October 4, 2024

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

Micky Tripathi, PhD, MPP
Assistant Secretary for Technology Policy
National Coordinator for Health Information Technology
Chief Artificial Intelligence Officer (Acting)
Department of Health and Human Services, Office of the National Coordinator for Health IT
Mary E. Switzer Building, Mail Stop: 7033A
330 C Street, SW, Washington, DC 20201

RE: Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability Proposed Rule [RIN 0955-AA06]

Dear Assistant Secretary Tripathi:

The College of Healthcare Information Management Executives (CHIME) respectfully submit our comments on the Assistant Secretary for Technology Policy's (ASTP) Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability (HTI-2) proposed rule as published on August 5, 2024, in the *Federal Register* (Vol. 89, No. 150).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With over 5,000 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve.

Key Recommendations

CHIME appreciates the opportunity to comment on ASTP's "Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability" proposed rule – henceforth referred to as "HTI-2" or the "HTI-2 proposed rule."

With the insight CHIME and its members have from being at the forefront of health IT issues, we urge ASTP when finalizing the HTI-2 proposed rule – to at a minimum, delay the proposed timelines, prioritize reducing provider burden and burden across the whole healthcare continuum when implementing provisions of the 21st Century Cures Act and updating the ONC Health IT Certification Program (Certification Program).

In our comments, we respond to various issues raised in the proposed rule and offer recommendations to constructively improve the final rule. We thank you for the opportunity to

share our views on ASTP's proposals. CHIME believes the following areas are important for ASTP to consider when finalizing the HTI-2 proposed rule.

- **Impact & Burden on Healthcare Industry**: Our concerns regarding the inadvertent, but substantial burden on the healthcare industry – especially hospitals and healthcare delivery organizations (HDOs) – are detailed throughout our comments below.
- **Timelines:** We strongly recommend that no timelines be imposed any sooner than 24 months following publication of the final rule.
- **Proposed Patient, Provider, and Payer Application Programming Interfaces (APIs):** CHIME members believe that there must be participation by all payers, not just "impacted payers"; greater standardization and a thorough analysis on the security implications is needed; and a more thorough review of the provider burdens that will ensue without addressing practical considerations.
    - **Interagency Coordination:** CHIME encourages ASTP and the Centers for Medicare and Medicaid Services (CMS) to continue to coordinate – including engaging with the healthcare industry – to ensure that this proposal and CMS's ongoing efforts around these APIs do not add redundancy and burden to hospitals and healthcare systems.
- **The United States Core Data for Interoperability Standard (USCDI) v4:** CHIME believes that ASTP should consider an alternate effective date of January 1, 2029. We have concerns that there is a significant cost burden that will stem from implementation of USCDI v3 and USCDI v4. Additionally, we encourage ASTP to prioritize and expedite the development of comprehensive vocabulary standards for all USCDI v4 elements, particularly where existing standards are limited or absent (e.g., "Care Team Member Identifier").
- **Revised End-User Device Encryption Criteria:** CHIME members are concerned that imposing uniform cybersecurity certification criteria will lead to unintended consequences, as detailed in our comments below. Applying a one-size-fits-all approach to cybersecurity policies may undermine the goal of enhancing electronic health information (EHI) and personally identifiable information (PII) security, instead introducing new vulnerabilities, escalating costs, and adding unnecessary complexity to critical systems essential for safe and reliable patient care across the U.S. Thus, we strongly oppose this proposal.

By creating this opportunity for stakeholders to engage – especially those with the subject matter and expertise in healthcare information technology (IT) – throughout the policy development and implementation process, we believe invaluable input will be garnered.

General Comments & Detailed Recommendations

CHIME appreciates ASTP's ongoing efforts to advance health data exchange and interoperability. This proposed rule seeks to advance interoperability, improve transparency, and support the access, exchange, and use of EHI through proposals for: establishing a new baseline version of the USCDI; standards adoption; adoption of certification criteria to advance public health data exchange; expanded uses of certified application programming interfaces (APIs), such as for electronic prior authorization (ePA), patient access, care management, and care coordination; and information sharing under the information blocking regulations.

The proposed rule would also purportedly "update the ONC Health IT Certification Program to enhance interoperability and optimize certification processes to reduce burden and costs."

The healthcare sector has evolved significantly to help shape, adapt, and adopt technology to support key healthcare goals around the exchange of information, privacy, security, and equity. ASTP has taken a laudable approach in their commitment to interoperability and promoting consistent health IT standards. However, while we have achieved tremendous progress, many gaps and challenges persist alongside new and emerging ones for the healthcare industry, providers, payers, and patients. It is paramount that as we continue this journey that we do not impose significant burdens on providers.

CHIME has and continues to be a staunch champion when it comes to the need for the use of technology standards aimed at facilitating better patient care. However, CHIME is concerned that this proposal could constitute a significant burden on mid-sized, small, rural, and under-resourced providers. Many hospitals and healthcare systems are experiencing significant challenges related to the ongoing implementation of the HTI-1 final rule, cybersecurity attacks, budgetary restraints, and workforce shortages. Therefore, CHIME is concerned that this proposal could inadvertently hinder the success of advancing interoperability across the healthcare continuum.

Impact on CHIME Members

CHIME has significant concerns regarding the cost-estimate ASTP has prepared in the regulatory impact analysis (RIA), as directed by Section 3(f)(1)) of E.O. 12866, that states: "**The average hospital user of certified health IT could be expected to face up to $69,203 on average additional costs associated with implementing technology that adopt these policies.** The average clinician practice site could be expected to face up to $2,250 on average additional costs associated with implementing technology that adopt these policies [emphasis added]."

Additionally, ASTP states: "We estimate that the total annual cost for this proposed rule for the first year after it is finalized (including one-time costs), based on the cost estimates outlined above and throughout this RIA, would result in $431.1 million. The total undiscounted perpetual cost over a 10-year period for this proposed rule (starting in year two), based on the cost estimates outlined above, would result in $398.1 million. We estimate the total costs to health IT developers to be $829.2 million."

ASTP states: "Based on our previous modeling for the ONC Cures Act Final Rule in 85 FR 25642, we assume that one-third of the estimated costs will be passed on to hospitals, with the remainder to clinician practices." **CHIME believes this modeling is outdated and inappropriate for this rulemaking. Nevertheless, one-third of $892.2 million amounts to $297.4 million—a significant burden, especially when combined with the financial and time costs still being incurred from the final HTI-1 rulemaking.**

Further, ASTP states that they:

> *Acknowledge that these estimated costs may not be borne solely by the developers of certified health IT and could be passed on to end-users through health IT developers' licensing, maintenance, and other operating fees and costs. We assume health IT developers may pass on up to the estimated costs of these policies, but not amounts above those estimated totals. We request comment on the increase in software licensing costs and other fees resulting from these proposals and if ongoing licensing costs and fees already consider the costs of meeting new regulations and certification requirements (i.e., some or none of the estimated costs of this proposed rulemaking would be passed on to technology end-users.)*

CHIME members believe that the ASTP estimated cost that will be passed on to our members – but not "amounts above" this estimation at $69,203, is grossly underestimated.

Not only will the costs be insurmountable for some – especially safety-net, critical access hospitals (CAHs), and rural hospitals and health systems – but our members will need to address EHR usability challenges and concerns as a result of this proposal. Further, they will need to create and implement significant clinician and staff education efforts. Additionally, these proposals will necessitate arduous workflow and configuration of EHRs, which requires individual EHR system usability and safety testing – a resource intensive and costly undertaking. **CHIME strongly believes that this proposal will – or as ASTP "assumes" – impose a substantial financial burden on our members in terms of passed-on costs from these requirements as well as implementation within their organizations.**

ASTP states that they are clear in their analysis and estimates of costs that they "do not assess the costs on healthcare providers to use this technology. This may include changes to how the provider electronically documents information in the medical record, changes to workflow, or how technology is implemented by a provider and at a particular healthcare delivery site. The costs estimate the expected burden on health IT developers to develop and provide the revised technology to their users, not the expected burden on users to use the revised technology […]."

However, notably – as ASTP acknowledges, "these policies first require effort by developers of certified health IT to reflect them in their software, ***they must then be implemented by end-users to achieve the stated benefits*** [emphasis added] – to improve healthcare delivery and the overall efficacy of the technology to document, transmit, and integrate EHI across multiple data systems."

Hospitals and healthcare systems across the country are already operating on slim margins. Given their limited resources, this proposal could also inadvertently – yet significantly – impact the types of services offered by our members. For instance, while surgical volume may generate revenue, services like behavioral health might not be as financially sustainable. Thus, an unintended consequence of additional financial burdens on these already razor-thin margins could be the reduction or elimination of essential services that are critical to the well-being of the communities and patients our members serve.

CHIME strongly believes that advancing interoperability will improve healthcare, but reducing financial burden and complexity must take a front seat. As proposed, we are concerned that these policies, while well-intended, will not achieve this goal. Furthermore, it could threaten to upend access to care which is already seeing erosion among some providers due to the aforementioned challenges.

Finally, imposing mandates of this magnitude disproportionately impact some providers in our sector more unevenly – especially safety-net providers and long-term and post-acute care providers who never received EHR incentives. While the Health Information Technology for Economic and Clinical Health (HITECH) Act[1] made significant investments in certain areas of our sector, more robust funding is needed to improve interoperability across the entire care continuum.

[1] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

Proposed Timelines

In April of 2023, ASTP proposed the "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing" proposed rule, referred to as "HTI-1" or the "HTI-1 proposed rule." The HTI-1 final rule was released in December of 2023, and published in the *Federal Register* on January 9, 2024. However, it was corrected and given an effective date of March 11, 2024.[2]

By December 31, 2024, developers with health IT certified to the clinical decision support certification criterion adopted at 170.315(a)(9) must: Update their certificate(s) for the decision support interventions certification criterion at 170.315(b)(11); and Provide such certified health IT to customers. Further, by this same date, Certified API Developers must publish their customers' service base URL information (FHIR Endpoints) according to specific adopted standards. In other words, by the end of this calendar year, health IT developers must update and provide to their customers certified health IT that conforms to new and revised standards and certification criteria included in the HTI-1 final rule. There are a multitude of other deadlines in the HTI-1 final rule, which vary and extend into calendar year 2029.

This proposed rule – published in the *Federal Register* on August 5, 2024 – imposes an overwhelming number of additional deadlines, which, when combined with the finalized deadlines in HTI-1, create an unmanageable burden for our members and their EHR vendors. Therefore, CHIME members believe that collectively, the timelines in this proposal – are overly ambitious at best, and aggressive and detrimental at worst.

Many of our members are extremely concerned about the proposed timelines; their EHR vendors must comply with the magnitude of policies in this proposed rule. They are unsure if their EHR vendor will realistically be able to meet these deadlines – and, in turn, their organizations will be unable to support and financially bear the burden of the continuous, ongoing series of upgrades. **The timelines need to be extended, and the operational expenses passed onto hospitals and healthcare systems should be limited.**

We recommend that ASTP implement reasonable timelines that take into account not only the timelines required for both EHR vendor development and provider training and implementation, but also one that factors in workforce shortages and other competing mandates, including existing ones (i.e., providers are still wrestling with implementing HTI-1, which was effective less than seven months ago), and forthcoming ones. Additionally, ASTP should strongly consider the significant financial burden this proposal – and the HTI-1 final rule – will impose on our members over a short period of time. Therefore, we strongly recommend that any timeline in this proposed rule not be effective any sooner than 24 months following the publication of the final rule.

The HTI-2 proposals will require that our members develop guidelines, policies, procedures and gather the data required to meet the requirements along with their vendor partners. Once that work is complete, the decisions need to be implemented and communicated across their organizations. This work will take a minimum of 18 to 24 months. **Furthermore, ASTP must ensure that hospitals and healthcare systems have the time needed to understand the significance of**

[2] 89 FR 8546

the policies included in the final rule, are prepared to meet its requirements, and have the technology and funding to support implementation.

We respectfully request that ASTP thoroughly reconsider the proposed timelines, as they would significantly increase the considerable time providers must spend navigating these regulatory changes and their rapidly evolving requirements.

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

CHIME members remain steadfast in their commitment to being partners with their patients to facilitate greater – and safer – interoperability. It is critical that regulations do not inadvertently create overly duplicative requirements, penalize healthcare providers unfairly, and add burden.

Patient, Provider, and Payer APIs

In the CMS Interoperability and Patient Access Final Rule[3] and the CMS Interoperability and Prior Authorization Final Rule,[4] CMS requires impacted payers to use certain standards and implementation guides (IGs) which ASTP has adopted in § 170.215, as well as the USCDI standard in § 170.213. Specifically, CMS has finalized technical requirements for the following APIs: Patient Access API, Provider Access API, Payer-to-Payer API, Prior Authorization API, and the Provider Directory API. In the CMS Interoperability and Prior Authorization Final Rule, CMS also recommended a number of IGs that may be used to support effective implementation of the required payer APIs.

ASTP is proposing certification criteria[5] for Health IT Modules that can be used to support more effective exchange of clinical, coverage, and prior authorization information. The proposed certification criteria, if finalized, would support the availability of health IT that can enable payers and healthcare providers to meet requirements established in the Interoperability and Patient Access Final Rule[6] and the Interoperability and Prior Authorization Final Rule.[7] As part of their proposals, ASTP includes further discussion of how each proposed certification criterion would support the availability of information and enable functionality CMS has identified as part of corresponding requirements. ASTP intends to continue to work with CMS in the future to ensure Health IT Modules certified to the proposed criteria enable efficient and effective support for CMS policies.

CHIME appreciates that ASTP has proposed the establishment of certification criteria to align with the CMS established API requirements and recommendations in the Interoperability and Prior Authorization final rule. In CHIME's comments to CMS' Interoperability and Prior Authorization proposed rule, our feedback could and can be distilled into a key topic – standardization. Critically, our members believe there must be a

[3] 85 FR 25510 through 25640
[4] 89 FR 8758 through 8988
[5] § 170.315(g)(30) – (36)
[6] 85 FR 25522 through 25569
[7] 89 FR 8768 through 8946

standardized process in place prior to implementing and/or mandating any technology standards.

The "impacted payers" included in the above regulations from CMS are Medicare Advantage (MA) Organizations; State Medicaid and Children's Health Insurance Program (CHIP) agencies; Medicaid Managed Care Plans and CHIP Managed Care Entities; and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs). **This means plans that are not considered "impacted payers" include Medicare fee-for-service (FFS); QHP issuers that offer stand-alone dental plans; Federally facilitated small business health options program exchanges; state-based exchanges; and employer-sponsored commercial plans.**

There are several practical issues that must be addressed before the efficiencies envisioned by ASTP and CMS are realized: 1) there must be participation by all payers, not just "impacted payers"; 2) greater standardization and a thorough analysis on the security implications is needed; and 3) a more thorough review of the provider burdens that will ensue without addressing these practical considerations.

Currently, with the ongoing evolution of healthcare data exchange facilitated by APIs it is essential to ensure that the data needed is standardized and ready to be exchanged via API, and that the burden of implementation is jointly placed on the vendors and payers, not just the providers. When referring to "standardization" outside of "technology standards" throughout our comments, we are broadly referring to standardization in terms of consistency, including consistent processes, timelines and deadlines, as well as shared burden and shared benefit.

Without all commercial payer plans being subject to these requirements – value, benefit, and effectiveness will likely remain low for providers, as many of their patient populations fall into the Medicare FFS and private payer categories.

The proposed certification criteria for APIs related to patients, providers, and payers, are not mandatory for payers. As ASTP notes, "CMS has not proposed to require that impacted payers subject to the API requirements in the CMS Patient Access and Interoperability and CMS Interoperability and Prior Authorization Final Rules obtain or implement Health IT Modules certified to the criteria in this proposed rule." ASTP also notes "that CMS has not identified health IT certified to the "prior authorization API – provider" criterion proposed[8] as necessary to complete the finalized electronic prior authorization measures in the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of MIPS."

While ASTP and CMS encourage greater interoperability, the lack of a legal mandate requiring payers to use certified health IT modules leaves a critical gap in achieving the full benefit of these proposals. Without enforceable standards that compel payers to adopt certified systems, the onus will continue to fall disproportionately on providers. This legal asymmetry may lead to fragmented adoption of these proposals, further limiting the anticipated efficiencies.

As proposed, the responsibility of ensuring interoperability rests heavily on hospitals and healthcare providers, who must ensure their systems can interface with multiple payers. Given the lack of standardization among payer systems, healthcare providers may have to invest in additional technology or staff training to manage the various workflows, further increasing their

[8] § 170.315(g)(34)

operational costs. Additionally, having different processes for the different payers will add complexity to the workload of health IT positions that are already difficult to fill for CHIME members. **These additional burdens, coupled with the complexities of integrating with non-certified systems, will offset much of the projected savings and add new layers of administrative complexity – ultimately leading to minimal burden or financial relief for hospitals and healthcare providers.**

CMS has not finalized or proposed requiring impacted payers to adopt or implement Certified Health IT under the Program. As this proposal notes in the RIA:

> *The CMS Interoperability and Prior Authorization final rule describes how the implementation of electronic, standards-based prior authorization and other information exchange integrated into the EHR can reduce burden on patients, providers, and payers resulting in an estimated $15 billion of savings over ten years. The proposals described below will help establish and build these standards and other technology into certified health IT for use by healthcare providers and others to achieve these estimated savings.*
>
> *The benefits, both quantifiable and not quantifiable, articulated in this impact analysis have the potential to remove barriers to interoperability and EHI exchange for all these healthcare providers.* ***Though these policies first require effort by developers of certified health IT to reflect them in their software, they must then be implemented by end-users to achieve the stated benefits – to improve healthcare delivery and the overall efficacy of the technology to document, transmit, and integrate EHI across multiple data systems*** *[emphasis added].*

Payers, unlike healthcare providers, do not directly use certified EHR systems to deliver care. Instead, they operate within their own systems, which are not held to the same certification and interoperability standards required of hospitals and healthcare providers. This disconnect creates inefficiencies in the exchange of prior authorization requests and responses. As payers are not subject to the same regulatory standards for EHR integration, their systems may be less equipped to handle the exchange of data seamlessly, thus undermining the streamlined workflow ASTP and CMS have envisioned. **Without mandatory alignment of payer systems with certified EHRs, the full potential for reducing administrative burden and the cost savings CMS estimates may never be realized.**

ASTP reiterates that, if finalized, certification to these criteria would be available for health IT developers (which may include payers and other developers providing technology to payers) seeking voluntary certification and any requirements for a certification criterion are only required in the sense that they are necessary to achieve certification. ASTP does not establish requirements for whether and in what ways patients, health care providers, payers or others use health IT. Instead, they enable the certification of Health IT Modules that may support a wide range of users. In this way, the Program helps to advance standards for certified Health IT Modules and increases the availability of interoperable health IT across healthcare and health related use cases.

As ASTP states: “The proposals in this proposed rule would not establish requirements for health IT beyond those Health IT Modules submitted for certification for these criteria under the Program, nor does the availability of these certification criteria require any individual or entity to use certified health IT, including payers subject to the CMS requirements.” Further, ASTP notes that their “goal in proposing these certification criteria and the related implementation specifications is to support health IT developers building these capabilities (and customers implementing them) in a manner

that is consistent with nationally recognized standards and supports testing and conformance to these standards through the ONC Health IT Certification Program."

While the vast majority of CHIME members are obligated to utilize Certified EHRs to participate in CMS programs including the Medicare Promoting Interoperability Program and the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS) – payers do not face the same obligation to adopt certified health IT systems. This leads to variability in how payers handle prior authorization requests, often forcing providers to use disparate systems or manual processes. **As a result, providers will likely continue to experience inefficiencies, including delayed authorizations and the need to manually re-enter or reconcile data, which can increase administrative costs and time. CHIME members believe that this ongoing friction in the EHI exchange process will erode the anticipated savings and efficiency gains outlined in this proposal.**

Without making these proposals a joint responsibility across stakeholders specifically across the entire ecosystem of healthcare payers – not simply a subset – ASTP and CMS are simply shifting more burden onto providers that are already severely strained, understaffed, and under-resourced. While we do not believe that is the agency's intent, we nonetheless believe that in practice this is what will occur.

Given the intersecting nature with CMS' final rules, CHIME urges ASTP to, at minimum, work with CMS to require impacted payers adopt and use certified payer APIs as a condition of their participation in CMS programs. **Currently, the Health Level Seven International (HL7®) IGs are only recommend by CMS – not required – and adding this requirement will further increase and incentivize payers to truly and effectively implement the required payer APIs.**

CHIME members believe that without greater standardization, integration understanding, and participation by all payers, these proposed APIs cannot lead to the efficiencies ASTP envisions and most certainly will not better enable providers to coordinate care for their patients and for patients to communicate with their providers. It furthermore could constitute a significant burden on many providers – especially long-term and post-acute care providers.

In many instances, each payer has the option to choose how to meet the final rules' indicated "legal requirements", such as providing a patient list to a provider. By continuing to allow each payer the option to choose their own process, a significant burden is placed on providers. For example, providers that accept multiple different payers will continue to face scenarios where retrieving a patient list could include as many as ten – if not more – different processes. If ASTP chooses to simply ignore the shared responsibilities of payers – and legal obligations – and require equal participation of payers, these APIs will create additional burden on providers and would render the proposal's stated intention to reduce provider burden completely moot. Further, without requirements for all payers to utilize the Patient Access API, Provider Access API, Payer-to-Payer API, Prior Authorization API, and the Provider Directory API, there remains limited applicability for providers to utilize them, as it would not impact a significant portion of their patient population.

Additionally, if each payer creates its own specification for how providers should access their respective API, then a scenario exists where a provider needs to maintain a multitude of specifications to connect to each individual API – this would defeat the intent of standardization. With each connection implementation different, providers would inherit a significant burden of having to work through potentially 10 or more different APIs for as many as twenty, and even up to eighty, different payers and connection specifications. Exponentially increasing the burden to

retrieve information has the potential to discourage healthcare providers from utilization of the Provider Access API. **As proposed, ASTP puts the onus of success on providers rather than the impacted payers – and standards of providers are not the same standards of payers. CHIME members are already burdened with navigating multiple payer workflows and processes, thus, this proposal actually adds to an already burdensome process.**

Furthermore, although CMS projects significant savings from electronic, standards-based prior authorization integrated into EHRs, the reality is more complex. Since payers are not the end-users of certified EHRs, hospitals and healthcare providers are likely to face ongoing challenges due to inconsistent interoperability, additional operational burdens, and fragmented implementation. These factors make it unlikely that the true benefits or savings will match the estimates put forth CMS' final rule and reiterated in this rulemaking.

CHIME continues to believe that API requirements should be consistent across all stakeholders – providers and payers. EHR vendors need to feed new information into the API, and the API needs to pull this information. Therefore, healthcare delivery organizations (HDOs) will need to change their prior authorization workflows. Then, changes to prior authorization workflows will need to be changed within each individual EHR. Thus, a standardized integration process is critical; the final rule must include the requirements for all stakeholders in order to realize success of these APIs. When measuring the metrics of success, there should be metrics of success for all stakeholders; measuring success in these policies should be non-punitive for providers.

In articulating our concerns, we want to reiterate that you will get no stronger champion than CHIME when it comes to the need for the use of standards aimed at facilitating better patient care. However, without making the Patient Access API, Provider Access API, Payer-to-Payer API, Prior Authorization API, and the Provider Directory API a joint responsibility across stakeholders specifically with the entire ecosystem of healthcare payers – not simply a subset – ASTP will simply shift more burden onto providers that are already severely strained, understaffed, and under-resourced.

<u>The United States Core Data for Interoperability Standard (USCDI) v4</u>

Based on feedback received through the ONC New Data Element and Class (ONDEC) submission system and other public feedback, ASTP released Draft USCDI v4 in January of 2023. Draft USCDI v4 included 20 new data elements and one new data class as well as updated minimum standard code set versions. ASTP then finalized and released USCDI v4 in July 2023, with four additional data elements in the Medications data class.

ASTP is proposing to update the USCDI standard[9] by adding USCDI v4 and by establishing an expiration date of January 1, 2028 for USCDI v3 for purposes of the Certification Program. In other words, as of January 1, 2028, any Health IT Modules seeking certification would need to be capable of exchanging the data elements that the USCDI v4 comprises, and update and provide customers with such technology.

CHIME agrees that expanding the data elements included in USCDI would increase the amount and type of data available to be used and exchanged through certified health IT. However, the newest baseline standard for the ONC Health IT Certification Program, USCDI v3, has not even taken effect yet – and will not until January 1, 2026. ASTP has proposed that the new required

[9] § 170.213

version of USCDI v4 will have an effective date of January 1, 2028. **Two years is an extremely limited timeframe for hospitals and healthcare systems to address both the workflow challenges and the significant financial costs involved. Therefore, CHIME believes that ASTP should consider an alternate effective date of January 1, 2029.**

CHIME members have expressed concern that there is a significant cost burden that will stem from implementation of USCDI v3 and USCDI v4. For example, members have noted that with each new data element added to the USCDI, EHR vendors often charge healthcare providers for a new API. **Given the already substantial cost and burden of the HTI-1 final rule – as well as this proposed rule – for healthcare providers over a short span of time, we urge ASTP to recognize that there are "hidden" financial burdens throughout these policies.**

Additionally, CHIME respectfully requests that ASTP continue to maintain a consistent and clear process for adopting new USCDI versions – which will assist providers and their EHR vendors maintain alignment with changing standards. Ensuring this process is done in a way that makes periodic adoption of new versions practicable should remain a priority for ASTP.

One of the data elements included in USCDI v4 – "Care Team Members: Information about a person who participates or is expected to participate in the care of a patient" – raises significant concerns for CHIME members. Specifically, the "Care Team Member Identifier," a "sequence of characters used to uniquely refer to a member of the care team. Examples include but are not limited to National Provider Identifier (NPI), and National Council of State Boards of Nursing Identifier (NCSBN ID)."[10]

Our members believe that it is crucial that ASTP provides clarity on what qualifies as an "identifier"—whether it's the billing NPI, the provider ID number assigned by a payer, or an identifier issued by an organization. Given that an NPI may not apply to all care team members, there needs to be standardization in the definition of an "identifier." Clinicians working in facility-based settings (e.g., hospitals and other post-acute care settings) may bill under the facility's NPI. Additionally, some healthcare professionals, like physical therapist assistants working under the supervision of a physical therapist, might have their services billed under their supervisor's NPI instead of their own. Further, not all care team members have a uniform identifier, or their identifiers may vary. Until there is a national, standardized solution for "Care Team Member Identifier", we strongly urge that ASTP ensure that this data element is optional.

Finally, CHIME encourages ASTP to prioritize and expedite the development of comprehensive vocabulary standards for all USCDI v4 elements, particularly where existing standards are limited or absent. Establishing robust, universally accepted terminology is critical to ensuring data consistency, interoperability, and the advancement of health information exchange across the nation.

<u>The Cybersecurity Landscape</u>

CHIME also urges ASTP to take into consideration the increasingly complex cybersecurity landscape hospitals and health systems must navigate and urge the agency to take this into consideration when finalizing this proposal. Hospitals and healthcare systems are spending an increasing amount of time, energy and resources navigating this highly challenging and evolving environment, which is an issue we have identified in several previous comment letters and during

[10] *USCDI Data element*. (2022, September 30). https://www.healthit.gov/isp/taxonomy/term/1291/uscdi-v4

conversations with ASTP. **This year has already proven to be incredibly challenging following the Change Healthcare cyberattack.**

On February 21, 2024, Change Healthcare discovered a threat actor gained access to one of their environments. A Russia-affiliated ransomware group known as ALPHV/BlackCat claimed responsibility. This is the most massive cyberattack on our sector to date – much larger than the WannaCry event experienced several years ago – and it wreaked unprecedented havoc on the entire healthcare ecosystem given the data clearinghouse and transaction hub role that Change provides at national scale. The interruption to patient care as well as the financial impact on our members has been devastating. This incident has been likened to the "Colonial Pipeline" of healthcare, highlighting the scale of Change Healthcare's impact with 15 billion healthcare transactions processed annually and touching one in three patient records. The concerns among our members are still ongoing as they recover from this incomparable event; Change Healthcare processes claims on behalf of hundreds of thousands of clinicians and providers – and to date, healthcare providers and patients affected by this breach are so numerous that a specific number is still not readily available.

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. Bringing down a hospital or multiple HDOs at once is a risk for the nation and it shakes the confidence and trust of everyday Americans which is precisely what hostile nation states intend. They are looking to exact both physical, financial, and psychological harm.

Healthcare data and patient information remain lucrative targets for theft and exploitation, particularly through ransomware attacks. Criminal groups and adversarial nation states utilize tactics, techniques and procedures across our Sector – including attacking large, publicly traded companies with far greater resources than most U.S. hospitals and health systems. The overall privacy and cybersecurity landscape has become infinitely more complex for all providers. Cybersecurity attacks are on the rise for providers of all sizes which pose a direct threat to patient safety.

The costs to recover from a data breach in the HPH Sector are staggering – averaging $10 million per incident, which is far higher than any other sector. As a comparison, the costs for a financial entity to recover from a breach are estimated to be $6 million. Healthcare has held the unfortunate title of top costliest industry for breaches since 2011.[11]

According to IBM's "Annual Cost of a Data Breach Report 2024": "The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10 percent spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs totaled USD 2.8 million, the highest combined amount for lost business and post-breach activities over the past 6 years."

The IBM Report also found that over "half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2 percent increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. The number of organizations facing a critical lack of skilled security workers rose dramatically, to 53 percent in

[11] *Cost of a data breach 2024 | IBM*. (n.d.). https://www.ibm.com/reports/data-breach

2024 compared to 42 percent last year. This year's research found a strong link between the worsening skills shortage and higher data breach costs."

Healthcare is and will remain a target for cyberattacks "since the industry often suffers from existing technologies and is highly vulnerable to disruption, which can put patient safety at stake."[9] Additionally, the fallout after an attack has also been shown to impact patient care – one report found that nearly a quarter of organizations suffering a cyber breach experience higher patient mortality rates. In short, cybersecurity is also patient safety.

Cybersecurity challenges and threats that our members are facing are what those who have been active in the cybersecurity landscape have known for years – healthcare is under constant threat and more resources are needed for healthcare providers. **The budget and resources our members would need to allocate to comply with this proposed rule are valuable funds and assets that could otherwise be directed toward critical investments to enhance hospital and healthcare systems' cybersecurity posture and safeguard patient care and patient data. Any investment in cybersecurity for the healthcare sector will be an investment not just in patient safety – but also national security.**

Revised End-User Device Encryption Criteria

To better protect EHI stored in Health IT Modules certified under the Program, ASTP is proposing to clarify the scope of information that needs to be protected in Health IT Modules certified to existing end-user device encryption criterion and revise the order and sequence of existing requirements to include new requirements for server-side encryption.

First, to clarify the scope of EHI that needs to be protected, ONC is proposing that on and after Jan. 1, 2026, the information that must be protected within Health IT Modules include all PII. This includes, but is not limited to, individually identifiable health information meeting the definition of ePHI, regardless of whether the information is held by or for a HIPAA covered entity or entity required to comply with the Privacy Act of 1974[12], as amended.

Second, ASTP is proposing to revise and include new requirements for server-side encryption and include the PII encryption requirements for servers in a way that maintains existing end-user device encryption requirements and applies the existing encryption standard and the default settings requirements broadly in one criterion. ASTP is proposing to rename the existing end-user device encryption criterion to "health IT encryption" to better describe the end-user and proposed server-side requirements together. ASTP is proposing to include the new server-side encryption requirement that must be met on and after January 1, 2026. This new server encryption requirement states that technology designed to store PII must encrypt the stored PII after use of the technology on those servers stops.

ASTP is proposing that the existing encryption standard and default settings requirements apply to the new server encryption requirement. ASTP asserts that pointing to an encryption standard and requiring that default settings be in place for encryption capabilities is consistent with the existing requirements for end-user device encryption. Health IT developers with Health IT Modules certified to this criterion will continue to have traceability. And, if these proposals are finalized, developers with Health IT Modules already certified would only need to consider updates to the applicable

[12] 5 U.S.C. § 552a

encryption standards, server-side encryption, and encryption of any non-encrypted PII for the purposes of maintaining Health IT Module certification in the future.

CHIME members have already taken proactive steps with server-side encryption and view this proposal as redundant, costly, and operationally burdensome. They are already using robust encryption algorithms to secure EHI and PII – and believe this proposal would impose duplicative encryption efforts, which leads to inefficiencies and will waste the existing investments they have already made. Although not yet publicly released, our 2024 Digital Health Most Wired (DHMW) survey revealed that 99% of respondents are already employing encryption at rest (device encryption). The survey encompassed nearly 48,000 facilities, including acute care, ambulatory, and long-term/post-acute care settings. Therefore, we believe this proposal would unnecessarily escalate costs and operational complexity without providing any significant enhancement to data security, ultimately undermining the value of the substantial encryption investments these facilities have already made.

Our members' existing systems are designed to be flexible and scalable, and these additional rigid certification criteria may hinder that adaptability, making them less agile in responding to both internal needs and external cybersecurity threats. Layering encryption in this manner can overcomplicate IT architecture, increasing operational risks and requiring more sophisticated key management systems. **Introducing new encryption keys at the server layer, alongside other layers, as this proposal would do – could actually increase the attack surface for potential breaches, while complicating disaster recovery and access control. Security standards and policies must account for the dynamic nature of cybersecurity threats.**

CHIME members believe that by generalizing cybersecurity policies to fit all health IT systems, this proposed new requirement will fall short of its intended goal of making EHI and PII more secure. Rather, it will inadvertently add new vulnerabilities and increase cost and complexity to mission critical systems required to provide care to patients across the U.S. safely and reliably.

Adding additional layers of encryption at the application level on top of hardware encryption can create complications. It might make it harder to quickly access or recover the data in case of system failures or during disaster recovery efforts. These extra encryption layers can affect the availability of the data – meaning it might be harder for authorized users to access it when needed, which could disrupt operations in a hospital setting where timely data access is crucial. **As many EHR vendors focus on application-level security, they would not – and arguably should not – have the needed level of insight into the underlying storage arrays used by hospitals and healthcare systems. Introducing server-side encryption across various vendor ecosystems without vendor collaboration or awareness could lead to fragmented implementations, increased complexity, and risk of misconfigurations.**

Further, encryption at the server-side level adds significant overhead to storage systems. The process of encrypting and decrypting data requires computational resources, which can strain performance, especially in hospitals and healthcare systems where patients' lives can depend on it. Additionally, the physical security of servers and encryption keys is already highly regulated and enforced within healthcare systems. Thus, the proposed additional server-side encryption does not increase security, especially when existing physical and procedural security measures are already in place. **CHIME members strongly believe that this proposal would result in substantial cost**

to them, and potentially the patients they care for – and strain both their finances and limited health IT workforce.

We believe that ASTP must understand the importance of aligning proposed regulations with real-world operational realities, cost concerns, and the risk-benefit analysis of layering additional encryption controls. Therefore, we strongly urge that ASTP not implement this proposal at all – and instead, maintain the few existing flexibilities for hospitals and healthcare systems to implement the appropriate cybersecurity measures in an already complex landscape, as discussed above in detail.

As noted in the proposed rule, ASTP "is responsible for implementation of certain provisions of the Health Information Technology for Economic and Clinical Health Act[13] (HITECH Act) including: requirements that the National Coordinator perform duties consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that promotes a more effective marketplace, greater competition, and increased consumer choice, among other goals; and requirements to keep or recognize a program or programs for the voluntary certification of health information technology." As ASTP also asserts: "This proposed rule seeks to fulfill statutory requirements; provide transparency; advance equity, innovation, and interoperability; and support the access to, and exchange and use of, EHI."

In other words, the primary purpose of the Health IT Certification Program is to ensure that Health IT Modules meet certain functional, interoperability, and usability requirements necessary to enable safe, efficient, and effective care delivery. Certification focuses on the capacity of systems to handle health data and enable compliance with existing healthcare laws – such as HIPAA.

Cybersecurity, while essential, is a complex and evolving field that demands flexibility and continuous updates based on the latest threats and technologies. Hardware encryption is widely adopted by our members; it is a robust control that ensures data security by safeguarding physical assets. **ASTP is proposing mandating additional software-level encryption, while the underlying security needs this proposal is attempting to address are currently being more effectively protected by hardware encryption.**

ASTP's proposal is simply an added layer that would pose unnecessary operational burdens without providing the proportionate increase in data protection. Further, enforcing static cybersecurity controls through the certification Program would limit our members and health IT developers' ability to adapt to emerging security challenges in real-time. Instead of ensuring core functionality, this proposal is inserting overly prescriptive regulation in areas where continuous innovation and improvement are needed – and significant funding is already being spent.

Additionally, our members, particularly those that are more well-resourced, already have mature cybersecurity protocols tailored to their unique environments. These include multi-layered defenses such as data encryption, intrusion detection, network segmentation, and physical security measures. **By imposing specific cybersecurity policies through the certification program, ASTP would be burdening healthcare providers of all sizes and financial means by forcing them into rigid compliance requirements that do not align with their individualized cybersecurity strategies. CHIME strongly urges ASTP to abandon this proposal entirely, as it would undermine the ability of healthcare providers to implement customized**

[13] Pub. L. 111-5, Feb. 17. 2009

cybersecurity strategies, impose unnecessary burdens on organizations of all sizes – ultimately diverting resources away from meaningful security improvements.

Mandating this specific cybersecurity policy through the Health IT Certification Program would stifle innovation, increase costs, and place unnecessary operational burdens on our members. Server-side encryption decisions should instead remain within the domain of each hospital or healthcare system, allowing them to implement appropriate, risk-based security measures that align with their operational and technological environments. Certification should focus on system functionality and interoperability, while cybersecurity is best addressed through other mechanisms that are more adaptive and tailored to the needs of diverse organizations.

Furthermore, this proposal directly conflicts with ongoing work – which CHIME members broadly support – being done by the White House's Office of the National Cyber Director (ONCD) to lay the groundwork for a comprehensive policy framework for cybersecurity regulatory harmonization. The ONCD is working in close collaboration with and across all critical infrastructure industries and other stakeholders in order to achieve better cybersecurity outcomes while lowering costs to businesses and their customers.[14]

CHIME appreciates that ASTP is working to protect EHI and PII. However, server-side encryption for each of our members is unique and therefore, any requirements, challenges, and the standard should reflect this. If ASTP is to move forward with this proposal regardless of feedback, any finalized encryption standard and default settings requirements that apply to the new server encryption requirement must allow for flexibility to implement controls, or alternate countermeasures based on risk – rather than a one-size-fits-all approach. While some systems could easily be updated to enable encryption, others may require significant investment – and our members believe that offering flexibility and alternative countermeasures could achieve the same goals as ASTP posits in this proposal.

Additionally – and critically – ASTP is proposing to include the new server-side encryption requirement that must be met on and after January 1, 2026. Given that this proposal will necessitate most organizations to procure new hardware and servers to maintain current server performance standards, this timeline is unrealistic and concerning. Even without considering the required development and implementation efforts, this process will be both costly and time-intensive. **Therefore, CHIME members strongly believe that it should be no earlier than January 1, 2028 – which offers alignment with many of the other proposed deadlines in this rulemaking. However, we reiterate that CHIME strongly recommends that all timelines in this proposed rule not be effective any sooner than 24 months following the publication of the final rule.**

Conclusion

CHIME members remain steadfast in their commitment to using technology to deliver high-quality care and facilitating interoperability and appropriate and secure access to records across the care continuum. Furthermore, CHIME has consistently been supportive of ASTP's efforts towards improving technologies used by clinicians.

[14] Office of the National Cyber Director. (2024). *Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information.* https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf

CHIME respectfully requests that ASTP take our comments on this proposal into consideration. While our members are fully capable and strong supporters of achieving significant progress towards true interoperability, it is important to acknowledge that we cannot accomplish everything simultaneously. A strategic, phased approach will allow us to address key priorities effectively without overextending financial and workforce resources.

Understanding the long-term ramifications of these proposed policies is critical, and CHIME urges ASTP to ensure these proposals do not inadvertently pass down burden onto hospitals and healthcare systems. This remains an extremely concerning indication, especially for our members that are under-resourced, rural, facing workforce shortages and burnout – all while serving the most vulnerable patients.

CHIME members are executives and senior healthcare IT leaders; thus, we are offering to continue to serve as a resource to ASTP as they continue towards the goals of this proposal – to advance interoperability, improve transparency, and support the access, exchange, and use of EHI.

In closing, we would like to thank you for providing the opportunity to comment and CHIME appreciates the chance to help inform the important work being done by ASTP. We look forward to continuing to be a trusted stakeholder and resource to you and continuing to deepen the long-standing relationship we have shared.

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

Sincerely,

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