

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809 | <u>www.ahima.org</u> | 312.233.1100

June 16, 2023

Dr. Micky Tripathi National Coordinator Office of the National Coordinator for Health Information Technology 330 C St SW Washington, DC 20024

Dear National Coordinator Tripathi:

On behalf of the American Health Information Management Association (AHIMA[®]), I am responding to the Office of the National Coordinator for Health Information Technology (ONC) *Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1)* proposed rule, as published in the April 18, 2023 *Federal Register.*

AHIMA is a global nonprofit association of health information (HI) professionals with more than 67,000 members and more than 100,000 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 providers. Our leaders work at the intersection of healthcare, technology, and business and are found in data integrity and information privacy job functions worldwide.

Following are our comments and recommendations on selected sections and requests for information of the HTI-1 proposed rule.

III. ONC Health IT Certification Program Updates

A. "The ONC Certification Criteria for Health IT" and Discontinuing Year Themed "Editions"

AHIMA supports the proposal to rename all certification criteria as "ONC Certification Criteria for Health IT" and remove "editions" from the program. This will lead to more efficiency in implementing updates to recognize standards advancement, voluntary use of standards between updates, incremental updates rather than system overhauls, and reasonable timelines. We agree with ONC that this change would help healthcare organizations and providers more easily identify which certification criteria are necessary for participation in other US Department of Health and Human Services (HHS) programs, including the Medicare Promoting Interoperability Program.

C. New and Revised Standards and Certification Criteria

1. The United States Core Data for Interoperability Standards (USCDI) v3

AHIMA applauds the proposed advancement to USCDI v3. We are particularly supportive of the new data classes and elements included in v3, such as the social determinants of health (SDOH) goals, care team member details, health insurance information, and various health status data elements. These new elements will support the providers' ability to gather and exchange all the information needed to make the best care plans for their patients. AHIMA has been an active participant in shaping USCDI v3 by providing input¹ to ONC on the addition of specific elements and classes to move to a more interoperable, patient-centered health system. We recommend ONC provide support to providers and their staff to implement these changes and ensure SDOH data can be collected, used, and shared appropriately. We also urge ONC to work with electronic health record (EHR) and health IT vendors and providers to determine if the January 1, 2025 deadline is realistic for provider operations and minimally disruptive to patient care.

When SDOH data is appropriately collected, used, and securely shared, the patient's entire healthcare team can gain insight into the patient's medical and non-medical story, allowing them to collaborate on improving the patient's health outcomes and well-being. In 2022, AHIMA partnered with NORC at the University of Chicago to study the operational realities of how SDOH data is collected, coded, and used in real-world healthcare settings.² Key findings included that nearly eight in 10 healthcare organizations collect SDOH data but face challenges related to the collection, coding, and use of this data, stemming from a lack of standardization and integration of the data, insufficient training, and limited use of SDOH data.

AHIMA launched <u>Data for Better Health</u>[™], a multi-year strategic initiative aiming to provide tools, resources, and education to support a better understanding of the importance of SDOH data and how it can be used to improve health and healthcare outcomes.³ We encourage ONC and other agencies to continue to partner with standards-setting organizations, health information professionals, and healthcare providers to establish standardized, clinically valid, and actionable SDOH data elements for collection, sharing, and use. The additional data elements in USCDI v3 are a great first step. AHIMA looks forward to ONC's continued leadership on improving standardization, providing support and resources for providers, and leading collaborative efforts on improving the collection, use, and exchange of SDOH data. We stand ready as a key partner in this effort.

5. Decision Support Interventions and Predictive Models

AHIMA supports the proposal to incorporate new requirements into the Certification program for Health IT Modules that support artificial intelligence (AI) and machine learning (ML) technology to increase transparency and we applaud ONC for filling a regulatory gap related to AI and ML. We encourage ONC to ensure this process can develop and advance as AI and ML evolves. Information included in the proposed transparency requirements is just one part of quality determination and we encourage ONC to include other elements such as the ability of AI and ML technology to continually evaluate performance and risks by responding to feedback and adjusting accordingly. This is important in acknowledging and working to avoid biases that may be ingrained in AI and ML technology.

AHIMA supports ONC's goal of making information about AI and ML technologies in the context of predictive decision support interventions (DSI) publicly available. Transparency and awareness are critical first steps in addressing system flaws and working towards improvement. However, ONC must consider the ability of

¹ Available at: <u>https://www.ahima.org/media/4tal5ohx/final-ahima-uscdi-v3-comment-letter_042022.pdf.</u>

² Available at: <u>https://ahima.org/media/03dbonub/ahima_sdoh-data-report.pdf.</u>

³ Available at: <u>https://www.ahima.org/advocacy/data-for-better-health/.</u>

providers, especially overburdened, small, and under-resourced providers, to evaluate this transparency data and make any decisions regarding its use. Further, if these technologies are already built into a provider's EHR system and hosted by the vendor, providers may not have the ability to choose whether to use, or request change of, a particular predictive DSI based on transparency information. We applaud ONC for proposing requirements focused on incentivizing vendors to provide this information in a standardized format and provide educational resources to help practices understand this data and use it appropriately. As ONC continues to hone these provisions AHIMA recommends the agency look for opportunities to maximize the ability for providers to exercise choice in the DSIs available to them and functionality allowing providers to request changes to DSI functions.

b. Summary of Proposals

AHIMA supports the replacement of the clinical decision support (CDS) criterion and the proposal to add a new certification criterion titled "decision support interventions (DSI)." It is important for ONC to regularly review and update previous regulation to conform to changes in the technology used within the healthcare continuum. ONC's work to update the CDS criterion to include the additional ML and AI algorithms is an important step in reacting to the new advancements in ML and learning algorithm technology available to assist in all areas of the medical field. It is important to note however, that CDS is a very specific and much different technology used throughout the provider community to assist in diagnosing patients. While CDS may be an extension of DSI, the specificity and the organizational policies built around CDS technology warrants the continued existence of a certification criteria separate from DSI. We understand this may create additional regulatory burden, but we feel it is important to ensure CDS, as we know it today, continues to have careful regulation and transparent deployment.

ONC has pledged throughout this proposed rule to continually evaluate the regulatory requirements related to DSI and modify regulatory requirements as needed to fit a changing technology environment. AHIMA recommends ONC evaluate the definitions of terms such as DSI and CDS as part of that pledge to continually reevaluate. The related definition proposals contained within HTI-1 focus on the present-day realities as well as some future possibilities in healthcare, but the definitions could be used to define DSI technologies beyond healthcare across the government. For instance, healthcare routinely looks to the National Institute of Standards and Technology (NIST) for definitions of key technology terms, and it should be expected industries will do the same with ONC. Reevaluating and revising definitions as needed ensures DSI stays aligned with the technology environment it is requiring the healthcare system to report on.

AHIMA supports the ONC proposal of allowing users to "review what, if any, of the following data elements were used in the DSI: Patient Demographics and Observations data specified in paragraph § 170.315(a)(5)(i), including data on race, ethnicity, language, sexual orientation, and gender identity; SDOH data elements as expressed in the standards in § 170.213; and the data elements of the Health Status Assessments data class as expressed in the standards in § 170.213." It is crucial for the provider community to be able to understand the nuances of how a DSI was created to evaluate if the DSI is the best solution fitted for their patient population. The explosion of conversation around DSIs over the last several years has brought to light the "black box problem."⁴ ONC's proposal of allowing providers to review what is used in the DSI does not fully solve the black box problem but does assist users of DSIs to better understand how it may have arrived at its conclusion. This could allow providers to evaluate and decide if the output of a DSI is correct or if there is a high potential of error due to how it was created.

The requirement to make this information available to review to users, such as providers, is not a perfect solution and the methodology proposed by ONC is not without its flaws. It is important to note that modifying the previous requirements related to CDS alerts to highlight the demographic information used in DSI may lead to alert fatigue

⁴ Available at: <u>https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained.</u>

if finalized as proposed. To better understand the extent of this concern, AHIMA recommends ONC convene a working group of stakeholders that includes developers, providers, and DSI experts to ensure these requirements accomplish the policy goal of providing the transparency ONC seeks to accomplish by proposing this requirement. Recommendations from the workgroup related to DSI alerts should be incorporated into the HTI-1 final rule.

A stakeholder workgroup would also be well suited to answer questions relating to the clinical relevance of having this data available in the EHR system. With relatively few true DSIs, with the exception of CDS, available in the health IT market at the time of this rule's proposal, it is difficult to understand how clinically useful this information is. We recommend ONC task the workgroup to discuss and test the availability of this information to better understand how useful it is to the provider and how it can be more useful at the time of care. At this time, AHIMA believes much of the information on the data elements used by a DSI is more helpful in the purchase and acquisition of a DSI versus during the course of delivering patient care.

Finally, as it relates to the availability of data elements for user review, ONC notes that vendors of Certified EHR Technology (CEHRT) products that create systems that interact with or enable a DSI are not compelled to report on data elements used to create the DSI if the third-party does not make those attributes available. ONC is not within its regulatory jurisdiction to require third parties not subject to the Health IT Certification Program to report information to ONC-Accredited Certification Bodies (ONC-ACBs). It is crucial to understand however, that this gap in regulatory language and applicability leaves open the possibilities for bad actors to use this loophole as a way to reduce their regulatory reporting burden. By doing so, providers may be left in the dark, just as they currently are as it relates to data elements used to deploy DSI. AHIMA recommends ONC work with its federal partners within HHS and other agencies to determine the best course of action to ensure the full scope of DSIs can be understood to help the care continuum understand a product prior to procurement and implementation.

AHIMA applauds ONC for its proposal to require Health IT Modules that, "enables or interfaces with predictive DSIs to employ or engage in and document information regarding their intervention risk management (IRM) practices" and supports the further development of these requirements. The three categories of "risk analysis," "risk mitigation," and "governance" are crucial for understanding the potential dangers a DSI poses to an organization. Providers can utilize this information to determine whether the risks associated with the DSI outweigh the potential benefits the DSI provides to an organization or a patient. Understanding the outcomes of these risk management activities will assist provider organizations with creating policies and procedures around the DSI. These policies and procedures could include details on when a DSI cannot be trusted, how to troubleshoot a DSI if it is providing nonsensical responses, and when something like a "kill switch" should be used on the DSI within a provider's system. It has already been documented that DSIs can "hallucinate⁵" when they are presented with problems they do not have enough information to solve or do not know how to solve. Understanding how developers tested for these outcomes and mitigated them can help providers understand how to do the same if it were to happen in their systems.

In the proposed rule, ONC requires this risk management reporting to happen on an annual basis but does not provide a process for the expansion of testing and reporting requirements. Part of the market value of these DSIs is the ability for them to learn and react to the data they come into contact with on a daily basis. That learning and reacting includes instances where the DSI is reacting to live situations and real data. It is crucial ONC requires reporting on how these DSIs evolve to determine if there are risk patterns or similarities in how the DSIs react to certain patient populations or medical situations. By requiring the collection and reporting of this data by the health IT developers, the care continuum can ensure there is constant surveillance of how widely used DSIs are evolving after deployment. This surveillance can potentially identify new problems or unintended outcomes that DSIs are producing and allow the developers to adjust course to ensure they function as intended. If there is no

⁵ Available at: <u>https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9939079/.</u>

regular reporting on the real-world evolution of these DSIs then the yearly reporting becomes less meaningful. Over a period of time the DSI trained in a "white room" closed environment will bear no similarities to the one being used by providers.

Much of the above information could be discovered and reported using robust real-world testing requirements that AHIMA urges ONC to require of certified technologies. Often the certified technologies mandated by ONC and, regularly updated through rulemaking, are rarely tested in a provider environment prior to mandated implementation. ONC can ensure critical real-world testing by requiring DSIs to be tested in real world scenarios with risk management data as part of that process being reported publicly. Real world testing will help both providers and health IT developers better understand these nascent technologies and better prepare for what their eventual widespread use will mean for healthcare as a whole.

It should be noted that some health IT developers may not be able to secure the above discussed information, especially from third parties. AHIMA has noted that requiring compulsory reporting of non-certified technologies is not in ONC's jurisdiction. ONC should evaluate other options to collect this information to ensure the key risk reporting information is not kept private. Trust in DSIs can increase with better transparency around how they intend to function. Lack of trust guarantees skepticism and reactive thinking when challenges or negative outcomes are experienced. ONC must ensure these reporting requirements are met and that if the third party is not able to provide the needed information, the vendor of the certified product must conduct its own risk management exercises.

Finally, with the understanding that DSIs operate in every aspect of the health system, not just patient care, ONC must work to ensure the advantageous work ONC is undertaking is shared throughout the federal government. It will take a whole of government effort to ensure widespread use of DSI technologies is done in a forthright and safe manner ensuring individual safety and quality of life is prioritized. An AHIMA member from a large multi-state health system detailed their experience with utilizing a DSI. They stated the expectation prior to implementation was that utilizing a DSI for revenue cycle would reduce administrative burden. Instead, human error caused the DSI to operate incorrectly, issuing refunds to numerous patients who were not entitled to receive them. Staff time then needed to be dedicated to reviewing the error and correcting it. This process took longer than it would have to issue the refunds if a human had conducted the operation. When looking at the potential problems a DSI could cause within a provider facility, this one is minimal, though it demonstrates the importance of strong oversight, governance, and proper implementation of these DSIs. It is easy to imagine how a poor implementation of a DSI that is reading test results could have life changing implications for patients. For this reason, AHIMA supports ONC's work in this area and implores the agency to do more to ensure it stays ahead of the rapid development of this technology.

c. Proposed Requirements for Decision Support Interventions (DSI) Certification Criterion

i. Proposed Structural Revisions and New Criterion Categorizations

AHIMA asks ONC to clarify whether the proposals related to DSI contained in HTI-1 only related to clinical DSIs and not those used in administrative and non-clinical functions within the provider organizations. AHIMA members were asked to describe the types of DSIs they interact with on a regular basis. All of the examples were of a nonclinical variety. Those technologies included DSIs that assisted in the release of information (ROI), patient matching, clinical document integrity (CDI), and scheduling. Most of these DSIs, with the exception of patient matching, are outside the scope of ONC's jurisdiction. That does not mean ONC should not work with other agencies within HHS to regulate these technologies. ONC now sits in a unique place as the only agency within HHS working to regulate broad DSIs. While the Food and Drug Administration (FDA) does regulate some AI in medical devices, it has a much narrower scope than what ONC is proposing. Working to ensure that all types of AI that impact patient care, not just those in the EHR, are regulated is crucial in protecting patients and providers from DSIs that are not fully understood or harmful. We recommend ONC work with other federal agencies to ensure all DSI technologies within a healthcare system are regulated.

ii. Proposed § 170.315(b)(11)(ii) Decision Support Configuration

AHIMA supports ONC's proposal to define the scope of data to be included in DSI Decision Support Configuration and support the inclusion of USCDI as the minimum set of data that should be included as part of the DSI. Creating parallel requirements for what should be included in a DSI and what should be included in a provider EHR will help protect against incongruency between the data available to the provider and data available to the DSI.

We urge ONC to ensure these requirements are feasible given the way DSI technology functions. Many of these learning technologies will continue to find data to help it understand and adjust to new scenarios it is encountering. To do that, DSIs may be able to choose the data they take in when making decisions and may require additional data to increase accuracy. As a result, we recommend ONC convene a stakeholder listening session with developers of DSI technologies to understand the appropriate minimum base set of data for DSI technology and how to ensure regulatory requirements remain flexible enough to account for a technology that is ever-changing, learning, and growing.

Additionally, AHIMA supports the ability of users to provide feedback data based on the information displayed through the DSI. The ability to provide feedback ensures that providers are not left without an ability to discuss the changes and adjustments that are needed for a DSI if it is not outputting the correct or expected result. While there are no requirements for a developer to use this information, the desire to improve these technologies should be enough incentive to coax a developer to take the information and improve their DSI. The ability to submit feedback is important, however, AHIMA lacks an understanding of why the data needs to exported by users in a computable format. It is unclear how a provider organization, including those that may not be able to alter its certified product or the interfacing AI, would use this data. We recommend ONC provide further guidance on why this functionality is needed and how having this data available to providers will assist them in the use and implementation of their DSI products.

v. Proposed § 170.315(b)(11)(v) Predictive Decision Support Interventions

Proposed definition of predictive decision support intervention

AHIMA supports ONC's proposed definition of "predictive decisions support intervention (DSI)" as written with the understanding that the proposed definition is broad enough to provide flexibility as the technology continues to develop and change. As ONC continues to develop this proposed definition, AHIMA recommends the agency examine the phrase "intended to support decision-making" to determine if it accomplishes the regulatory goal that is intended by the definition. Many processes that are undertaken related to the administration and delivery of healthcare services support decision-making. For instance, whether a procedure requires prior authorization may dictate what service or type of service a patient receives. As a result, is ONC inferring a predictive DSI that assists in processing prior authorization claims is included as part of this proposed reporting program? Questions like these are ones ONC should clarify prior to a compulsory compliance date with guidance or education that encompasses the publication of the final rule to assist in understanding the applicability of the rule.

Similarly, AHIMA requests clarification from ONC on whether patient matching algorithms are subject to the predictive DSI definition, and thus included in the previously mentioned risk management and reporting requirements. AHIMA believes these patient matching algorithms fall under this definition given that the models use example data to determine accuracy prior to implementation and produce an output stating which patient it

believes matches to which record given the data it is presented with. The proposed definition states that models and algorithms that are locked to the relationships learned in training data are included in this definition and AHIMA believes the patient matching algorithms belong in this category. By being able to understand the matching algorithms themselves, the healthcare continuum can better react and hone its data capture practices ensuring the algorithms receive the best quality data to guarantee the best possible match given the algorithms' determinations. AHIMA would be grateful if ONC can provide clarity whether it intends for patient matching to be included in this algorithm in the final rule.

Attestation for predictive decision support interventions

AHIMA supports the proposal to require developers of certified health IT with Health IT Modules certified to attest "yes" or "no" as to whether their Health IT Module enables or interfaces with one or more predictive DSIs, as this will help providers understand the capabilities of their EHR systems. As previously mentioned, transparency is important in helping providers understand the factors involved in the resources they use. We encourage ONC to consider whether providers should know additional details, beyond whether the predictive DSI enables or interfaces with their EHR. Additional specifics could include details on future DSI plans and how the EHR's interaction with the DSI might impact their clinical and administrative processes.

The use of the predictive DSIs within the EHR is still in its infancy. It is true that there has long been significant use of DSIs in healthcare to assist in multiple processes. The DSIs we have come to know today are much different than the ones that healthcare has long relied on to take the guess work out of healthcare management. It is important for ONC to ensure, at a minimum, that any final rule related to DSIs continues to require health IT developers to identify how they may potentially interface with a DSI in the future. Given the infancy of the technology, there is a significant cost associated with harnessing a DSI's power. Smaller health IT developers may not have the ability to access these tools yet. They may be planning to do so in the future, and it is important to know whether their systems being designed today support future implementation.

AHIMA did want to make ONC aware of a potential gap in the definition of "interfaces with" and urges ONC to close the gap by reevaluating the definition. The proposed definition of "interfaces with" contained in the proposed rule states, "interfaces with" means that the Health IT Module facilitates either (1) the launch of a predictive model or DSI or (2) the delivery of a predictive model or DSI output(s) to users when such a predictive model or DSI resides outside of the Health IT Module . . .We would also consider a Health IT Module to 'interface with,' a predictive DSI in scenarios where an application is launched from a certified Health IT Module, including through the use of a single sign-on functionality." While this interpretation of the definition is broad, it excludes the possibility for predictive DSIs to be enabled through the use of the APIs included as part of the 2015 Edition Cures Update certification criterion.⁶

Certified health IT products currently implemented in eligible provider facilities have functionality allowing for a third-party application to access and utilize data contained within an EHR with no special effort required on the part of the provider facility. This means a third-party program or application not contained within an EHR could access patient data and execute algorithms or processes similar to if the DSI was directly interfacing with the EHR. The difference is that the API-enabled DSI would not need to report any of the risk management or transparency requirements to an ONC-ACB. Additionally, without closing the gap to ensure DSIs that utilize an API designed to be accessed by a patient or provider are included under ONC's definition of "interfaces with," a potential scenario arises where providers need to navigate to third-party websites or use other devices to receive information from a DSI for the sole purpose of avoiding federal reporting requirements. The developer of the DSI may be

⁶ Available at: <u>https://www.healthit.gov/condition-ccg/application-programming-interfaces.</u>

incentivized to do so in order to avoid the transparency and risk reporting requirements to assist them in protecting their intellectual property and shield them from potential competitors in the market.

This potential scenario has additional ramifications beyond a lack of trust and transparency. It could put significant burden on providers related to computer use and click throughs. An API-enabled DSI that outputs into another website could require a provider to leave the EHR platform, open a web browser, login, and then navigate to the area of the application that provides the DSI result. If a provider is trying to determine a risk factor for a patient, considering their blood pressure, heart rate, and other information utilizing a DSI configured in this manner could forestall the process and take longer that it would otherwise if the DSI was included directly in the EHR. ONC must work to ensure there are not incentives for health IT developers to create other pathways for DSIs to access patient data, thus ensuring providers are not placed under additional administrative burden to utilize these potential lifesaving and life altering technologies.

vi. Proposed § 170.315(b)(11)(vi) Source Attributes

AHIMA supports the requirement for developers of certified health IT to directly display source attribute information for end users of the technology to review. It is crucial for this information to be available to those using the technology to understand how a DSI may have arrived at the experienced output. Without this information, it will be difficult for provider organizations to override a DSI if it is outputting something that does not make sense relative to the scenario it was presented with. As noted above though, AHIMA would like additional clarity on how the information being available at the point of care should be used in real time. Most of the source attribute information will be relevant to the organization while it makes procurement and implementation decisions versus during care delivery. To that end, we recommend ONC convene stakeholders to provide feedback on how best to move forward with this requirement to ensure implementation accomplishes the intended policy goals. This stakeholder convening should include, but not be limited to, health IT developers, DSI developers, and health IT end users including, providers and patients. Together this convening should provide a set of concrete recommendations to ONC on how to inform providers with actionable information presented in a usable format.

vii. Proposed § 170.315(b)(11)(vi)(A) Source Attributes – Demographic, SDOH, and Health Status Assessment Data Use

AHIMA supports ONC's inclusion of SDOH data in the mandatory source attribute inclusions for DSI. Requiring vendors to report on these data elements' inclusion will assist providers in both ensuring the whole patient is cared for and that there is transparency as part of that whole-person care. We encourage ONC to continue to evaluate if additional SDOH data elements should be used as source attributes as the DSIs evolve to encompass more complex care settings and care conditions.

viii. Proposed § 170.315(b)(11)(vi)(C) Source Attributes for Predictive Decision Support Intervention

Proposed new source attributes for predictive DSI

AHIMA supports ONC's addition of 14 new source attributes for predictive DSIs that enable or interface with Health IT Modules. Providing a clear set of requirements for DSIs that encompasses a floor for data inclusion creates a predictable environment for providers. This ensures that DSIs will not provide a radically different experience for providers and subsequent outcomes for patients despite where they choose to receive care. We do however note that by allowing developers to not report and display source attribute information for certain data standards, ONC has opened the door for potential misuse of this requirement by developers who partner with third parties for the DSIs included in their products. With the ability to report "if available," the pressure to have

and report that information is no longer placed on the developer. This creates a less transparent and more opaque system where providers may receive a DSI output, but never fully understand what was used to arrive at that conclusion. We recommend ONC determine a process for ensuring this information is reported and that the "if available" is only applicable in specific circumstances.

Intervention Details

AHIMA supports ONC's proposal of creating three source attributes related to intervention details. This will allow a provider to better navigate the decision-making process when deciding between different DSIs. We encourage ONC to continue monitoring the use of these source attributes and modify this requirement as appropriate.

Intervention Development

AHIMA supports ONC's proposal of creating three source attributes related to the development of the DSI models. As providers determine which DSIs are best suited to service their population, understanding how a DSI was created and with what data is important. The value of this information is compounded by the importance of both the process of development and external validation process attributes. All three elements in tandem allow a provider to have a window into how the DSI was created and how it may function in the real world. We recommend that in addition to these source attributes, ONC include information on whether the DSI was tested or trained during real world testing. By including this information provider organizations can anticipate if the DSI model is going to behave as intended or if the organization should be prepared for model growing pains.

Quantitative Measures of Intervention Performance

AHIMA supports the inclusion of Quantitative Measures of Intervention Performance. Ensuring that there is objective data to measure and evaluate these DSI models is crucial to helping provider organizations ensure they are selecting the correct predictive algorithm to interface with. This information will help a provider weigh the pros and cons of using a selected model relative to the answer it provides. Not everything in care delivery is risk free and having quantitative information helps ensure whatever course of action is taken is relative to the related risks and outcomes experienced by the patient.

Ongoing Maintenance of Intervention Implementation and Use

AHIMA supports the inclusion of the Ongoing Maintenance of Implementation and Use source attributes for evaluation and reporting of predictive models. As mentioned elsewhere in our comments, these predictive DSI models are designed to learn, adapt, and change as they encounter data within the provider facility. Having access to information on how the models may perform over time while evolving will assist provider organizations in creating appropriate policies and procedures around when and how to utilize DSI models.

ix. Proposed § 170.315(b)(11)(vi)(D) Missing Source Attribute

AHIMA understands the need for ONC to include proposed requirements allowing for health IT developers that do not own or operate, but interface with, a DSI module to have the ability to report that they were unable to receive attribute details to support the above noted ONC requirements. We urge ONC to reconsider the proposal as currently written to ensure this exception does not operate as an opt-out for the reporting of attribute information. There are numerous ways in which bad actors could manipulate this proposed exception to ensure they never have to report source attribute information. It is crucial that providers and patients are able to receive transparency into the DSI models that are making complex decisions regarding individuals' medical care. While good faith circumstances may exist when an attribute is not available to be reported, ONC should ensure it is the

exception, not the norm. If this exception is not reviewed and strengthened, this could pose a high risk for ONC to receive no transparency information regarding DSI models.

xi. Proposed § 170.315(b)(11)(vii) Intervention Risk Management (IRM) requirements for Predictive Decision Support Interventions

AHIMA supports the ONC requirement for developers of certified health IT to engage in and report IRM for predictive DSIs. As stated above, it is crucial for these activities to be undertaken and the results be published for providers to be able to understand the impact and challenges related to a DSI they are considering implementing. Additionally, AHIMA would like ONC to consider real world testing requirements related to these IRM practices. As proposed, there is no requirement for these activities to take place outside of a controlled development environment. It is crucial for these DSIs to be tested in real situations with real patient data. The reality of medical care is that it cannot always be simulated and DSIs must be stress tested to better understand how they will perform in an uncontrolled environment. Many AHIMA members have indicated that DSIs are often at the behest of the humans who implement them. One small error in implementation or during use could lead to significant burden. To ensure DSIs are successful ONC should ensure they are tested in real world scenarios before they are adopted, not after.

Proposals in § 170.315(b)(11)(vii)(D) Annual Review

AHIMA supports the proposal to require developers of certified health IT to attest "yes" to an annual review and update of DSI documentation as necessary, however we urge ONC to consider whether this accounts for when DSIs change through learning in the hospital environment each year. The required attestation and update of documentation on risk analysis, intervention, and mitigation should include information regarding the assessment of adjustments the DSI has made in response to learning and feedback, as well as changes the DSI has or needs to complete.

d. Proposed Updates to Real World Testing Condition for CDS Criterion

AHIMA supports adding the CDS Criterion to the list of applicable certification criteria for real-world testing. Realworld testing is critical to assess how new approaches work with existing infrastructure, identifying workflow constraints, costs, and needed education for providers before implementation. AHIMA and several other leading healthcare organizations created the Health IT End-Users Alliance, a group focused on advancing end-user leadership in health IT policy and standards development to ensure better alignment across regulatory requirements and optimal use of technology to support clinical operations.⁷ Leveraging health IT end-user input, including health information professionals and physicians, will help ensure implementation of the CDS Criterion, future certification criteria, and other elements discussed in this rule are effective, efficient, minimally burdensome, and beneficial.⁸

7. Standardized API for Patient and Population Services

c. FHIR Endpoint for Service Base URLs

AHIMA supports the continued development of FHIR Endpoint for Service Base URLs but urges ONC to coordinate efforts with the Centers for Medicare & Medicaid Services (CMS) and other relevant HHS agencies to ensure the needed infrastructure is there to support the use and access of these URLs. AHIMA previously responded to CMS'

⁷ Available at: <u>https://hitenduser.org/.</u>

⁸ Available at: <u>https://hitenduser.org/wp-content/uploads/2022/09/Real-world-testing-consensus-statement_FINAL.pdf</u>.

request for information on establishing a national provider directory.⁹ We continue to stand by the comments we made in that response to CMS and recommend ONC review other responses to CMS' request to ensure the service base URL proposal contained in HTI-1 would work in tandem with CMS' ongoing efforts to develop a national directory. The FHIR endpoint for service base URLs proposed by ONC would be a welcome addition to a national provider directory and would help providers across the nation seamlessly locate how to exchange patient data.

Additionally, AHIMA supports the quarterly review of the contents of these service base URLs but recommends ONC convene stakeholders to determine the best process for continuing to monitor the utilization of the URLs and whether adjustments need to be made to this review timeframe. Without an active national directory for these URLs to be located by providers, it is unclear when or if a shorter review and update cadence will be needed. If updates or changes need to be made, AHIMA recommends ONC include those changes in subsequent proposed rules.

ONC proposes that organizational information that is out of date and unusable for more than 90 days would be considered in violation of the proposed requirement and asks if that time should be adjusted to 30 or 60 days. In order for FHIR Endpoint URLs to be useful they must be accurate. If the URLs are inaccurate or non-functional it could hinder the exchange of health information. Under ONC's information blocking requirements, any Endpoint URL that is knowingly incorrect would constitute a delay or barrier to information exchange which in turn would constitute information blocking. With that in mind, AHIMA recommends ONC notify organizations of inaccurate or non-functional data after 30 days with a formal warning of non-compliance. If the organization does not correct the errors, then they should be found in violation at 60 days. It is understandable that mistakes happen, and organizations need time to rectify those errors, but if an unusable FHIR Endpoint URL is allowed to linger it could hinder and prevent the intended flow of health data across the health system. Allowing this data to be inaccurate for 90 days or longer may lead to organizations being unable to receive or send patient data for a time longer than necessary and would be out of sync with other federal requirements that mandate data exchange.

e. SMART App Launch 2.0

AHIMA supports the adoption of SMART App Launch 2.0 and the adoption date in companion with the January 1, 2025 expiration of the SMART v1 Guide. It is crucial for ONC to continue adoption of the SMART framework as it develops to ensure patients have the ability to access their health data through the APIs enabled by the 2015 Edition Cures Update certified products. These SMART App tools also will continue supporting innovative solutions for how providers can interact with and present data to their patients. Health data is not easy to understand and interpret by patients and SMART App tools can enable innovative ways for providers to present this information to patients. AHIMA applauds ONC's continued patient focus with their SMART on FHIR work now and in the future.

8. Patient Demographics and Observations Certification Criterion in § 170.315(a)(5)

AHIMA supports the proposal to update the "Demographics" criterion to the "Patient Demographics and Observations" criterion. We also support the data element inclusion and updates that are proposed by ONC. These proposals will assist providers in helping the patient see themselves accurately in their medical data. It is crucial for ONC to continually review the standards and data classes related to these sensitive data elements to ensure it aligns with their real-world use. Additionally, ONC must ensure that these data element changes are done with widely adopted and real-world tested data standards. By ensuring standards are available and used to back up these changes, the healthcare community can quickly adapt within the timelines envisioned by ONC.

⁹ Available at: <u>https://ahima.org/media/mmkkaag0/final-ahima-cms-national-provider-directory-api-comments.pdf</u>.

9. Updates to Transitions of Care Certification Criterion in § 170.315(b)(1)

AHIMA supports the proposed replacement of the fixed value set for the USCDI data element "sex" enabling health IT developers to specify any appropriate value from the SNOMED CT code set with specified standards. This change continues to demonstrate ONC's willingness to update these requirements as real-world needs change.

10. Patient Requested Restrictions Certification Criterion

AHIMA supports the development and implementation of data segmentation technology in health data systems and certified health IT products. The inability to segment data in technology products limits the ability for providers and patients to control the health data being moved throughout the health system. States across the nation have a patchwork of privacy laws allowing patients at specific ages the option to shield data from a parent or guardian. Additionally, many adult patients have sensitive health issues they may not want shared across the medical system with other providers. Currently, many EHR systems do not have the ability to respect these privacy changes or support state privacy laws. This leads to situations where often the protection of health data exists as an all or nothing exercise. For example, minor patients who want to restrict access to their data from a parent or guardian must prevent complete access to their medical record. Conversely, those who want to send part of a health record to a provider and leave sensitive areas out of the exchange, are left having to decide the risk/reward of sharing the sensitive information or not sharing the data at all. This in turn hinders care coordination and over-utilization of resources because additional testing may be required.

Issues related to the inability to segment data are not only a privacy concern for patients, but a safety one as well. Some patients themselves, as part of their treatment, must be shielded from diagnoses. This is especially the case with several mental health conditions such as cases of dissociative identity disorder (DID).¹⁰ Those experiencing DID and under treatment for similar disorders may not be aware they suffer from DID. Exposing them to this information can be detrimental to their treatment and dangerous to their safety. Without the ability to segment data, a real risk exists for a patient diagnosed with DID having their condition exposed to them if they go to another area of a medical facility, such as an emergency department (ED), and receive their records for an unrelated visit that denotes their diagnosis or treatment for DID.

Because of the above reasons, AHIMA supports ONC's proposal to create a new Patient Right to Request a Restriction criterion but urges ONC to account for several patient safety and exchange related concerns raised by AHIMA membership.

ONC proposes a standards agnostic approach to implementing the privacy flag process for patients. AHIMA continues to believe there are various options to improve data segmentation and users should not be locked into one solution. It is crucial for ONC to propose a set of multiple standards that are guaranteed to interoperate and accomplish the intended policy goals. A standards agnostic approach may sound like a good one, but in practice the lack of predictable standards often creates a technology space where every solution is slightly different. By opening the door to standards agnosticism, ONC is creating a development environment where every developer can create their own solution forcing the end user to need to understand and cope with multiple standards for accomplishing a simple process. We recommend ONC propose a set of standards that should be used to accomplish the intended purpose of the patient right to request a restriction criterion. One option would be for ONC to utilize the HL7 CDA DS4P IG developed by convening a set of stakeholders from all areas of the healthcare continuum. Should ONC utilize the HL7 CDA DS4P IG, we encourage the agency to work with other federal

¹⁰ Available at: https://www.nami.org/About-Mental-Illness/Mental-Health-Conditions/Dissociative-Disorders.

agencies to establish a federally supported collaborative process to engage stakeholders, including end-users, to define the needs to data segmentation and evaluate, pilot test, and improve the IGs for CCDA and FHIR.

ONC should also work with the broader health IT community to identify expectations for rigorous real-world testing of data segmentation solutions, such as the needed metrics, methods of accountability, assurance that testing results are impartial, external expert review of testing methods and results, impact on health equity, and public reporting of the outcome. Standards should not be considered mature until real-world testing has been completed and comprehensive report-outs on the testing are made public. Inclusion of standards and IGs in regulation should also not be considered a mark of maturity.

The AHIMA membership operates in the unique position that places them at the center of most patient directed data exchange requests initiated in the provider facility. Health information (HI) professionals within provider facilities work with the data in systems on a daily basis and help both patients and providers get access to health data when and where they need it. Due to this experience, AHIMA cautions ONC that strict guard rails need to be implemented to ensure patient safety is not compromised in the name of protecting patient privacy.

One example provided by AHIMA members of a patient safety concern would be a patient flagging their medication list for privacy protection. If the patient needed to go to another ED at a future date, the ED would not know which medications the patient is taking. If the patient is not conscious or does not remember their medications, a potential risk for an adverse drug event exists. Similarly, if a patient were to protect other fields such as diagnoses, allergies, etc., it could prevent another physician in another facility from knowing about crucial medical details that could place the patient's safety in jeopardy. ONC has asked whether a final rule should include criterion allowing for emergency disclosures or termination of a patient directed restriction. Both of these options could help assuage concerns related to patient harm due to the inability for a provider to access a portion of a patient's record because of a privacy request by allowing them to disregard that request if needed.

AHIMA members also highlighted a policy and procedure barrier to honoring a patient's request for data privacy restrictions. The proposed rule indicates certified health IT should include a way for patients to flag individual USCDI elements for patient directed privacy restriction. While it is easy to flag individual USCDI data elements for protection from a policy and procedure standpoint, difficulty arises when managing patient expectations as it relates to protecting data that may be stored in standard elements and also be documented elsewhere in the record. For instance, the notes and other free text fields may contain information about a patient's diagnosis or medications. If a patient were to only flag the USCDI elements for diagnosis or medications their privacy request would, by the letter of the text, be honored, but the information would be transferred through a free text element anyway. The question remains then whether the patient's privacy wishes are respected if the data was still transmitted. ONC should convene stakeholders including providers and patients to discuss the challenges related to honoring patient requested privacy requests.

In addition to policy and procedure concerns related to honoring patient directed privacy requests, there are functional issues regarding honoring these requests if ONC were to change the requirement from requests grounded in the USCDI to all data in the medical record. Expanding this requirement to all data in the medical record would put significant burden on a provider facility and HI professionals to require them to go through a patient's full record to find information about specific medical issues a patient is experiencing. If a patient was able to be that specific about what they want to be restricted in data exchange, the process would be difficult if not impossible to complete. When ONC convenes the above requested stakeholder group it should be discussed how best to honor patient directed requests from a technical perspective.

Despite the challenges related to accomplishing data segmentation for privacy there are several solutions ONC should investigate to overcome the patient safety concerns. One option would be for the health IT products that

enable patients to select patient directed privacy restrictions through their portal to implement a warning or alert system for specific data elements contained within a patient record. For instance, if a patient were to select their medication list for privacy restriction, an alert would appear warning the patient that this could put them at risk for future adverse drug interactions. Similarly, for crucial data elements there could be a requirement for a patient to call their provider to discuss the implications of protecting the information. These are just two of the many options available to make patient directed privacy restrictions easier and offer opportunities to educate patients on the considerations and implications related to restricting disclosure of their medical data. More may exist, but AHIMA recommends ONC work with the health IT developers to assess how to empower patients to control the exchange of their data.

AHIMA members remain ready and willing to be active parts of the discussion on how to implement data segmentation activities including, but not limited to, the development of patient directed privacy restrictions. HI professionals act as a gateway into the data exchange world and can serve as a tremendous asset to ONC and health IT developers as they seek clarity on the real-world implications of policy changes and technology developments. We look forward to working with ONC now and in the future to make patient control of their data a reality.

11. Requirement for Health IT Developers to Update their Previously Certified Health IT

AHIMA supports ONC's proposals contained in the Requirements for Health IT Developers to Update their Previously Certified Health IT. It is crucial for providers to receive their updated products in a timely matter so they can begin the implementation and testing process as soon as possible. It is important for ONC to understand that this process could be streamlined by encouraging testing of the health IT products in provider facilities while the products are being developed. The current process sees the health IT products developed prior to providers even having the opportunity to test or trial the products in their facilities. By encouraging testing prior to product delivery, developers could accelerate their development times and simplify provider implementation timelines.

Until ONC adopts this updated approach to health IT development, AHIMA supports the requirements for health IT developers to begin implementation activities prior to the delivery date of new products. This proposed regulatory language change ensures providers will not be left to hastily implement their health IT products once they are delivered to comply with the CMS Promoting Interoperability Program attestation dates. We applaud ONC for putting the provider at the center of the development cycle and encourage them to find other areas within its regulatory purview to do the same.

E. Real World Testing – Inherited Certified Status

AHIMA supports ONC's efforts to ensure real world testing continues for all certified health IT products, whether new or significantly updated. As previously stated in this letter, it is crucial for real world testing to remain a fixture of the health IT and standards development process. We continue to urge ONC to find other opportunities to prioritize real world testing in the development of these health IT products and related standards. As a founding member of the Health IT End Users Alliance¹¹ AHIMA firmly believes end users of these health IT products and standards have a critical role to play in identifying what standards to prioritize to improve workflow and how the related products can support. We welcome ONC's continued work to foster such dialogue and encourage the agency to work to ensure health IT products serve all of the health system.

F. Insights Condition and Maintenance of Certification

¹¹ <u>https://hitenduser.org/wp-content/uploads/2022/09/Real-world-testing-consensus-statement_FINAL.pdf</u>

AHIMA supports ONC's continued measurement activities related to the use and interaction of certified health IT with the healthcare continuum and patients. It is important for measurement activities to be undertaken to ensure the policy goals advanced by the policy provisions contained within ONC proposed rules are accomplished. ONC has a long history of aggressive measurement of certified health IT and AHIMA encourages ONC to continue that activity into the future.

It is important to note however, AHIMA urges ONC to ensure the burden of completing and responding to the measurement activities are not passed down to the provider from the health IT developer. While measurement activities need to take place in the real-world environment, collecting the data and responding to the measurement of those activities should remain a responsibility of the health IT developer. AHIMA encourages ONC to either examine and modify the proposals contained in this proposed rule to ensure they do not require provider input or create guard rails to ensure health IT developers do not overly burden providers to complete measurement activities.

One example of a proposed measure that may increase reporting burden on the provider is the Measurement Area: Individual Access to Electronic Health Information. The proposed measure requires the health IT developer to report on the different methods individuals use to access their health information, including measuring the extent they use third-party apps. As AHIMA and other stakeholders have cautioned ONC in the past, the technical ability to measure third-party app use via an open API is difficult and close to impossible. The API would not log or capture how many apps attach to the API and knowing if an app was successful in accessing a patient's electronic health information (EHI) would only be known if a patient were to authenticate through a portal. That authentication is not always required to access certain information within the EHR. In addition to this limitation, gathering information such as this would need to happen at the provider level and be aggregated by the health IT developer. This creates a scenario where providers would be responsible for collection of data on EHI access and use, while the health IT developer is reporting what the providers produce. The measures themselves are designed to place the reporting burden on the health IT developer and in the above scenario it is clear the measure would not accomplish that goal.

An additional example where this potential exists is with the proposed Individuals' Access to Electronic Health Information Supported by Certified API Technology Measure. Similar to the above-mentioned measure, the measurement of a patient's access to their EHI would likely be completed by the provider. One difference to the previously referenced proposed measure is the increased reporting burden due to the reporting complexity. ONC proposes as part of this measure to have health IT developers report on two distinct numerators and three distinct denominators. This additional reporting complexity has the potential to fall on the provider as they are the entity most likely to collect and hold information on how patients access their information through API technology – if that measurement is even possible.

As shown above, significant risk exists for the measurement of health IT products to fall to the provider community. AHIMA recommends ONC convene stakeholders to find the best solution as it relates to reporting on these crucial measures. This convening should consist of representatives from the developer and provider community, including those who do the administrative measurement work inside of provider facilities. AHIMA remains focused on this type of regulatory burden as it is our members, the HI professionals, who will likely be tasked with completing these activities. HI professionals are already overburdened as it is and adding additional reporting burden without clear policy objectives would be problematic. For this reason, ONC must act to ensure these measurement activities are completed by the appropriate parties.

G. Requests for Information

1. Laboratory Data Interoperability Request for Information

AHIMA supports the inclusion of additional standards and laboratory-related certification criteria. It is crucial for ONC to encourage health standards development organizations to develop standards for the areas of the health system with the least developed standards environments. Laboratory data is some of the least exchanged and hardest pieces of digital health information to access. To move closer to an interoperable healthcare system, laboratory data standards must continue to be developed, tested, and adopted in certified health IT products. Without the ability to access and exchange patient laboratory data, the health system will be forced to run duplicate or unnecessary tests because they do not have access to that section of a patient's record. Increased development of laboratory standards ensures health IT developers are able to access standards to implement into their products that are as technically sophisticated as other areas of a patient's record. Maintaining a consistent level of standards implementation and maturity across the whole patient record eases the exchange burden and makes it more likely for health IT developers to implement the standards when otherwise not required.

2. Request for Information on Pharmacy Interoperability Functionality within the ONC Health IT Certification Program including Real-Time Prescription Benefit Capabilities

AHIMA supports ONC continuing to adopt additional standards and certification criteria that support real world electronic prescribing workflows. This would continue to support the CMS initiatives related to electronic prescribing and electronic prior authorization. The largest barrier to providers participating in both processes is often not a lack of will, but rather a lack of ability due to technical barriers. Continuing to remain involved in adopting updated prescribing and NCPDP standards workflows ensures providers will have the tools available to them to close the process gaps in participating in these cost savings and price transparency efforts.

iii. Requirements for Use of NDC or RxNorm Codes

AHIMA would support a future benefit certification criterion that requires demonstration of compliance with both NDC and RxNorm. AHIMA members approached about this proposal did not provide any feedback about potential adoption of both NDC and RxNorm. There was no indication of burden associated with the adoption of this requirement from the health information professional perspective. AHIMA encourages ONC to convene additional stakeholder listening sessions to determine the burden and cost associated with adopting this proposal.

iv. ICD-10-CM and SNOMED-CT in the Clinical Segment

AHIMA would support the potential requirement of the Clinical Segment in the NCPDP RTPB standard version 12 as part of any future real-time prescription benefit certification and the demonstration of use for both ICD-10-CM and SNOMED CT within the clinical segment. However, AHIMA cautions ONC in preparing for the ICD-11 implementation within a certified health IT environment. At this time, it is unclear when ICD-11 will be implemented in the US or whether it will require a clinical modification. We encourage ONC to work with the National Committee on Vital and Health Statistics (NCVHS) to stay involved in the ICD-11 development and implementation process.

ii. Electronic Prior Authorization

CMS proposed requirements in the recent Advancing Interoperability and Improving Prior Authorization Processes proposed rule that requires providers to engage in and report on electronic prior authorization.¹² To fulfill those requirements and participate in electronic prior authorization, providers need technology and data standards to

¹² Available at: <u>https://www.federalregister.gov/documents/2022/12/13/2022-26479/medicare-and-medicaid-programs-</u>patient-protection-and-affordable-care-act-advancing-interoperability.

support those processes. In our prior comments to ONC regarding electronic prior authorization certification, AHIMA noted that multiple systems are often involved in the workflow associated with prior authorization including registration systems, revenue cycle management systems and practice management systems. Many of these systems are not certified today. Conversely, under the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA transaction standards apply to providers, payers, and clearinghouses but not health IT developers. We continue to recommend that to successfully facilitate electronic prior authorization processes, the same rules should apply to health IT developers, payers, and providers to ensure that all follow the same "rules of the road."¹³ Otherwise, lack of such consistency may delay implementation of these measures, therefore further delaying administrative relief for provider organizations and timely access to care for patients. AHIMA urges ONC to work with CMS to further align the HIPAA transaction standards with any electronic prior authorization certification requirements to ensure that all systems involved in the workflow associated with electronic prior authorization certification are accounted for.

IV. Information Blocking Enhancements

- A. Defined Terms
- 1. Offer Health Information Technology or Offer Health IT

AHIMA supports the proposed clarification that the provision of subsidies for certified health IT, implementation and use activities including login credentials for surveillance and production of patient portals, and consulting and legal services do not fall under the definition of offer health IT. AHIMA and L&M Policy Research conducted a qualitative study of AHIMA members in 2022 to explore current understanding of information blocking compliance, challenges and success factors, and the role of HI professionals in the process. Our results found that smaller organizations lack resources and dedicated staff to understand and establish internal policies to address grey areas in information blocking regulations, deal with questions and concerns, and continually monitor and update systems.¹⁴

Smaller and otherwise under-resourced organizations, like some of those represented in the study results, can benefit from these types of assistance, and may rely on such arrangements and activities to participate in an electronic and interoperable data sharing environment. We agree with ONC that these organizations should not fall under the definition of offer health IT and be subject to more stringent reporting or information blocking requirements because they rely on partnerships and collaborations to accomplish the goals of electronic health information exchange.

- 3. Information Blocking Definition
- B. Exceptions
- 1. Infeasibility

a. Infeasibility Exception – Uncontrollable Events Condition

AHIMA supports the proposal to change the language in this exception from "due to" to "because of" to reflect that an uncontrollable event negatively impacted the feasibility of fulfilling access, exchange, or use of EHI. This

¹³ Available at: <u>https://www.fiercehealthcare.com/regulatory/hhs-kicking-can-down-road-not-including-electronic-prior-authorization-hti-1-proposed</u>.

¹⁴ Available at: <u>https://journal.ahima.org/page/health-information-professionals-at-the-forefront-of-information-blocking-</u> <u>compliance.</u>

creates more certainty for providers related to needed documentation to fulfill the Uncontrollable Events Condition.

b. Third Party Seeking Modification Use

AHIMA appreciates that ONC is concerned about the quality of data in a patient's EHR and is signaling that providers are entitled to do their best to secure the integrity of the data within their EHR system. We support the accuracy, quality, and integrity of patient health data within the EHR.

However, we urge ONC to consider whether this proposed condition could inhibit care coordination. Providers involved with a patient's care team that may not have business associate agreements with each other may wish to contribute to a patient's EHR to create a more complete medical record for that patient. This can be particularly important for providers from another state sending information to the patient's primary care provider, specialists sharing information with the patient's primary care provider, or patients using a third-party app in efforts to modify or add to their record. We urge ONC to consider whether patients should be consulted before data is either incorporated into their EHR from another provider or denied, and if so, how this would be done in a minimally burdensome manner for providers.

Additionally, if finalized, this proposal should include more specificity and details on fulfilling this condition in practice. The proposed rule does not explain how a provider should demonstrate fulfilling this condition. If this proposed condition is finalized, in the final rule, ONC should include information on how providers can demonstrate they have concerns about the accuracy or reliability of data and the process by which they should prove and document those concerns. ONC should offer recommendations to providers on how to store information received by a third party if providers would like to keep but not integrate this data into an individual's record. If implemented, it may be helpful to work with health IT developers to implement a mechanism to allow providers to maintain data that has not been integrated or multiple versions of a patient's medical record. That way, providers can accept third-party modifications or additions without triggering automatic edits to a patient's medical record.

We encourage ONC to examine what entities have access to providers' EHRs, including payers, and why certain entities may request to access or change authenticated documents or clinical notes. ONC should study potential harms from incorporating and not incorporating modifications or additions of EHI in these situations, as well as the process and potential burden that providers may bear in attempts to determine whether certain actors should or should not have access to make such modifications.

AHIMA also encourages ONC to consider the long-term impact of implementing this condition. For instance, ONC should consider if this type of condition would be possible in a future environment in which the Trusted Exchange Framework and Common Agreement (TEFCA) is actively exchanging data. In an interoperable system where health information is shared closer to real-time, ONC should consider whether providers will be able to evaluate the accuracy or reliability of data that a third party would like to add to an individual's EHI.

c. Manner Exception Exhausted

AHIMA supports the proposal to create the Manner Exception Exhausted Condition. In the final rule, we recommend ONC provide more specifics on the types of characteristics that would designate entities as similarly situated and recommend guidance on ways for actors to easily group and document entities that are similarly situated to reduce burden in fulfilling this condition.

2. Manner Exception – TEFCA Reasonable and Necessary Activities

b. TEFCA Condition for the "Manner Exception"

AHIMA supports this proposal and supports the implementation of the TEFCA to further interoperability in the US, and we are encouraged by initiatives to make participation more efficient and beneficial. When fully operational, TEFCA will allow providers to exchange health data more easily, thereby reducing the burden of compliance with information blocking requirements. We believe participation in the TEFCA should remain voluntary and be an option to improve data exchange in the US.

However, we urge ONC to consult stakeholders to ensure this condition does not inadvertently allow actors to use participation in the TEFCA as justification to avoid easier and more feasible options of electronic exchange outside of the TEFCA that may be available through alternative methods. For example, the Common Agreement does not include rules for participant fees, creating a possibility that a participant could charge a large fee for another organization to exchange data. Under this proposed condition, the participant could be exempt from information blocking because they offered TEFCA exchange as a solution, even though the fees could be a barrier to information exchange. Thus, if this condition is finalized, we encourage ONC to work with The Sequoia Project to ensure the Common Agreement is updated and appropriate SOPs are in place to avoid this example and similar gaps that may exist.

C. Information Blocking Requests for Information

3. Health IT Capabilities for Data Segmentation and User/Patient Access

As previously mentioned, AHIMA supports the development and implementation of data segmentation technology in health data systems and certified health IT products. With current capabilities, data segmentation is not feasible among many health care organizations that HI professionals operate within. AHIMA believes there are several options to implement data segmentation, but we reiterate our recommendation that ONC propose a set of standards to accomplish data segmentation.

Data segmentation will not be possible in real-world settings without commonly used standards. Patient-directed data segmentation is critical for patients, but the existing infrastructure is limited in supporting these goals. When ONC moves forward with processes and standards development to segment data, ONC must support real-world testing of standards with end-user input before implementation to ensure standards are effective in health care settings of all sizes, characteristics, and capabilities.

When implemented, provider organizations should have the ability to track patient requests for data segmentation and we encourage ONC to work with health IT developers to build this functionality into their products. Additionally, it may be helpful for health IT systems to include a clear flag in the medical record if particular data elements were requested by the patient to be segmented and private. By doing so, it is clear to other providers on the patient's care team that data was segmented out at the patient's request, rather than omitted from the record on behalf of the provider sharing the data.

AHIMA applauds ONC for the work and dedication to advance interoperability demonstrated by the release of the HTI-1 proposed rule. HI professionals nationwide look to ONC as a partner in helping patients access and exchange vital health information. As ONC continues to develop HTI-1 please know AHIMA and its membership stand ready to assist ONC in any capacity needed. Until then, if AHIMA can provide any further information, or if there are any questions regarding this letter and its recommendations, please contact Andrew Tomlinson, Director of Regulatory Affairs, at (312) 223-1086 or <u>andrew.tomlinson@ahima.org</u>.

Sincerely,

un D-

Lauren Riplinger, JD Chief Public Policy & Impact Officer