made in an accessible fashion. While both things may be true, there is no guarantee user-centered design will continue or that health IT developers that receive federal funding will ensure accessibility-centered design continues. Even though a vendor may be exempt from these solutions, provider organizations will

most likely still need to comply with user-centered and accessibility-centered design techniques to ensure they remain in compliance with other federal laws and that their users are able to utilize implemented technology. With these criteria no longer included within the Certification Program, provider organizations may need to pay additional fees for health IT technology that enables usability and accessibility as developers would be under no obligation to provide it at no additional cost.

If the removal of these criteria were to be finalized, ASTP/ONC could create a scenario where provider organizations are charged for design techniques previously included as part of a CEHRT product. While it is important to spur innovation, this should not happen in a way that shifts additional cost to the provider community. These certification criteria continue to be an important fixture of health IT design and should remain in place.

8. Transport Methods and Other Protocols Certification Criteria

AHIMA recommends ASTP/ONC preserve the certification criteria proposed for removal contained within 45 CFR § 170.315(h)(1) as the technologies included in these criteria remain critical to enabling the access, exchange, and use of critical pieces of PHI. Much of the nation's HI professionals rely on document-based exchange architectures to exchange information that is not supported by architectures like the USCDI, or languages such as FHIR. It is important for ASTP/ONC to preserve the ability for providers, particularly under-resourced or rural providers, to have access to these exchange modalities to ensure they are able to participate in interoperable data exchange. If ASTP/ONC were to remove the technologies outlined in these areas of the Certification Program, provider organizations may be forced to pay for exchange technology they previously received as part of their standard health IT deployment. Until a time when these technologies are no longer relied upon, AHIMA recommends ASTP/ONC preserve them in the Certification Program to avoid increasing the technology cost burden placed on provider organizations.

B. Standards and Implementation Specifications for Health Information Technology

1. United States Core Data for Interoperability Version 3.1 Update (USCDI v3.1)

AHIMA supports ASTP/ONC's continued expansion and advancement of USCDI with the addition of standardized data classes and elements. A more comprehensive version of USCDI will move the healthcare system towards improved nationwide interoperability while prioritizing the quality and validity of patient health data. Adopting more complete versions of USCDI will enable more information to be available to all providers and HI professionals at the point of care, empowering them to deliver more tailored, patient-centered care. Additionally, adding more data classes and elements over time in a predictable fashion creates a wide-ranging standard for complete, standardized patient medical records, leading to quicker, more efficient, and complete interoperability.

However, the proposed advancement to USCDI v3.1 includes a reduction rather than expansion of data elements. AHIMA urges ASTP/ONC not to finalize the proposed removal of and revisions to these data elements. These elements are central to a patient's demographic information, create a more accurate and complete picture of the patient, and are critical to achieving accurate patient matching efforts across HI professional supported healthcare organizations, and the patient's broader healthcare journey. Additionally, the rollback of an already approved and adopted version of USCDI creates confusion among the health IT community and inhibits progress towards accomplishing interoperability of quality and complete patient health information.

ASTP/ONC is currently seeking feedback on the USCDI Draft v7, yet this proposed rule continues to make revisions to v3. Each new advancement of USCDI brings the industry closer to optimal data exchange and interoperability

through the addition of standardized data elements. AHIMA encourages ASTP/ONC to improve alignment between advanced versions of USCDI versions adopted in regulation. A more aligned feedback and adoption cycle ensures USCDI evolves with the changing landscape of health information in alignment with the real-time needs of the healthcare community and health data exchange.

D. Conditions and Maintenance of Certification Requirements for Health IT Developers

3. Real World Testing

Real-world testing is critical to the success of health IT policy initiatives and implementation of effective technology that accomplishes the goals and reduces the burden it was created to address. Without real-world testing that involves health IT end-users who are using these tools, new technical approaches and regulatory requirements will not be sufficiently grounded in real-world experiences. AHIMA urges ASTP/ONC to refrain from removing the Real World Testing requirement within the Conditions and Maintenance of Certification requirements. Real-world testing plays a crucial role in ensuring CEHRT meets the needs of HI professionals and providers once implemented and that implementation does not cause increased burden due to poorly designed technology or technology that does not meet real-world workflows. Other consequences due to a lack of adequate real-world testing include:

- Adoption of standards that require significant workarounds by healthcare organizations to implement;
- Incomplete or immature standards;
- Standards and policies that do not achieve the desired goal when deployed;
- Excessive burden added to end-users;
- Wasted money on failed implementations; and
- Confusion from patients with respect to technological capabilities.

With such factors at play in the absence of adequate real-world testing, AHIMA urges ASTP/ONC to preserve this requirement in the Certification Program and strengthen the use of real-world testing to ensure innovation is realized in health IT with minimized administrative burden. Ensuring real-world testing remains a robust requirement of the Conditions and Maintenance of Certification program is one way to realize that potential. As the founding member of the Health IT End-Users Alliance[4], AHIMA is eager to provide our critical feedback and collaborate with ASTP/ONC on the best methods and pathways to include diverse end-user input in the development and testing of new standards and technological approaches.

IV. Information Blocking (Part 171)

With the ever-expanding nature of artificial intelligence (AI) technologies, AHIMA understands the intent of ASTP/ONC in broadening the definitions of access, exchange, and use of EHI. However, we encourage ASTP/ONC to consider if it is necessary to expand these definitions in regulation when they may be widely understood to include AI tools. Modifying the definitions to be more specific creates confusion among actors about what would be excluded from this definition, such as other types of AI. This may inadvertently create a regulatory gap for certain types of technologies that may not meet the definition and thus would not be subject to the information blocking requirements. It is also unclear how liability would be assigned if an information blocking complaint involves the use of an AI tool. AHIMA recommends ASTP/ONC not modify the definition of access, exchange, and use and provide guidance and resources to actors on how the information blocking requirements and exceptions

[4]Available at: https://hitenduser.org/.

interact with AI. If finalized, we encourage ASTP/ONC to provide more specific explanation with exemplars of the inclusion of AI in this definition and clarify who is liable if an AI tool is at fault for inhibiting access, exchange, and use of EHI.

Proposed changes to the Infeasibility and Manner exceptions and the proposed removal of the TEFCA Manner exception appear based on the findings that the conditions and exceptions are either unnecessary or subject to misuse. AHIMA recommends ASTP/ONC share the data referred to in the proposed rule about the documented use and misuse of the conditions to better inform stakeholders about the rationale behind these proposed revisions.

Overall, AHIMA appreciates ASTP/ONC's continued evaluation of the information blocking program to ensure it evolves with health data exchange and interoperability. The design and intent of the information blocking regulatory framework has improved patient and provider access to and exchange of data without special effort and AHIMA supports the goals of the program. We appreciate ASTP/ONC's intent in modifying the definitions and exceptions to fit the needs and capabilities of actors who must comply with information blocking. However, stability and predictability in the program is paramount to ensuring actors can achieve effective compliance. AHIMA encourages ASTP/ONC to balance future revisions to information blocking with the importance of stability in the information blocking program without injecting additional complexity into the compliance process. When modifications are needed, ASTP/ONC should simplify and streamline exceptions where possible to provide better clarity to HI professionals, end-users, and other actors who must comply with the requirements.

Thank you for the opportunity to comment on this proposed rule. AHIMA remains committed to being a partner to ASTP/ONC in improving data exchange by fostering innovation with common sense, fundamental requirements in the Certification Program and a stable, predictable, information blocking regulatory framework. If AHIMA may provide any further information, or if there are any questions regarding this letter and its recommendations, please contact Andrew Tomlinson, senior director of regulatory and international affairs at Andrew.Tomlinson@ahima.org or Tara O'Donnell, manager of regulatory affairs at Tara.Odonnell@ahima.org.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy and Impact Officer