May 23, 2019

Don Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Dr. Rucker:

AMIA appreciates the opportunity to comment on this Notice of Proposed Rulemaking (NPRM) on policies to implement provisions of the 21st Century Cures Act and enhancements to ONC's Health IT Certification Program.

AMIA is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers, public health experts, and educators who bring meaning to data, manage information, and generate new knowledge across the research and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across care settings and patient populations.

In 2014, the AMIA Board of Directors chartered the multidisciplinary EHR 2020 Task Force to develop recommendations for how to address many health information technology (IT) challenges from a wide range of perspectives by the year 2020.[1] The EHR 2020 Task Force Report published in the *Journal of the American Medical Informatics Association* in June 2015[2] and offered numerous recommendations across four broad categories:

1. Address burdensome clinical documentation requirements so the patient's story is not subservient to billing and regulatory reporting;
2. Refocus regulations to streamline Meaningful Use and quality reporting, and reorient health IT certification to test for interoperability;
3. Increase transparency in how health IT meets certification and in how systems perform after they're deployed in a live environment to improve usability and safety of EHRs; and

[1] June 2014, https://www.amia.org/ehr-2020-task-force
[2] Payne TH, Corley S, Cullen TA, et al. Report of the AMIA EHR-2020 Task Force on the status and future direction of EHRs, *Journal of the American Medical Informatics Association*, Volume 22, Issue 5, September 2015, Pages 1102–1110, https://doi.org/10.1093/jamia/ocv066

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

4. Foster innovation through use of public, standards-based APIs and more granular data standards so that we can build toward the next generation of EHRs and realize the benefits of the "learning health system."

Alongside testimony from a diverse mix of stakeholders, Congress took these and other AMIA recommendations – such as the need for patients to have complete copies of their electronic health information in a computable format – into consideration when crafting the 21st Century Cures Act of 2016.[3] The Cures Act established an ambitious agenda for how EHRs must evolve to deliver on the many as-yet-undelivered promises first described nearly a decade ago in the HITECH Act.[4] Among these ambitious changes was a new statutory definition of "interoperability," in the context of health IT that: (1) enables the secure exchange and use of electronic health information without special effort on the part of the user; (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (3) does not constitute information blocking.[5] Added to this comprehensive definition was a new adjunct to ONC's Certification Program that outlines specific conditions for and maintenance of Certification. One such condition is that certified health IT have "published application programming interfaces and allows health information from such technology to be accessed, exchanged, and used without special effort…including providing access to all data elements of a patient's electronic health record…"[6]

AMIA commends ONC for translating these ambitious statutory imperatives from the Cures Act into regulation. We support many of these proposals and we note that numerous provisions in this NPRM operationalize the recognition conveyed by Congress that change is needed to the status quo. This NPRM will fundamentally transform the current landscape for health IT. The reliance on discrete data standards such as FHIR and the establishment of new Conditions and Maintenance of Certification requirements will enable our national healthcare system to reorient away from siloed legacy systems toward an orchestrated interoperability architecture based on open APIs and advanced intermediary applications and services, as first described in 2014 by the landmark JASON report.[7]

Despite these important and foundational changes to the current state, this NPRM perpetuates an imbalance where patients, clinicians, and researchers are beholden to health IT developers for routine access, exchange, and use of health data. If finalized as proposed, this NPRM will solidify a dynamic where health data must be standardized before it is available for patient care or research.

---

[3] Testimony of Thomas H. Payne, AMIA Board Chair-elect and EHR 2020 Task Force to the Senate Health, Education, Labor & Pensions Committee. June 9, 2015. Available at: https://www.amia.org/public-policy/testimony-thomas-h-payne-amia-board-chair-elect-and-ehr-2020-task-force-senate-health

[4] Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5)

[5] Section 4003 of 21st Century Cures Act

[6] Section 4002 of 21st Century Cures Act

[7] JASON. A Robust Health Data Infrastructure. April 2014. https://www.healthit.gov/sites/default/files/ptp13-700hhs_white.pdf

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

May 23, 2019

While the informatics community fiercely advocates for the standardization of biomedical, clinical and health data,[8] AMIA flatly reject a policy that requires data to be standard before it can be used for patient care.

The US Core Data for Interoperability (USCDI) was proposed in 2018 as a data policy with three distinct categories of data classes and elements: "emerging," "candidate," and "supported" data elements.[9] In comments submitted to ONC in 2018, we noted that this policy construct failed to account for the constantly-evolving category of non-standard or unstructured data, produced in vast quantities from information systems ranging from wearables to genomic sequencing labs.[10] Further, we warned that this policy would require that health data graduate from "candidate" to "emerging" to "supported" before it was routinely available for patient care or research. The 2018 policy specified that certified health IT would be expected to exchange only the small subset of highly constrained, standard data elements known as "supported" data elements.

In this NPRM, ONC has provided the technical underpinnings for 15 data classes and roughly 50 "supported" data elements, but it has failed to account for the overwhelming majority of data elements that could be considered "candidate," "emerging," or "unstructured." While the proposed EHI Export for Patient Access (§170.315 (b)(10)(i)) and Database Export (§170.315 (b)(10)(ii)) provide mechanisms to make these data available, we are concerned such criteria will be insufficient to flip the paradigm of dependency where patients, clinicians, and researchers are at the mercy of health IT developers to access their data routinely.

As the USCDI represents a national data policy as well as a named standard in this NPRM, AMIA strongly recommends ONC establish a "share now, standardize as needed" policy supported with the "Unstructured Document" document-level template[11] (and corresponding C-CDA-on-FHIR IG[12]) as part of USCDI's Clinical Notes data class. This reorientation would address a dependency to standardize data before it is routinely available for patient care / research by (1) establishing a baseline expectation that all EHI, not just data supported by C-CDA or FHIR, is available to patients, clinicians, and researchers when authorized and (2) positions patients, clinicians and researchers, rather than health IT developers, to identify data types in need of concerted standardization. Appendix A includes a graphical representation of this recommendation. This approach is consistent with the USCDI data policy articulated by ONC in 2018 because it would enable health IT to exchange not just USCDI "supported" data elements, but would also provide a means for health IT to share structured (but potentially non-standardized) "candidate" and "emerging" data elements, as well as the constantly-evolving class of data that is neither standard, nor structured as an unstructured document.

[8] AMIA Policy Principles: Health IT Data Standards & Interoperability: https://www.amia.org/sites/default/files/2018-2019-AMIA-Health-Informatics-Policy-Priorities.pdf#page=14
[9] USCDI Draft Policy (2018) https://www.healthit.gov/sites/default/files/draft-uscdi.pdf
[10] AMIA Comments (Feb. 2018) https://www.amia.org/sites/default/files/AMIA-Comments-on-USCDI.pdf
[11] HL7 Implementation Guide for CDA®, Release 2: Unstructured Documents https://www.hl7.org/implement/standards/product_brief.cfm?product_id=259
[12] C-CDA on FHIR Implementation Guide (IG) http://www.hl7.org/fhir/us/ccda/

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

In addition to the "bottom-up" graduation of "emerging," "candidate," and "supported" data classes articulated in the 2018 policy, a "share now, standardize as needed" approach would create market incentives to improve interoperability over the near-term for unstructured EHI. Health IT developers would have more impetus to coordinate with standards development organizations (SDOs) to standardize important, yet unstructured data, if they are forced to share such data routinely. Sharing non-standard data requires time and resources to build interfaces and enable interoperability, so enabling patients, clinicians, and researchers to demand unstructured data will incentivize standardization of frequently sought-after data due to the expense driven by the demand.

One way to operationalize this recommendation is to include the "Unstructured Document" document-level template and corresponding C-CDA-on-FHIR IG as part of USCDI's Clinical Notes data class. This approach would establish an expectation that health IT can exchange emerging, candidate, and unstructured data – not just the supported data elements named as part of the USCDI at §170.213. Adding the Unstructured Document and corresponding FHIR specification as part of the USCDI's Clinical Notes requirements would better address the Cures Act "all data elements" provision mandated by Congress, and it would provide a rational basis for a policy where all EHI is subject to information blocking provisions as a Condition and Maintenance of Certification.

These recommendations notwithstanding, AMIA strongly supports many proposals made by ONC in this NPRM. Below, we offer summary feedback based on the proposed rule's three major components: (1) Standards and Enhanced Certification Criteria; (2) Conditions and Maintenance of Certification; and (3) Information Blocking. Additional details on ONC's granular proposals can be found as an enclosure to this transmittal letter.

Standards and Enhancements to Certification Criteria

We appreciate ONC proposing a set of standards and specifications that both reflect where industry is in 2019 and where industry is going in the future. We support the use of FHIR as the standard for APIs, underpinned by specific Implementation Guides (IGs) and new concepts such as the US Core Data for Interoperability (USCDI), API Resource Collection for Health (ARCH), and the Standards Advancement Process. Our national healthcare system will be in continual pursuit of interoperability. Interoperability is not an end point, but a process. Use cases, data standards, and data sources will continue to evolve over time. The best approach ONC can take is to create informational feedback loops between implementers, users, and policymakers through clear and transparent processes to (1) identify anticipated changes to use cases, data standards, and data sources, and (2) establish sensible baselines that will encourage investment and innovation. To ONC's specific proposals in this section of the NPRM, AMIA offers the following recommendations:

- **Establish FHIR Release 4 (R4) as the foundational standard underpinning the USCDI and ARCH.** FHIR R4 is a normative standard today, which means it provides

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

better assurances of durability than prior Releases and will better accommodate future Releases.

- **Reference US Core IGs, rather than Argonaut IGs, for FHIR R4 implementation specifications.** Argonaut IGs have provided early uses cases with much-needed specificity, but they are tied to FHIR Release 2 and provide too much optionality for other uses portended by this NPRM. Further, it is not clear that Argonaut plans to update their IGs on a go-forward basis. Meanwhile, the US Core IGs are specified to FHIR R4 and maintained by HL7, an ANSI-accredited SDO with a proven track record of standards stewardship and an organization whose processes are compliant with the National Technology Transfer and Advancement Act. We note that these recommendations have implications for the draft test procedures released by ONC in early April.[13] These test procedures must reflect the use of FHIR R4 and US Core IGs. An integral aspect of this recommendation is that ONC finalize this NPRM as an Interim Final Rule, or IFR. Please see below for further discussion of why this is important.
- **Include the definition for electronic health information (EHI) at §171.102 as a persistent criterion of the USCDI policy listed at §170.213, and include the "Unstructured Document," document-level template (and corresponding C-CDA-on-FHIR IG) as part of USCDI's Clinical Notes data class as a means to enable broader access, exchange, and/or use of EHI through certified health IT.** AMIA is concerned the "structure first, share later" approach articulated by ONC's 2018 draft policy[14] and supported through technical specifications in this NPRM inappropriately positions health IT developers to control which data routinely and consistently are available for access, exchange, and use and which data are not. While we acknowledge that both HIPAA and forthcoming enforcement of the Information Blocking provision will compel actors to share non-standard/non-structured EHI when such data is requested, there will remain a wide disparity in capability to fulfill such requests if those data are separate from the USCDI policy.
- **Amend the EHI Export for Patient Access (§170.315 (b)(10)(i)) criterion to make data available via functional API, without necessarily standardizing the API or the data payloads.** AMIA notes that the bifurcation of the USCDI and EHI Export for Patient Access proposed by ONC creates a two-tiered system of access for patients: FHIR-based, API-enabled access for USCDI v1 supported data elements, and a static snapshot of all other EHI on the other. To correct this, ONC should require that certified EHRs support the EHI Export for Patient Access (§170.315 (b)(10)(i)) via functional API, analogous to a "GET request," so that industry stakeholders and government regulators can work toward a standardized API for managing export requests in future rulemakings, even as candidate, emerging, and unstructured data elements themselves are likely to remain developer-specific (i.e. non-standardized) for some time into the future. This recommendation follows ONC's original approach to §170.315(g)(8) APIs. ONC made access via APIs a functional

[13] Draft Test Procedures for (g)(10)-certified APIs: https://www.healthit.gov/sites/default/files/page/2019-03/170_315g_10_Standardized_API_for_Patient_and_Population_Services.pdf
[14] USCDI Draft Policy (2018) https://www.healthit.gov/sites/default/files/draft-uscdi.pdf

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

requirement, but it did not name a standard, with an expectation that standards would develop as the functionality become more widely available.

- **Constrain §170.315(g)(10) as proposed with the ARCH.** This will allow ONC to more efficiently dictate which USCDI data classes and data elements must be available for clinical, patient-facing and plan-facing exchange, while allowing the USCDI itself to be more inclusive of a broader set of standard and non-standard EHI.
- **Require certified health IT to export all EHI they produce and electronically retain as part of the "Database Export" at §170.315 (b)(10)(ii).** We support ONC's proposed approach to be agnostic regarding specific export standards initially, while requiring publication of documentation necessary to consume an export. However, we anticipate that even with documentation, successful consumption of a database export will require clear examples that are functional and work in the developer's sandbox.

Conditions and Maintenance of Certification (CMCs)

AMIA is focusing its attention on the API CMCs (omitting focus on fees), the Real World Testing (RWT) CMCs, Communications CMCs and the Assurances CMCs. Across these CMCs, we found most of the requirements to be effective translations of Cures statute into verifiable regulation. Some CMCs address a host of unintended consequences and unforeseen market reactions to the previous decade of Certification-related regulations (such as Assurances, RWT, Communications CMCs), while others attempt to prematurely address anticipated consequences and market reactions (such as API and Assurances).

It is worth noting that some of these CMCs require specific technical and/or functional requirements that position ONC to not only dictate timelines for development, but also timelines for technology adoption. Historically, the Centers for Medicare and Medicaid Services (CMS) has set expectations for provider adoption of certified health IT, but this NPRM includes provisions that would require adoption absent corresponding or complementary CMS requirements. While we understand the need for, and agree with, policies that compel adoption of new standards and functionality, we caution that ONC's purview should remain on certification and technology requirements, not provider adoption policies. Therefore, AMIA requests that ONC establish timelines for which certified health IT must be developed and avoid establishing timelines for clinical deployment in this NPRM. If the policy goal is to have all hospitals and physicians with deployed technology by 2022, we recommend ONC establish development deadlines no later than 2021 for (g)(10)-APIs, EHI export, and other functions with a 24-month timeline, and rely on CMS to establish an appropriate deployment timeline.

To ONC's specific proposals in this section of the NPRM, AMIA offers the following recommendations:

- **Finalize documentation and "pro-competitive provisions" CMCs for (g)(10)-APIs to increase the likelihood that they will be transparent, well-documented, and openly available in a fair and nondiscriminatory way.** While we have refrained from

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

commenting on permitted fees and the related aspects of this NPRM, we strongly support ONC's efforts to use CMCs to ensure that (g)(10)-APIs foster a robust and innovative ecosystem of patient-, clinician-, and researcher-facing applications. Finalizing the transparency and non-discrimination provisions will be particularly important.

- **Require API Technology Suppliers to verify the existence of a privacy notice for each application requesting registration by an API User.** We recommend all Third-Party API Users must attest "yes" or "no" to having a privacy notice for each application meant to register with the API Technology Supplier. These privacy notices should be commensurate with ONC's Model Privacy Notice.[15] This attestation will provide (1) transparency to First-Order API Users about the existence or lack of stated privacy practices and data uses and (2) regulators a means to enforce acts of deceptive/misleading conduct.
- **Finalize all Communications CMCs as proposed.** Regarding unqualified protections, work to develop corresponding guidance on reporting pathways to patient safety organizations (PSOs) and "government agencies."
- **Delineate expectations for EHI Export and (g)(10)-API access development timelines from deployment timelines for Assurances CMCs, API CMCs, and RWT CMCs.** While we support a two-year time horizon for development, implementation, and go-live, we do not support ONC dictating the adoption schedule for providers. ONC should shorten the development timeline by 12 months to allow providers 12 months to evaluate and implement these functionalities in production. We reiterate that ONC should remain focused on the technology, while other HHS agencies and offices dictate adoption policies.
- **Update 2015 Edition to 2020 Edition, rather than simply revising the 2015 Edition base definition.** We understand that other regulatory references, most notably those made by CMS, will also need updating, but ONC should proceed with the Edition concept it established in 2014 as a means to describe significantly different functionality and versions of software.

Information Blocking

AMIA views with skepticism any presumption that impeded data flows are categorically deemed "information blocking." In meetings with ONC and OIG during the summer of 2017, we provided policymakers with our "Socio-Technical Interoperability Stack," (see Appendix B). Information Blocking is not simply the absence of interoperability; interoperability may not occur for myriad reasons. In addition to being dependent on standards for syntax, semantics, and transport, interoperability within the healthcare context needs agreement on when and how data should be presented within workflows. Which data appear in a patient's record on what timeline may change depending on clinical workflows, types of data, and patient characteristics. Healthcare interoperability also depends on a host of public policies, such as 42 CFR Part 2 or HIPAA, as well as business drivers, intellectual property, contractual obligations, and medico-legal interpretations.

[15] See https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn.

May 23, 2019

As we interpret the information blocking definitions and provisions in this NPRM, we note that the breadth of the policy appears to capture all categories of the Socio-Technical Interoperability Stack and nominally requires all EHI be available whenever requested. While we strongly support this policy goal, we caution ONC and OIG against reflexively labeling a lack of exchange as implicating the information blocking provision. We also caution ONC against pursuing too vigorously an agenda focused on information blocking at the expense of other important activities related to its core competency of coordinating standards and enhancing layers of the Traditional Technology Stack.

Having noted these observations, AMIA views most of the Information Blocking exceptions and associated conditions to qualify for such exceptions as reasonable. However, we recommend the following for ONC to consider as it finalizes the Information Blocking exceptions and related provisions:

- **Finalize the policy so that all EHI is subject to the information blocking rule.** While we weighed an alternative recommendation to constrain the universe for which a claim of information blocking could be levied to a subset of EHI (e.g. the USCDI or ARCH) such an approach would perpetuate the "standardize first, share later" paradigm we caution against. Further, such a constraint would leave a host of "emerging," "candidate," and "unstructured" data classes outside the reach of this policy and likely prove more difficult to access, exchange and/or use because there is no legal requirement to share those data. Such a constraint would keep in place the status quo, which is clearly insufficient.
- **Institute a period of enforcement discretion to help stakeholders learn and avoid wasteful litigation.** To help stakeholders adjust to the new information blocking provisions and new definitions for EHI, AMIA recommends a period of enforcement discretion that would have OIG require corrective action plans – rather than levy fines which would likely lead to litigation – where claims of information blocking are found to be warranted. This period should not last more than 3 years from finalization of this NPRM and all claims – substantiated and unsubstantiated – should be made publicly available for stakeholders to study.
- **Revisit and ultimately reduce the scope of the definitions for "Health Information Network" and "Health Information Exchange," by focusing on whether the actor has (1) decision-making authority for governance of access, exchange, or use of EHI; (2) substantial influence of a technology or service that facilitates interoperability; and (3) handles data predominantly considered EHI, rather than non-health data.** The current definitions appear to be too broad to be implemented effectively without significant burden to ancillary actors. The unintended consequences of exposing an unforeseen number of individuals and entities to the HIN or HIE designation is likely to create an immense undue burden on many participants throughout the healthcare industry. This burden is only exacerbated by the "transitive" nature of the proposed policy to implicate both certified and non-certified software developed by the accused information blocker and the burden of proof that lies upon those accused of information blocking.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

- **Finalize the definition of EHI as proposed and associate actors that access, exchange, or use EHI as those that produce and electronically retain EHI.** We note that the definition of EHI is quite broad, but such a scope is important to advance and promote access, exchange, and use of health data, especially as data sources and data types evolve.
- **Subdivide the definition 'API User' into two separate classes of stakeholder.** API Data User should be split into 3rd Party and 1st Order API Users to delineate between those API Users who develop third-party software to read/write with (g)(10)-certified APIs, and those API Users who are end users of such third-party software, such as patients, clinicians, and researchers. A delineation of some kind is important because these are two very different types of stakeholder with different roles, requirements, and rights to EHI.
- **Ensure that claims of exception to Information Blocking are (1) well-documented; (2) reviewed by OIG in a timely manner; and (3) publicly available online in a searchable manner.** We urge ONC and OIG to be precise and consistent when allowing exceptions so that they do not become the new path to information blocking. Exceptions can be justified using weak claims (especially for exceptions related to harm and for infeasibility) so we recommend that ONC and OIG require detailed explanation of the rationale for the exception, with evidence, and that OIG review claimed exceptions in a timely manner. The results of each investigation, regardless of outcome, should be publicly available online via searchable database so that clarifying guidance and educational information can be broadly disseminated in a timely fashion.

While AMIA supports numerous ONC proposals, this NPRM contains a host of technical requirements that have important and far-reaching policy implications. Specifically, we believe explicit attention should be paid to how these policies will impact patient privacy beyond the current parameters of HIPAA, and we question ONC's efforts to dictate adoption timelines for providers.

Privacy in a Robust, API-driven App Ecosystem

Most urgently and acutely, the functional requirements for APIs are buttressed by a series of policies that reinforce the need to make all patient data available via APIs. While AMIA strongly supports such an approach, this NPRM contains a confluence of policies meant to position patients as mediums to a vast, yet nascent ecosystem of clinician-, researcher- and patient-facing apps, which will rely on new-found access to data produced and retained by certified health IT.[16] When this future is viewed alongside the current reality of scant consumer protections outside the HIPAA-

[16] Farr C. Health care is one of Apple's most lucrative opportunities: Morgan Stanley. CNBC https://www.cnbc.com/2019/04/08/apple-could-top-300-billion-in-sales-from-health-care-morgan-stanley.html

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

regulated environment, the near-term goal espoused by the "without special effort" clause in Cures has the real and significant potential to create privacy risks and opportunities for fraud.[17, 18]

We do not raise these concerns to advise ONC against proceeding with these policies. The challenges posed to privacy, fraud, and abuse in the near-term API-driven future are far too large for ONC to handle on its own; these challenges likely are beyond the scope of HHS, and even the current statutory authority of the whole Executive Branch to address adequately. We anticipate that Congress will need to act to fill the consumer protection gaps residing just beyond the reach of HIPAA – either now, as part of ongoing consumer data protection legislation, or at some point after more demonstrable harm is committed against Medicare and Medicaid beneficiaries and other patients who understand erroneously that their data is protected from misuse.[19, 20]

To address these privacy concerns, AMIA encourages ONC to influence – in a positive manner – the continued blurring of clinical and consumer information systems. For example, this NPRM is silent on elements of – and in fact discourages – API Technology Suppliers from instituting a vetting process for API Users. Further, the NPRM is silent on the rights and responsibilities of API Data Providers in relation to API Users. While the notion of a government-run app store or a centrally-managed app vetting process would not be palatable for several reasons, AMIA recommends a host of direct and indirect actions to help promote the privacy and security of patient data:

1. As stated above, ONC should disambiguate API Users into two distinct stakeholder groups. 3rd Party API Users who develop software and interact with API Technology Suppliers and 1st Order API Users who are end users of the software developed by 3rd Party API Users;
2. ONC should, as an API Condition and Maintenance of Certification provision, ensure that API Technology Suppliers require 3rd Party API Users to attest to having in place a Privacy Notice, modeled from ONC's work,[21] for each app the 3rd Party API User develops as part of the API Technology Supplier's registration process; and

[17] Petersen C, Lehmann C. Social Media in Health Care: Time for Transparent Privacy Policies and Consent for Data Use and Disclosure. Appl Clin Inform. 2018 Oct;9(4):856-859. https://www.ncbi.nlm.nih.gov/pubmed/30485880

[18] Grundy, Chiu. et al. sought to understand how user data are shared by top rated medicines related mobile applications (apps) and to characterize privacy risks to app users, both clinicians and consumers. They found that sharing of user data is routine, yet far from transparent. 79% of sampled apps shared user data and 55 unique entities, owned by 46 parent companies, received or processed app user data, including developers and parent companies (and service providers. Q Grundy Q, Chiu K. et al. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019;364:l920 https://www.bmj.com/con.tent/364/bmj.l920

[19] Mathews A. Tech, Health Firms Race to Help Consumers Manage Personal Data. Wall Street Journal. April 2, 2019. https://www.wsj.com/articles/tech-health-firms-race-to-help-consumers-manage-personal-data-11554197400

[20] Harwell D. Is your pregnancy app sharing your intimate data with your boss?. Washington Post. April 10, 2019. https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.06d4c3edf544

[21] See ONC Model Privacy Notice at: https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

3. ONC could define "patient authorized representative" narrowly as "a person within the continuum of medical care or with a medical power of attorney or legal guardianship" for purposes of EHI Export for Patient Access (§170.315 (b)(10)(i)) as it defines "users" of such functionality. This would be distinguishable from requests made by insurers or third-party legal requests that seek information without appropriate patient-direction and beyond what is part of the HIPAA "Designated Record Set;" and
4. Take explicit and public steps to implement recommendations of the 2016 API Task Force[22] to foster secondary markets for application endorsements, where stakeholders (e.g. health IT developers, patients, consumer advocacy groups, clinical specialty societies and provider organizations) can endorse apps for meeting specified expectations of performance. This kind of infrastructure would enable third-party app discovery services where consumers can filter apps based on those criteria they consider most important. Further, it would provide API Data Providers, API Technology Suppliers, and 1st Order API Users that apps of potential use have met specified requirements, as prioritized by various stakeholders.

Regulatory Responsibilities to Develop and Deploy Certified Technology

Another example of how specific technical or functional requirements may complicate existing policies is with ONC-defined timelines for technology adoption. Historically, the Centers for Medicare and Medicaid Services (CMS) has set expectations for provider adoption of certified health IT through the EHR Incentive Payment Program and more recently through various Medicare & Medicaid payment rules. However, this NPRM includes provisions that would require adoption of specific certified functionalities on a specific timeline without corresponding or complementary CMS requirements. These functionalities include the need to have deployed APIs (§170.315(g)(10)), the ability to provide both a EHI Export for Patient Access (§170.315 (b)(10)(i)) for patients; and an Assurance Condition & Maintenance of Certification requirement that updates the definition of Base EHR at §170.315(b)(10) for which all providers must possess.

While we understand the need for, and agree with, policies that compel adoption of new standards and functionality, we recommend that ONC remain focused on certification and technology requirements, not provider adoption policies. Therefore, AMIA recommends that ONC establish timelines for which certified health IT must be developed, not deployed. If the policy goal is to have all hospitals and physicians with deployed technology by 2022, we recommend ONC establish development deadlines no later than 2021 for (g)(10)-certified APIs, EHI export, and other criteria currently proposed to be deployed within a 24-month timeline. A preferred approach would be to define explicit timelines for deployment and leave other HHS agencies – such as CMS – to establish adoption/deployment timelines. This division of regulatory authority provides stability for regulated industry, accountability for regulators, and transparency for all stakeholders.

[22] ONC Federal Advisory Joint Application Programming Interface (API) Task Force Recommendations, 05/12/2016 https://www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf#page=16

May 23, 2019

Last, we strongly recommend ONC proceed with a regulatory schedule that includes an Interim Final Rule (IFR) with a 30-day comment period. This will allow ONC to make final determinations on the readiness of FHIR Release versions and related Implementation Guides later in 2019, rather than at the time when clearance by other agencies is initiated. An IFR will also give ONC the option to incorporate stakeholder feedback on a range of options and ideas it did not propose in this NPRM, but which will nonetheless increase the likelihood of ONC achieving its policy objectives.

We continue to appreciate ONC's work in this important area, and we are eager to bring the expertise of health informatics professionals to this national priority. Thank you for considering our comments. Should you have questions about these comments or require additional information, please contact Jeffery Smith, Vice President of Public Policy at jsmith@amia.org or (301) 657-1291. We look forward to continued partnership and dialogue.

Sincerely,

Douglas B. Fridsma, MD, PhD, FACP, FACMI
President and CEO
AMIA

Peter J. Embi MD, MS, FACP, FACMI
AMIA Board Chair
President & CEO
Regenstrief Institute

(Enclosed: Detailed AMIA Recommendations to ONC Cures Act NPRM)

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

May 23, 2019

Table of Contents:

Section III – Deregulatory Actions for Previous Rulemakings

Removal of Randomized Surveillance Requirements

ONC proposes that ONC-ACBs must conduct in-the-field, randomized surveillance to specify that ONC-ACBs may conduct in-the-field, randomized surveillance. They further propose to remove § 170.556(c)(2), which specifies that ONC-ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. They also propose to remove the requirements in § 170.556(c)(5) regarding the exclusion and exhaustion of selected locations for randomized surveillance. Additionally, they propose to remove the requirements in § 170.556(c)(6) regarding the consecutive selection of certified health IT for randomized surveillance.

AMIA Response: AMIA Supports this removal considering new and more detailed conditions and maintenance of certification requirements for which CEHRT must adhere and ONC-ACBs must corroborate.

Removal of Certain 2015 Edition Certification Criteria and Standards

ONC has identified both criteria and standards for removal as proposed below and believes the removal of these criteria and standards will reduce burden and costs for health IT developers and health care providers by eliminating the need to: design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting and disclosure requirements; maintain and update certifications for certified functionalities; and participate in surveillance of certified health IT.

AMIA Response: AMIA supports removal of the identified criteria and standards from 2015 Edition criteria for the reasons articulated by ONC and because there are no longer CMS requirements to engage in such functions for some of these listed criteria. However, we note that

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

secure messaging and patient-specific education resources remain important aspects of health IT-supported care delivery, and we urge ONC to be receptive to user complaints regarding the degradation of such functions.

Removal of Certain ONC Health IT Certification Program Requirements

ONC proposes to remove certain mandatory disclosure requirements and a related attestation requirement under the Program. They believe removal of these requirements will reduce costs and burden for Program stakeholders, particularly health IT developers and ONC-ACBs.

AMIA Response: Again, AMIA supports removal of these requirements considering the establishment of conditions and maintenance of certification requirements.

Recognition of Food and Drug Administration Processes

ONC's authority over health IT developers' health IT certified under the Program, they propose to establish processes that would provide health IT developers that can document holding precertification under the FDA Software Precertification Program with exemptions to the ONC Health IT Certification Program's requirements for testing and certification of its health IT to the 2015 Edition "quality management systems" criterion (§ 170.315(g)(4)) and the 2015 Edition "safety-enhanced design" criterion (§ 170.315(g)(3)). ONC also believes that such a "recognition" could, depending on the final framework of the FDA Software Precertification Program (e.g., the key performance indicators used to demonstrate performance and outcomes of excellence), be applicable to the functionally-based 2015 Edition "clinical" certification criteria (§ 170.315(a)). ONC welcomes comments on these and other aspects of its proposed "recognition" approach, including the 2015 Edition certification criteria that should be eligible for "recognition."

AMIA Response: As we understand it, FDA's Pre-Cert Program specifies that the business unit or business center – not the entire organization or entity – is granted precertification status. Given this understanding, we would only support the "recognition" described by ONC in circumstances where the business unit or center that has received precertification also produces and manages development of CEHRT. There needs to be 1-to-1 alignment between the developer of the CEHRT and the precertified entity – a business unit that develops Software-as-a-Medical Device (SaMD) inside a larger developer of CEHRT, for example, should not be deemed as meeting Edition "quality management systems" criterion (§ 170.315(g)(4)) and the 2015 Edition "safety-enhanced design" criterion (§ 170.315(g)(3)).

Section IV – Updates to the 2015 Edition Certification Criteria

United States Core Data for Interoperability Standard (USCDI)

ONC proposes, as a Maintenance of Certification requirement for the real-world testing Condition of Certification, that health IT developers with health IT certified to the five above-identified certification criteria prior to the effective date of a subsequent final rule would have to update such certified health IT to the proposed revisions. They further propose, as a Maintenance of Certification requirement for the real-world testing Condition of Certification, that health IT developers must provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of a final rule for this proposed rule.

AMIA Response: AMIA supports removal of the CCDS definition and inclusion of the USCDI standard (USCDI v1). We recommend that the USCDI v1 be supported through FHIR Release 4 and US Core IGs. While we support efforts to make this functionality available within 24 months of this final rule, we recommend ONC establish a developer timeline to have such capability certified within 12 months for those developers who are currently certified to the 2015 Edition. Further, we recommend ONC abstain from establishing deployment timelines and work with other HHS agencies to establish an adoption/deployment timeline with the expectation that such functionality will ultimately be available within 24 months as intended. This will give providers an additional 12 months to adopt the updated standards and relieve ONC from having to dictate both development and deployment deadlines.

Also, we note that ONC is requesting an exemption for USCDI from The National Technology Transfer and Advancement Act (NTTAA) requirements that standards adopted by the Federal government must be developed or adopted by voluntary consensus standards bodies. We do not support this exemption, but rather believe that a fair and openly participative process must be utilized for the development of USCDI standards moving forward.

Updated Versions of Vocabulary Standard Code Sets

ONC proposes that the USCDI Version 1 (USCDI v1) include the newest versions of the "minimum standard" code sets included in the CCDS available at publication of a subsequent final rule. They request comment on this proposal and on whether this could result in any interoperability concerns.

AMIA Response: AMIA supports the requirement to use the newest version of the "minimum standard" code sets included in the CCDS available at publication of a subsequent final rule for the USCDI v1. This approach has worked well in previous Edition updates and we anticipate that so long as newer versions maintain a reasonable degree of backward compatibility there should be little concern for ongoing interoperability.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

ONC is also considering changing the certification baseline versions of the code set for these criteria from the versions adopted in the 2015 Edition final rule to ensure complete interoperability alignment.

AMIA Response: AMIA supports requirements to use minimum standard code sets for these criteria.

The USCDI v1 includes new data elements for "address" and "phone number." The inclusion of "address" (to represent the postal location for the patient) and "phone number" (to represent the patient's telephone number) would improve the comprehensiveness of health information for patient care.

AMIA Response: AMIA strongly supports inclusion of these new data classes and data types. We recommend ONC point towards established standards for address, such as the USPS standard, and phone number.

The USCDI v1 includes a new data class, titled "clinical notes." "Clinical notes" is included in the USCDI v1 based on significant feedback from the industry since the 2015 Edition final rule. Specifically, ONC proposes to include the following clinical note types for both inpatient and outpatient (primary care, emergency department, etc.) settings in USCDI v1 as a minimum standard: (1) Discharge Summary note; (2) History & Physical; (3) Progress Note; (4) Consultation Note; (5) Imaging Narrative; (6) Laboratory Report Narrative; (7) Pathology Report Narrative; and (8) Procedures Note. ONC seeks comment on whether to include additional note types as part of the USCDI v1.

AMIA Response: We support the inclusion of "clinical notes" as a data class within the USCDI v1. However, we recommend ONC include the full suite of C-CDA documents-level templates as part of this data class, understanding that not all templates have corresponding FHIR IGs. Of particular interest are the "Unstructured Documents" document-level template and the Operative Report Note,[23] and we recommend ONC include those note types as part of "clinical notes," data class to improve exchange of both structured and non-structured data. Further, we note that C-CDA on FHIR[24] is an active community whose contributions will help improve interoperability of notes – both as structured and free-text data. We encourage ONC to support this effort as it progresses.

The USCDI v1 also includes a new data class, titled "provenance." "Provenance" has been identified by stakeholders as valuable for interoperable exchange. ONC proposes to further delineate the provenance data class into three data elements: "the author," which represents the person(s) who is

[23] as defined in CMS Conditions of Participation §482.51(b)(6).
[24] http://hl7.org/fhir/us/ccda/index.html

responsible for the information; "the author's time stamp," which indicates the time the information was recorded; and "the author's organization," which would be the organization the author is associated with at the time they interacted with the data. ONC requests comment on the inclusion of these three data elements and whether any other provenance data elements, such as the identity of the individual or entity the data was obtained from or sent by (sometimes discussed in standards working groups as the provenance of the data's "last hop"), would be essential to include as part of the USCDI v1 standard.

AMIA Response: AMIA supports this new data class and data elements. However, we anticipate that more granularity will be needed for Provenance Data Elements, such as "role of the individual," (e.g. ordering/verifying/supervisor author). Additionally, there could be at least two more important aspects of provenance, such as path and validity. The path would identify how the data got from the originator to the current location. The validity would be shared by a validation key, usually some form of hash or checksum, that allows the recipient to confirm that the data has not been changed since it left the originator. AMIA recommends ONC make "Provenance" a functional requirement, rather than a named standard given that more work needs to be done before an industry consensus standard and consensus based best practices for tagging and use are available.

Unique Device Identifier (UDI) for a Patient's Implantable Devices: CDA Implementation Guide

ONC requests comment on whether it should add this UDI IG as a requirement for health IT to adopt in order to meet the requirements for UDI USCDI Data Class. In addition, they do not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, request comment on the cost and burden of complying with this proposed requirement.

AMIA Response: AMIA supports further investigation by ONC and the standards community with respect to the value and costs of implementation of the sending (and receiving) UDI parts in discrete aspects as defined in this guide, or as a string that can be parsed when needed, as is currently defined in C-CDA R2.1. There is considerable interest and concern by stakeholders who advocate for each option and we recommend more work is warranted. This may be another instance where an IFR would provide additional opportunity for ONC to delay a final determination. The primary question is whether stakeholders prefer the optionality of the locations for the parsed UDI within this resource meets their needs.

Medication Data Request for Comment

The USCDI v1 "Medication" data class includes two constituent data elements within it: Medications and Medication Allergies. With respect to the latter, Medication Allergies, ONC requests comment on an alternative approach.

May 23, 2019

AMIA Response: Reviewing USCDI, Section 1 "Representing Patient Allergies and Intolerances; Medications," there are a series of comments that seem to address the concern of Medication Allergies, with the noted limitations. There are comments about the use of RxNorm, medication class, SNOMED and MED-RT, yet no conclusion.

The concern as a clinician is documenting (a) medication allergy versus (b) medication intolerance or (c) medication adverse reaction. These items (b & c) do not seem to be addressed in the USCDI.

§ 170.205(a) Patient summary record

ONC proposes to adopt the HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1 C-CDA Companion Guide to support best practice implementation of USCDI v1 data classes and enhance the implementation of other 2015 Edition certification criteria that also reference Consolidated Clinical Document Architecture (C-CDA) Release 2.1 (§ 170.205(a)(4)). Those criteria include:

1. "transitions of care" (§ 170.315(b)(1));
2. "clinical information reconciliation and incorporation" (§ 170.315(b)(2));
3. "care plan" (§ 170.315(b)(9));
4. "view, download, and transmit to 3rd party" (§ 170.315(e)(1));
5. "consolidated CDA creation performance" (§ 170.315(g)(6)); and
6. "application access – all data request" (§ 170.315(g)(9)).

AMIA Response: AMIA supports adoption of the C-CDA Companion Guide to promote better adherence – and improved interoperability – of data contained in Clinical Notes. We agree the companion guide should be used to encourage best practice and agree that the C-CDA standard itself should be used for certification criteria. In addition, we encourage ONC to reference the latest version available of C-CDA and C-CDA companion guide at the time of this final rule publication.

§ 170.205(b) Electronic prescribing

ONC proposes to update the electronic prescribing (e-Rx) SCRIPT standard used for "electronic prescribing" in the 2015 Edition to NCPDP SCRIPT 2017071, which would result in a new e-Rx standard becoming the baseline for certification. In addition to proposing to adopt the NCPDP SCRIPT 2017071 standard for the transactions that are listed in the current "electronic prescribing" criterion (§ 170.315(b)(3)), ONC proposes to adopt and require conformance to all of the NCPDP SCRIPT 2017071 standard transactions CMS adopted at 42 CFR 423.160(b)(2)(iv) for NCPDP SCRIPT 2017071.

AMIA Response: AMIA supports the proposed update, as NCPDP SCRIPT 2017071 becomes mandatory for Medicare Part D electronic scripts January 1, 2020 and includes – among other helpful enhancements – support for Risk Evaluation and Mitigation Strategy (REMS). We also note that 42 CFR 423.160 addresses common concerns of providers, particularly an ability to determine

that a prescription has been filled by the patient. Communications between prescribers and dispensers have been limited; this recommendation includes other components meeting current prescribing practices; e.g., refill prescription transactions, prescription changes, cancelling prescriptions, and so on.

§ 170.205(h) Clinical quality measure data import, export and reporting

ONC proposes to incorporate by reference the latest annual CMS QRDA IGs, specifically the 2019 CMS QRDA I Implementation Guide for Hospital Quality Reporting and the 2019 CMS QRDA III Implementation Guide for Eligible Professionals (EPs) and Eligible Clinicians. A Health IT Module would need to be certified to both standards to provide flexibility to providers. However, ONC solicits comment on whether it should consider an approach that permits certification to only one of the standards depending on the care setting for which the product is designed and implemented. They also solicit comment on the future possibility of FHIR-enabled APIs replacing or complementing QRDA reports for quality reporting and improvement.

AMIA Response: AMIA recommends that ONC cite the CMS version(s) of the QRDA IG for certification similarly to how the C-CDA companion guide is sited, but only require certifying to the CMS version. QRDA is an IG of the CDA which re-uses C-CDA templates and the CMS IG is an implementation guide using QRDA. However, citing only the CMS IG may lead to misalignment with the base standards and reduce incentives to update the base standard. In addition, the Joint Commission also uses base QRDA and has their own version constrained for Joint Commission use cases. There may be other CMS Deemed Authorities, such as Healthcare Facilities Accreditation Program or Del Norske Veritas Healthcare with different standards and IGs. AMIA agrees that implementers should not have to certify for both. By default, if an implementer passes certification for the CMS QRDA, they should also pass the base QRDA.

§ 170.315(b)(10) Electronic health information export

ONC proposes to adopt a new 2015 Edition certification criterion for EHI export in §170.315(b)(10). This criterion is intended to provide patients and health IT users with a means to efficiently export the entire electronic health record for a single patient (b)(10)(i) or all patients (b)(10)(ii) in a computable, electronic format, and facilitate the receiving health IT system's interpretation and use of the EHI, to the extent reasonably practicable using the developer's existing technology.

Patient Access (b)(10)(i)

In the patient access context, ONC proposes that a user must be able to timely execute the single patient EHI export at any time the user chooses and without subsequent developer assistance to operate. The health IT developer should enable the user to make data requests and receive the export efficiently, without unreasonable burden. For example, the health IT developer should not:

require the user to make a request multiple times for different types of EHI; provide unreasonable delays for the export; or prohibit reasonable user access to the system during the export process.

"Timely" does not mean real-time; however, ONC stresses that any delays in providing the export must be no longer than reasonably necessary to avoid interference with other clinical functions of the health IT system. The export capability does not require that data be received instantaneously. Rather, a non-conformity would exist if delays were causing or contributing to users being presented with data files that no longer contained current, accurate, or valid data.

AMIA Response: AMIA strongly supports patients' right to have access to complete copies of their entire medical record in a computable format. We see the spirit of this new criterion as aligned with this right, but we caution that the EHI Export for Patient Access needs refinement as proposed.

There are several layers of ambiguity that will inhibit uniform implementation and widespread use of this functionality. First, we note that patients requesting an EHI export will likely obtain vastly different payloads based on three factors: (1) the health IT developers certified to deliver the export; (2) the implementation decisions and customizations at each implementation; and (3) the institution's interpretation of what constitutes EHI. Second, we note that widespread use of this functionality might be inhibited if the task of making sense of data falls largely on patients and families, rather than the developers or clinicians delivering the export.

Export difference across developers
Given that ONC does not propose specific transport, content, or syntax standards for EHI export (either Patient Access or Database Export), it is difficult to understand how ONC will judge conformance to this criterion. As we have seen in numerous other certification criteria, it is likely that developers are much more uniform in their conformance testing than in the real world, and it is very likely that this lack of specificity will deliver different exports for similar patients.

Export differences based on implementation decisions and customizations
ONC expects that EHI exports will encompass "all the EHI that the health IT system produces and electronically manages for a patient or group of patients." Holding aside the ambiguity of "produces and electronically manages," there is the simple fact that providers have made implementation decisions and customizations that likely differ across sites, even when using the same developer, which will enable some systems to deliver data that other systems cannot.

Export differences based on interpretation of EHI definition
ONC defines EHI broadly. EHI is a legalistic griffin of electronic Protected Health Information (ePHI) and Individually Identifiable Health Information (IIHI). Generally, health providers have struggled to define the Designated Record Set (DRS) consistently, which by comparison is a more constrained concept. Given that the definition of EHI not only dictates which data must be delivered via Patient Access and Database Export, but also scopes those data for which acts of Information Blocking could be implicated, there is a high probability that institutional interpretations will create differences in what similar patients receive as part of this criterion.

AMIA supports a broad definition of EHI and inclusive concept for what an EHI Export for Patient Access should deliver. In order to improve these differences and increase the utility of such exports, AMIA recommends ONC look for ways to constrain and/or guide implementation of these policies, while keeping the intent of these policies broad and inclusive. Specifically, AMIA recommends ONC:

- Specify that transport standard for EHI Export for Patient Access leverage RESTful protocols (e.g. APIs); and
- Require that the syntax standard utilize the C-CDA "Unstructured Documents" document-level template or as-yet-developed FHIR profile(s).

By specifying a functional requirement for EHI to be made available via API, we anticipate that industry stakeholders and government regulators can work toward a standardized API for managing export requests in future rulemakings, even as the non-USCDI data payloads themselves are likely to remain developer-specific (or unstructured documents of free text) for some time into the future. Further, this paradigm will encourage more innovation to make the data useful to patients and families than a single and/or periodic "data dump" as the current proposal portends.

Definition of user for EHI export
As previously defined under the Program, "user" is a health care professional or his or her office staff; or a software program or service that would interact directly with the certified health IT. ONC typically would expect the "user" in this case to be a provider or his or her office staff who will be performing the request on behalf of the patient given that a request of this nature would likely occur in the context of an individual exercising their right of access under the HIPAA Privacy Rule. ONC seeks comment on whether this portion of the EHI export criterion should be made more prescriptive to only allow the patient and his or her authorized representative to be the requestor of their EHI, similar to how ONC have previously scoped such criteria as "view, download, and transmit to 3rd party."

AMIA Response: AMIA supports a dual interpretation of "user" to include both a health care professional (or his/her office staff) or a patient using a technology application to execute the request without needing a provider to do so on their behalf. Given the breadth of data presumably available via EHI Export for Patient Access we also recommend that ONC establish an explicit expectation for its "use," in addition to "users." Specifically, the EHI Export for Patient Access should be tied to "HIPAA compliant uses," which would be provider access for treatment, payment, or operations for the purposes of continuity of care, and patient data access for whatever purpose they deem appropriate.

We do not support inclusion of "software programs or services," as a "user" in the context of EHI Export for Patient Access without express consent from the patient, the patient's legal guardian or caregiver. Give the current regulatory gaps that exist outside HIPAA, we are concerned that health app terms and conditions could expose all a patient's EHI without the patient's knowledge or desire. Clear guidance and education will be needed.

Privacy and security concerns related to users
ONC acknowledges potential privacy and security concerns may arise when EHI is exported and, therefore, proposes that for provider-mediated requests, a developer may design the health IT to limit the type of users that would be able to access and initiate EHI export functions.

AMIA Response: We expect the same systems and controls that protect record requests today to be in place for EHI export functionality, up to and including limitations based on type of provider utilizing this functionality.

Transitions Between Health IT Systems aka Database Export (b)(10)(ii)
ONC proposes that a health IT developer of health IT certified to this criterion must, at a customer's request, provide a complete export of all EHI that is produced or managed by means of the developer's certified health IT.

AMIA Response: AMIA supports this functionality and we generally support flexibility regarding how the outcome of a database export is achieved so long as the system provides the relevant data dictionary and documentation, as outlined by ONC, and is required to complete a Database Export as part of initial Certification.

Scope of EHI
For both use cases supported by this criterion, EHI export encompasses all the EHI that the health IT system produces and electronically manages for a patient or group of patients. ONC seeks comment on the terminology used ("produces and electronically manages") and whether that captures its intent or whether there are any alternatives to the language it should consider to further clarify its intent.

AMIA Response: AMIA recommends ONC be consistent in its terminology by describing the scope of EHI as all the EHI that the health IT system "produces or can access, exchange, or use" for a patient or group of patients. The pertinent concept is that all ePHI and IIHI an EHR has access to should be included as part of the EHI export. Alternatively, "produce or electronically retains," would be preferred to the existing "produce and electronically manages." At a minimum, the requirement should be specified as both (1) produces and (2) electronically retains.

ONC understands that EHRs may not be the standard storage location for images and solicit comment on the feasibility, practicality, and necessity of exporting images and/or imaging information. ONC requests comment on what image elements, at a minimum, should be shared such as image quality, type, and narrative text.

AMIA Response: AMIA recommends that imaging reports, at a minimum, be among the image elements shared as part of the EHI Export. If a specific medical-grade image is requested by the patient, providers should have processes to deliver this information to the patient, but the EHI export may not be relied upon to deliver these kind of data.

ONC solicits comment on whether it should require, to support transparency, health IT developers to attest or publish as part of the export format documentation the types of EHI they cannot support for export.

AMIA Response: We agree that ONC should require health IT developers to publish as part of the export format documentation the types of EHI they cannot support for export. Without this documentation, determining what has been done will simply be impossible and over time, never determinable.

Timeframes

ONC seeks input on EHI export and timeframes. In particular, beyond exporting all the EHI the health IT system produces and electronically manages, should this criterion include capabilities to permit health care providers to set timeframes for EHI export, such as only the "past two years" or "past month" of EHI?

AMIA Response: Should ONC adopt our recommendation to make the criterion of EHI Export for Patient Access enabled through a functional (e.g. non-standard) API, this question would be rendered moot. However, if ONC proceeds with an export that is a static data snapshot, we would recommend this functionality. Giving export users an ability to choose a time frame will be important so that patients do not receive 2 years of data if they only want 1 month. However, we caution that this functionality should be dynamic and not locked to a specific time interval, especially a very short one. For someone with frequent visits or tests, they would have to remember to login and export their data at frequent intervals so as not to miss the opportunity to export the information.

Replaces the 2015 Edition "Data Export" Criterion in the 2015 Edition Base EHR Definition

ONC welcomes comments on whether this will leave health care providers without an export capability for an inordinate period of time such that ONC should require health IT developers to support the "data export" functionality for health care providers until the health IT developer attests to providing the new EHI export functionality to all of its customers.

AMIA Response: Although CCDs don't contain the complete contents of a patient's record, as the new EHI proposal requires, they do contain critical patient information that is structured and coded (unlike the EHI proposal). The structured/coded contents of CCDs are important for automated

migration of patient data when provider organizations switch from one EHR to another. Hence, we recommend that that 2015 edition certification requirement be retained at least until the new EHI export functionality is implemented and in use and we understand the degree of structuring/coding and standardization that EHR vendors will implement in complying with the new EHI proposal. Although the NPRM seems to be moving away from the C-CDA standard in favor of FHIR, there is still significant utility in CCDs for purposes such as bulk data export.

Section V – Modifications to the ONC Health IT Certification Program

§ 170.523 Principles of proper conduct for ONC-ACBs (Authorized Certification Bodies)

ONC proposes to clarify that HHS has the ability to access certification records for the "life of the edition," which begins with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations, not solely during the 3-year period after removal from the CFR.

AMIA Response: AMIA supports this clarification.

Section VI – Health IT for the Care Continuum

Approach to Health IT for the Care Continuum and the Health Care of Children

In order to implement the second part of Section 4001(b) of the Cures Act for the adoption of certification criteria to support the voluntary certification of health IT for use by pediatric health care providers, ONC has identified both the 2015 Edition certification criteria and the new or revised criteria in this proposed rule that it believes supports these 10 recommendations for health IT for pediatric care and sites of service.

AMIA Response: AMIA appreciates ONC's proposed clinical recommendations and believes that they represent a positive step forward for improving EHRs in the pediatric setting. Nonetheless, we recommend that ONC go further by developing the individual technical worksheets into detailed guidance and/or implementation specifications. For example, the 2015 Edition test method includes the detailed certification criterion along with both a Certification Companion Guide, and a formal test procedure. We believe that the development of pediatric-specific certification criteria to meet the proposed recommendations, along with certification companion guides and formal test procedures, will provide vital information to help guide implementation. ONC should be sure to involve both pediatric and usability experts in the development of the implementation guides and test procedures.

We also recommend additional ways to align 2015 Edition criteria with the pediatric setting. These include: 1) requiring vendors to involve pediatric patient and pediatric-specific factors in developing some of their test scenarios required for the 2015 Edition; 2) requiring inclusion of pediatric clinicians as part end-user testing; and 3) providing developers mock pediatric patient data for EHR testing. AMIA supports ONC's efforts to align the clinical recommendations with current and new certification criteria. We believe that taking these additional steps will strengthen the new voluntary certification program.

Request for Information on Health IT and Opioid Use Disorder Prevention and Treatment

2015 Edition Certification Criteria

ONC seeks comment on certification criteria previously adopted in the 2015 Edition that can support clinical priorities, advance interoperability for OUD (including care coordination and the effective use of health IT for the treatment and prevention of OUD). ONC seeks comment on how these criteria and what additional 2015 Edition certification criteria may be considered a clinical and interoperability priority for supporting OUD treatment and prevention. They also seek comment on the value of developing a potential future nonbinding informational guide or resource to provide useful information for OUD providers and sites of service related to specific clinical priorities and use cases of focus.

AMIA Response: We note that the limitations of many of the 2015 Edition certification criteria in general would also apply to patients with OUD. For example: The summary of care records that are typically transmitted are not generally very informative. Problem lists are typically incomplete and/or erroneous, accuracy of medication related information is variable, and there is not sufficient detail on current/past treatment and/or the patient's "story" to support care. Additionally, it is not possible to share with providers who do not use an EHR (as is common in psychiatry and SUD treatment). The use of approaches such as Direct for secure communication outside of a formal EHR does not seem to have achieved sufficient use to be of any benefit.

Clinical information reconciliation and incorporation is similarly of little help, unless each provider has EHR access and an ability to transmit and receive information. Given the high rates of erroneous information in EHRs, there is a risk that direct incorporation of information will propagate errors rather than reduce them. Further, depending on the mental status of the patient, reconciliation is often particularly challenging at the time of transfer. Instead, historical information may need to be confirmed and incorporated over time.

The electronic prescribing capacity is very helpful. Unfortunately, it does not necessarily simplify review of longitudinal information about prescriptions or information about dose adjustments between prescriptions.

Social, psychological and behavioral data are essential to obtain for individuals with OUD. as with all patients. We thus support inclusion of such information.

In relation to the issue of social data, it would be a major improvement if changes in standards were made to remove the substance use history (including opioid use) from "social history." Use of substances should not be framed as a "social" activity and drug use should not be conceptualized as "recreational." Rather, the history of substance use and treatment for substance use should be incorporated into the medical history just as a history of psychiatric illness, treatment, and hospitalizations is a part of the medical history. However, as long as EHRs include substance use with social history, it will be impossible to change clinical documentation and focus on the fact that these are medical disorders that require medical interventions, including medication assisted treatment and other non-medication interventions.

Developing specific informational material for ways to support OUD treatment and prevention in the EHR may be helpful, particularly if it could clarify aspects of 42 CFR Part 2 and/or make OUD specific implementation suggestions.

Revised or New 2015 Edition Certification Criteria in this Proposed Rule
This proposed rule contains additional proposals to revise or add new criteria to the Program to better support care across the continuum. ONC seeks comment specifically on the applicability of these criteria to the OUD use case.

AMIA Response: For data segmentation for privacy and consent management, the current state of commercial EHRs provides minimal flexibility in terms of tagging data that should be viewed as having a higher level of privacy (whether this is related to substance use, mental health, reproductive health, or adolescent medicine) and provides minimal flexibility in terms of patient-driven requests for enhanced privacy. We also acknowledge that standards for Data Segmentation for Privacy (DS4P) and Consent2Share (C2S) are under specified, currently unsupported through an active HL7 group, and in need refinement.

We support replacement of the current 2015 Edition DS4P criteria with the new DS4P-send and DS4P-receive criteria to support improved options for data segmentation in complex use cases. Likewise, we support the adoption of a FHIR-based consent management directive for APIs. These functionalities will be critical for the privacy of patient data, but the C2S standard is deficient in a number of areas that must be addressed. We strongly encourage ONC to engage with HL7 and healthcare stakeholders to rapidly improve the C2S standard through pilots. We acknowledge and appreciate ONC's current LEAP in Health IT Special Emphasis Notice towards fulfilling this recommendation.

We note that the underdevelopment of DS4P and C2S standards is likely due to the fact that these functions have never been required of certified health IT. To better ensure more rapid development ONC should require as part of certification the DS4P standards as proposed and a functional requirement to enable consent directives with FHIR-based APIs. We anticipate that many developers will choose to leverage the nascent C2S standard, but given that it is not actively

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

supported through SAMHSA or HL7 we do not support ONC solidify the current standard in regulation.

As for e-prescribing standards and PDMPs, the benefits delineated are welcome. With respect to REMS, it would be essential to mandate pharmacies to accept REMS information via this route. Ideally, any REMS-required documentation should be integrated into the EHR workflow to eliminate a need for a separate login and passwords for the REMS websites. It is additionally essential for PDMPs to be integrated directly into the workflow without additional data entry and logins by clinicians and without additional costly subscription add-on software products.

Emerging Standards and Innovations

ONC is engaged in a number of health IT and standards initiatives exploring innovation and emerging standards to inform future health IT policy. In some cases, these efforts may not be mature enough or best suited for adoption in the Program; however, ONC seeks comment on the potential consideration of these initiatives for future direction of ONC policy.

AMIA Response: We believe that CDS Hooks hold great promise for multiple aspects of integrating clinical guidelines into EHRs, including but not limited to OUD guidelines. As such, AMIA supports the development of CDS Hooks. For example, the CDC opioid guidelines appear to be having a number of unintended consequences in individuals with chronic pain who were on stable doses of opioids with apparent benefit and no evidence of misuse. Personalization of alerts as may be intermediated by CDS hooks would better identify appropriate candidates for opioid therapy.

In terms of care plans, we agree that having a shared care plan may be helpful in coordinating care across settings and could be valuable for individuals with many chronic disorders, and not just OUD. However, we note that the value of a care plan and the associated burden for clinicians may be very different depending upon the way that the care plan requirements are framed. Having a list of care plan elements, similar to current problem lists, would certainly be reasonable and could support collaboration and continuity of care. An elaborate SMART-goal based treatment plan requirement, however, would be unhelpful, burdensome, and distract from actual provision of care.

The field of behavioral health has been struggling for decades with the need to create formal multidisciplinary treatment plans, in addition to the treatment-related plans that are part of the assessment/plan of a clinical note. This distinct document currently has to be comprehensive and based on an inventory of the patient's strengths and disabilities. It also has to include individualized (i.e., free-text) measurable short-term and long-range goals using a "SMART" format in patient-centered wording, including a specific delineation of the treatment modalities used to fulfill the goal, the responsibilities of each member of the treatment team in reference to the goal, associated documentation that justifies treatment aimed at addressing each goal in daily clinical notes for each goal, reassessments of each goal within the specified time frames, and associated revisions of goals depending on patient progress. These efforts are highly duplicative and burdensome in terms of documentation and there is currently no evidence that these formats do anything to enhance care

over a more typical problem-oriented medical record note. Indeed, both the American Psychiatric Association and the National Association for Behavioral Health Care have pointed out the huge regulatory burden imposed on inpatient and other CMS-regulated facilities as a result of these treatment plan requirements.

Additional Comment Areas

ONC further seeks comment on effective approaches for the successful dissemination and adoption of standards including the NCPDP SCRIPT 2017071 standard that can support the exchange of PDMP data for integration into EHRs and also enable further adoption and use of Electronic Prescribing of Controlled Substances (EPCS). ONC seeks comment on the priority challenges and opportunities for these topics and on any technical and policy distinctions, as appropriate.

ONC also seeks comment on how successful implementation of health IT that supports OUD can aid in the achievement of national and programmatic goals, especially where they may align with initiatives across HHS and with stakeholder and industry led efforts. Finally, ONC seeks comment on a topic that involves health IT for both pediatric care and OUD prevention and treatment – Neonatal Abstinence Syndrome (or NAS).

AMIA Response: With regard to EPCS, it would be very helpful if standards could evolve to permit easier authentication of EPCS and use of dual factor authentication on a single device. However, to send a controlled substance prescription, they must use their phone to generate the automated authentication number and they must log in to a separate device to send the prescription. This creates problems when traveling or in other contexts where a second device is not readily available.

As for how health IT can aid in achieving national and programmatic goals, we believe that there should be recommended, standardized approaches that could both facilitate a streamlined ability to identify individuals with OUD from chart information and make sure that this gets added to the problem list if confirmed by a clinician. Some EHR systems have automated rules by which the system adds information to the patient's problem list, but these are not always accurate or helpful. With OUD, however, there is often information in the EHR that suggests an OUD is present; this could be used to give the clinician the option of adding OUD to the problem list.

Finally, our members who work in behavioral and mental health stress the importance of certification criteria to require that vendor systems be able to handle ordering, documentation and tracking of long-acting medications including long-acting injectable medications and other long-acting preparations (e.g., implants). A number of medications that are used for opioid treatment fall into this category, specifically long-acting intramuscular naltrexone and long-acting subcutaneous injections and implants of buprenorphine. The administration details of such treatments are not easy to document (unlike immunization administration which is typically configured for recording lot numbers and other information). These medications are typically ordered as "one-time" doses because they are given infrequently. As a result, they do not continue to appear as "active" medications on medication lists and do not continue to be available in the system for drug-drug

interaction checking despite their long half-lives. When long-acting medication are not readily viewable in EHRs, patient safety can be compromised. With the opioid medications, such as buprenorphine, an inability to view these long-acting formulations may lead to over-prescribing of opioids. This is compounded by the lack of inclusion of many of these compounds (including methadone administered in methadone maintenance programs) in PDMPs.

Section VII – Conditions and Maintenance of Certification

§ 170.402 Assurances

ONC proposes, as a Condition of Certification, that a health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program (Program) conforms to the full scope of the certification criteria to which its health IT is certified.

AMIA Response: AMIA supports this requirement.

ONC proposes that, as a complementary Condition of Certification, health IT developers of certified health IT must provide an assurance that they have made certified capabilities available in ways that enable them to be implemented and used in production environments for their intended purposes. More specifically, developers would be prohibited from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

AMIA Response: AMIA supports this requirement.

ONC proposes, as a Condition of Certification requirement, that a health IT developer that produces and electronically manages EHI must certify health IT to the 2015 Edition "electronic health information export" certification criterion in § 170.315(b)(10). Further, as a Maintenance of Certification requirement, ONC proposes that a health IT developer that produces and electronically manages EHI must provide all of its customers of certified health IT with health IT certified to the functionality included in § 170.315(b)(10) within 24 months of a subsequent final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer. Consistent with these proposals, they also propose to amend § 170.550 to require that ONC-ACBs certify health IT to the proposed 2015 Edition "EHI export" when the health IT developer of the health IT presented for certification produces and electronically manages EHI.

AMIA Response: AMIA supports the spirit of these requirements. We anticipate that 24 months following the effective date of a final rule should be sufficient time for the health IT developer to have upgraded their certified health IT to deliver an EHI export. However, we caution ONC against using this current wording: "must provide all of its customers…" This wording implicates both certified health IT developers and their customers as requiring this functionality within 24 months, extending ONC's regulatory reach beyond health IT developers to providers.

While we support a two-year time horizon for development, implementation, and go-live, we do not support ONC dictating the adoption schedule for providers. ONC should shorten the development timeline by 12 months to allow providers 12 months to plan and implement these functionalities in production. We reiterate that ONC should remain focused on the technology, while other HHS agencies and offices dictate adoption policies.

AMIA also supports the requirement that ONC-ACBs certify health IT to the proposed 2015 Edition "EHI export" when the health IT developer presents for certification produces and electronically manages EHI.

Trusted Exchange Framework and the Common Agreement – Request for Information

ONC requests comment as to whether certain health IT developers should be required to participate in the TEFCA as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

AMIA Response: It is difficult to answer this specific question, given that the TEFCA and its provisions are not yet finalized. We would, however, caution ONC against instituting a compulsory participation policy for the TEFCA, as it was envisioned in statute as a voluntary agreement.

§ 170.403 Communications

ONC states that this proposed Condition of Certification is needed to significantly improve transparency around the functioning of health IT in the field. This will help ensure that the health IT ultimately selected and used by health care providers and others functions as expected, is less likely to have safety issues or implementation difficulties, enables greater interoperability of health information, and more fully allows users to reap the benefits of health IT utilization, including improvements in care and quality, and reductions in costs.

AMIA Response: AMIA strongly supports Cures legislation and ONC's interpretation via this NPRM to make certified health IT performance more transparent. We are particularly supportive of new policies that will enable users and researchers of health IT safety to communicate broadly about their experiences and their findings.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

May 23, 2019

Protected Subject Areas

ONC proposes that the protection afforded to communicators under this Condition of Certification would apply irrespective of the form or medium in which the communication is made. Developers must not prohibit or restrict communications whether written, oral, electronic or by any other method if they concern protected communications, unless permitted otherwise by this Condition of Certification.

AMIA Response: AMIA strongly supports the articulated subject areas for which protected communications applies. We appreciate the examples offered in the NPRM and support them unequivocally.

Communications with Unqualified Protection

ONC proposes a narrow class of communications—consisting of five specific types of communications—that would receive unqualified protection from developer prohibitions or restrictions.

AMIA Response: AMIA supports the notion of communications with unqualified protections. However, we note that across these scenarios there is little if any corresponding guidance on reporting pathways to patient safety organizations (PSOs) and "government agencies." We recommend ONC work with federal partners to develop reporting protocols for patient safety, cybersecurity, and other protected communications so that these important kinds of communications are readily understood and acted upon.

Permitted Prohibitions and Restrictions

ONC proposes that health IT developers would be permitted to impose certain narrow kinds of prohibitions and restrictions.

AMIA Response: AMIA believes the facts of each case will require close scrutiny, but generally, we believe the permitted prohibitions and restrictions are reasonable.

Maintenance of Certification Requirements

ONC proposes that a health IT developer must notify all customers and those with which it has contracts/agreements, within six months of the effective date of a subsequent final rule for this proposed rule, that any communication or contract/agreement provision that contravenes this Condition of Certification will not be enforced by the health IT developer. Further, they propose that this notice would need to be provided annually up to and until the health IT developer amends the contract or agreement to remove or make void any contractual provision that contravenes this Condition of Certification.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

AMIA Response: AMIA views this enforcement prohibition and notification timeline as reasonable. We request ONC explicitly state that any permitted communication made following the effective date of the final rule be inadmissible as a violation of a contract/agreement regardless of whether the customer has been notified.

ONC further propose as a Maintenance of Certification requirement in § 170.405(b)(2) that health IT developers must amend their contracts or agreements to remove or make void any provisions that contravene the Condition of Certification within a reasonable period of time, but not later than two years from the effective date of a subsequent final rule for this proposed rule.

AMIA Response: AMIA requests that ONC clarify that such amendments need not be prescriptive or require unrelated aspects of such contracts to be renegotiated. Given that such provisions in contracts will be unenforceable by law as of the effective date of a final rule, we do not see a need for a prescriptive timeline. ONC could instead require that such contracts be amended at "the earliest available opportunity," or "at the behest of the customer of certified health IT."

VII.B.4 Application Programming Interfaces

§ 170.102 Definitions

API Data Provider refers to the organization that deploys the API technology created by the "API Technology Supplier" and provides access via the API technology to data it produces and electronically manages. In some cases, the API Data Provider may contract with the API Technology Supplier to perform the API deployment service on its behalf. However, in such circumstances, the API Data Provider retains control of what and how information is disclosed and so for the purposes of this definition is considered to be the entity that deploys the API technology.

API Technology Supplier refers to a health IT developer that creates the API technology that is presented for testing and certification to any of the certification criteria adopted or proposed for adoption at § 170.315(g)(7) through (g)(11).

API User refers to persons and entities that use or create software applications that interact with the APIs developed by the "API Technology Supplier" and deployed by the "API Data Provider." An API User includes, but is not limited to, third-party software developers, developers of software applications used by API Data Providers, and patients and health care providers that use apps that connect to API technology on their behalf.

AMIA Response: We recommend ONC divide the API Users category into (1) patient and health care provider end users of software as "First-Order API Users" and (2) third-party software developers and developers of software applications as "Third-Party API Users." This differentiation may provide ONC with more latitude to treat these parties differently in advantageous ways.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

§ 170.315(g)(10) Standardized API for patient and population services (Certification Criterion)

ONC proposes to adopt the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard as a foundational standard within its suite of proposals. Specifically, ONC proposes to adopt FHIR Draft Standard for Trial Use (DSTU) 2 (hereafter referred to as "FHIR Release 2") as a baseline standard conformance requirement. Given FHIR Release 4's public release, however, and that the industry will begin to implement Release 4 in parallel with this rulemaking, ONC requests comment on options it could pursue for a final rule.

AMIA Response: AMIA encourages ONC to finalize Option 4 – adopt only FHIR Release 4 in the final rule for reference in proposed § 170.315(g)(10). Release 4 is a normative standard and represents an achievable target for certified health IT to advance towards over the near-term. While we note that Option 4 places more responsibility on IGs to be up-to-date, compatible and ready for widespread implementation sooner, we are concerned that previous Releases contain too much optionality and the IGs that support them do as well.

In addition, AMIA recommends ONC proceed with a regulatory schedule that includes an Interim Final Rule (IFR) with a 60-day comment period, so that ONC can monitor progress of FHIR R4 adoption and US Core IG uptake over the next several months. This IFR gives ONC the ability to make a more informed final assessment on this set of questions, and it allows ONC to finalize a range of ideas and options that are necessary to meeting its policy objectives, but that were not included as part of this NPRM.

Proposed Adoption of Associated FHIR Release 2 Implementation Specifications

ONC proposes to adopt in § 170.215(a)(2) an implementation specification that would list a set of base FHIR resources that Health IT Modules certified to the proposed criterion in § 170.315(g)(10) would need to support. ONC refer to this proposed initial set of FHIR resources as the "API Resource Collection in Health" or "the ARCH." The ARCH would align with and be directed by the data policy specified in the proposed US Core Data for Interoperability (USCDI) standard (discussed in section IV.B.1 of this proposed rule).

AMIA Response: Given our support for FHIR R4, AMIA does not support adoption of associated FHIR Release 2 Implementation Specifications. Rather, we recommend ONC proceed with naming HL7 US Core Implementation Guides at § 170.215(a)(2). While we are cognizant that there is less experience with US Core IGs, than Argonaut IGs, we anticipate that the industry will coalesce around US Core IGs over the coming months, especially if ONC signals FHIR R4 as the standard underpinning the USCDI.

ONC refer to this proposed initial set of FHIR resources as the "API Resource Collection in Health" or "the ARCH." The ARCH would align with and be directed by the data policy specified in

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

the proposed US Core Data for Interoperability (USCDI) standard (discussed in section IV.B.1 of this proposed rule).

AMIA Response: Again, we recommend ONC proceed with naming US Core as the FHIR standard underpinning USCDI and ARCH.

ONC proposes to include 15 FHIR resources in the ARCH's first version. Based on prior industry efforts, including the Argonaut Project to map FHIR resources to the previously defined Common Clinical Data Set (CCDS), ONC knows that the following 13 FHIR resources map to and support the equivalent data classes specified in the USCDI: AllergyIntolerance; CarePlan; Condition; Device; DiagnosticReport; Goal; Immunization; Medication; MedicationOrder; MedicationStatement; Observation; Patient; and Procedure. In addition to these 13 FHIR resources, ONC have included two additional FHIR resources: 1) the Provenance resource; and 2) the DocumentReference resource to accommodate clinical notes.

AMIA Response: All of these FHIR resources are available in the US Core and we anticipate that these resources will better accommodate FHIR R4. AMIA reiterates our position that the "unstructured document" document-level template be included as part of clinical notes.

§ 170.404 Application programming interfaces (Condition of Certification)

Cures Act Condition and Interpretation of Access to "All Data Elements"

For the purposes of meeting this portion of the Cures Act's API Condition of Certification, ONC interpret the scope of: the ARCH; its associated implementation specifications; and the policy expressed around the data elements that must be supported by (g)(10)-certified APIs (i.e., FHIR servers) to constitute "all data elements." As these updates occur, the industry would be able to incrementally approach the totality of data that can be electronically accessed, exchanged, and used pursuant to the Cures Act's reference to "all data elements."

AMIA Response: AMIA views this interpretation of the Cures language as insufficient. As stated previously, we strongly recommend ONC finalize a policy that makes EHI available through the use of a "documented API," for individual EHI export, rather than the "standard API" defined for USCDI v1. This would operationalize a "share now, standardize as needed" approach.

Transparency Conditions

ONC proposes to establish a compliance date of six months from the final rule's effective date (which would give developers approximately eight months from the final rule's publication date) to revise their existing API documentation to come into compliance with the final rule.

AMIA Response: AMIA supports this timeline.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

Terms and Conditions Transparency
ONC proposes to require API Technology Suppliers to publish all terms and conditions for use of its API technology. ONC consider "terms and conditions" to include any fees, restrictions, limitations, obligations, registration process requirements, and other terms or conditions that would be material and needed to:

- develop software applications to interact with the API technology;
- distribute, deploy, and enable the use of software applications in production environments that use the API technology;
- use software applications, including to access, exchange, and use EHI by means of the API technology;
- use any EHI obtained by means of the API technology; and
- register software applications (as discussed in more below).

AMIA Response: AMIA supports this provision.

ONC specifically proposes to permit API Technology Suppliers to institute a process to verify the authenticity of application developers so long as such process is completed within five business days of receipt of an application developer's request to register their software application with the API technology's authorization server.

AMIA Response: AMIA supports an expedited process to onboard new API users and a 5-business day timeframe to register an app developer with the API technology's authorization server. We also appreciate that ONC wants to give API Technology Suppliers the ability to design an authentication / registration process that suits their needs. However, AMIA strongly recommends that ONC require Technology Suppliers to verify that the application developer is utilizing a privacy notice commensurate or comparable to ONC's Model Privacy Notice. Such a requirement appears to be among the few policies ONC can institute to help alleviate data privacy concerns and mitigate consumer fraud / abuse that will be possible in this new, API-driven ecosystem.

<u>Openness and Pro-competitive Conditions</u>
As a general condition, ONC proposes in § 170.404(a)(4) that API Technology Suppliers must grant API Data Providers (i.e., health care providers who purchase or license API technology) the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

AMIA Response: AMIA supports this policy, with the caveat that when patients request access to their data via registered app, API Data Providers must enable patients such access.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

Non-Discrimination
ONC proposes to require that API Technology Suppliers must provide API technology to API Data Providers on terms that are no less favorable than they would provide to themselves and their customers, suppliers, partners, and other persons with whom they have a business relationship.

AMIA Response: AMIA supports this policy.

ONC proposes that any terms and conditions associated with API technology would have to be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

AMIA Response: AMIA supports this policy.

API Technology Supplier would be prohibited from offering or varying such terms or conditions on the basis of impermissible criteria, such as whether the API User with whom the API Data Provider has a relationship is a competitor, potential competitor, or will be using EHI obtained via the API technology in a way that facilitates competition with the API Technology Supplier.

AMIA Response: AMIA supports this policy.

Rights to Access and Use API Technology
ONC proposes that an API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment.

AMIA Response: AMIA supports this policy. However, we request that ONC elaborate on the responsibilities of API Data Providers to make data available through APIs. For instances, are hospitals able to vet or register or otherwise collect information from API Users who access Data Providers' data? We reiterate our concerns for non-patient actors who gain access to EHI via APIs and we recommend that ONC differentiate between 3rd Party API Users and 1st Order API Users as so that these different stakeholders can be acknowledged as being different and treated differently under the law.

ONC proposes to prohibit an API Technology Supplier from imposing any collateral terms or agreements that could interfere with or lead to special effort in the use of API technology for any of the above purposes (e.g. fees to license, non-compete, exclusivity, etc.).

AMIA Response: AMIA supports this policy.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

Maintenance of Certification Requirements

ONC proposes in § 170.404(b)(1) a specific requirement for API Technology Suppliers that they would need to "register" (in connection with the API technology functionality proposed in § 170.315(g)(10)(iii)) and enable all applications for production use within one business day of completing its verification of an application developer's authenticity as described in proposed § 170.404(a)(2)(ii)(C).

AMIA Response: We are generally supportive of a process that creates low barriers to entry for application developers. In conjunction with the 5-day window an API Technology Supplier must verify the authenticity of an app developer, we view a one business day turnaround to enable applications for use to be reasonable. We note that as with other scenarios, volume may become an issue for API Technology Suppliers if they have many dozens of apps to verify during a given period.

ONC proposes to adopt in § 170.404(b)(2) a specific requirement that an API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed, and make such information publicly available (in a computable format) at no charge.

AMIA Response: AMIA supports this requirement.

ONC proposes in § 170.404(b)(3) that an API Technology Supplier with API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date.

AMIA Response: We note that development must precede deployment, therefore a development deadline must be established long before 24 months to enable a deployment timeline of 24 months. To reiterate an earlier recommendation, we recommend that ONC establish a development deadline for all existing API Technology Suppliers certified to § 170.315(g)(8) and leave deployment deadlines to other HHS offices and agencies. For API Technology Suppliers who have no pre-existing certification, we recommend ONC require adherence to certification criterion in § 170.315(g)(10) by 2021.

2015 Edition Base EHR Definition

ONC proposes to add compliance timeline language to the 2015 Edition Base EHR definition for the transition from §170.315(g)(8) to §170.315(g)(10) that would reflect a total of 24 months from

the final rule's effective date (which practically speaking would be 25 months because of the 30-day delayed effective date).

AMIA Response: We note that development must precede deployment, therefore a development deadline must be long before 24 months to enable a deployment timeline of 24 months. To reiterate an earlier recommendation, we recommend that ONC establish a development deadline for all existing API Technology Suppliers certified to §170.315(g)(8) and leave deployment deadlines to other HHS offices and agencies. For API Technology Suppliers who have no pre-existing certification, we recommend ONC require adherence to certification criterion in §170.315(g)(10) by 2021.

VII.B.5 Real World Testing

§ 170.405 Real world testing

The Cures Act requires, as a Condition and Maintenance of Certification under the Program, that health IT developers have successfully tested the real-world use of the technology for interoperability in the type of setting in which such technology would be marketed. ONC proposes to limit the applicability of this Condition of Certification to health IT developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange. ONC also solicit comment on whether any other 2015 Edition certification criteria should be included or removed from the applicability list for this Condition of Certification.

- The care coordination criteria in § 170.315(b);
- The clinical quality measures (CQMs) criteria in § 170.315(c)(1) through (c)(3);
- The "view, download, and transmit to 3rd party" criterion in § 170.315(e)(1);
- The public health criteria in § 170.315(f);
- The application programming interface criteria in § 170.315(g)(7) through (g)(11); and
- The transport methods and other protocols criteria in § 170.315(h).

AMIA Response: We agree with the list of certification criteria developed by ONC for RWT. With respect to the public health criteria at § 170.315(f), we note that public health organizations (like AIRA, APHL, ISDS, CSTE, and NAACCR) and most public health agencies have well-developed resources and processes to on-board provider organizations for interoperability transactions, test their interfaces with both hypothetical and real data, and ensure ongoing quality of the data being exchanged. Ideally, ONC would ensure that new requirements do not interfere or detract from the well-established testing processes that are already in place. At minimum, AMIA recommends ONC ensures that its RWT requirements do not create infrastructure for testing of public health transactions without public health involvement.

In addition, AMIA recommends ONC require EHI Export for Patient Data Access as an additional criterion for real world testing, for certified health IT that is certified for § 170.315(b)(10). Requiring

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

certified health IT to demonstrate this capacity outside the lab setting will be critical.

ONC proposes Maintenance of Certification requirements that would require health IT developers to submit publicly available prospective annual real-world testing plans and retrospective annual real-world testing results for its certified health IT that include certification criteria focused on interoperability. The plan would also need to address the health IT developer's real-world testing for the upcoming calendar year and include, for each of the certification criteria in scope:

- The testing method(s)/methodology(ies) that will be used to demonstrate real-world interoperability, including a mandatory focus on scenario- and use case-focused testing;
- The care and practice setting(s) that will be tested for real-world interoperability, including conformance to certification criteria requirements, and an explanation for the health IT developer's choice of care setting(s) to test;
- The timeline and plans for voluntary updates to standards and implementation specifications that ONC has approved (further discussed below);
- A schedule of key real-world testing milestones;
- A description of the expected outcomes of real-world testing;
- At least one measurement/metric associated with the real-world testing; and
- A justification for the health IT developer's real-world testing approach.

AMIA Response: These categories seem reasonable for RWT plans. However, we do question how ONC will ensure that plans and the plan results will be representative of the certified health IT's entire customer base. AMIA suggests for future consideration, and informed by experience with RTW, that a client of certified health IT subject to this provision be chosen at random.

ONC proposes that a health IT developer would submit annual real-world testing results to their ONC-ACBs via a publicly accessible hyperlink no later than January 31, of each calendar year for the preceding calendar year's real-world testing. Real-world testing results for each interoperability-focused certification criterion must address the elements required in the previous year's testing plan, describe the outcomes of real-world testing with any challenges encountered, and provide at least one measurement or metric associated with the real-world testing. As noted above, developers are encouraged to use metrics demonstrating real-world use from existing networks and communities. ONC seeks comment on whether ONC should require developers submit real-world testing results for a minimum "core" set of general metrics/measurements and examples of suggested metrics/measurements. ONC also invites comment on the proposed annual frequency and timing of required real-world testing results reporting.

AMIA Response: AMIA supports this cadence of RWT plan submission and review. We recommend that ONC should consider a minimal core set of metrics tied to a specific and pervasive health issue, such as congestive heart failure or diabetes.

Standards Version Advancement Process
ONC proposes to establish the Standards Version Advancement Process not only to meet the Cures Act's goals for interoperability, but also in response to the continuous stakeholder feedback that ONC has received through prior rulemakings and engagements, which requested that ONC establish a predictable and timely approach within the Program to keep pace with the industry's standards development efforts.

AMIA Response: AMIA supports the Standards Version Advancement Process. Along with the Interoperability Standards Advisory, the USCDI, and the ARCH, we see this as another important policy that will provide ONC a sub-regulatory mechanism to be more responsive to evolving standards development for health IT interoperability, based on engagement with industry stakeholders.

Section VIII – Information Blocking

§ 171.103 Information blocking

AMIA Response: AMIA views with skepticism any presumption that impeded data flows are categorically "information blocking." In meetings with ONC and OIG during the summer of 2017, we provided policymakers with our "Socio-Technical Interoperability Stack," (see Appendix B). Information Blocking is not simply the absence of interoperability; interoperability may not occur for myriad reasons. In addition to depending upon standards for syntax, semantics, and transport, interoperability within the healthcare context needs agreement on when and how data should be presented within workflows. Which data appear in a patient's record on what timeline may change depending on clinical workflows, types of data, and patient characteristics. Healthcare interoperability also depends on a host of public policies, such as 42 CFR Part 2 or HIPAA, business drivers, including intellectual property, contractual obligations, and medico-legal interpretations.

As we interpret the information blocking definitions and provisions in this NPRM, we note that the breadth of the policy appears to capture all categories of the Socio-Technical Interoperability Stack and nominally requires all EHI be available whenever requested. While we strongly support this policy goal, we caution ONC and OIG to avoid labeling a lack of exchange as implicating the information blocking provision. We also caution ONC about pursuing too vigorously an agenda focused on information blocking at the expense of other important activities related to its core competency of coordinating standards and enhancing layers of the Traditional Technology Stack.

§ 171.102 Definitions
Health Care Providers

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

May 23, 2019

ONC is considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition.

AMIA Response: AMIA supports this definition. We acknowledge that this expanded definition includes actors outside the traditional purview of in-patient and ambulatory care; however, these actors, including skilled nursing, home health, and long-term care are important players in the care continuum. These actors should be able to claim an exclusion to the information blocking provision if they do not possess certified health IT.

Health IT Developers
ONC proposes that "health IT developer of certified health IT" means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health IT (one or more) certified under the Program.

AMIA Response: ONC indicates that the rule would apply to vendors developing CEHRT and their products, whether those products are certified or not. One potential side effect is that vendors who provide public health applications (like IIS) as well as CEHRT software/modules would find that all of their products (CEHRT or not) subject to these regulations.

ONC is concerned about health IT developers who refuse to provide its customers with access to EHI following termination or withdrawal of certification. ONC is considering (1) including developers and offerors of certified health IT that continue to store EHI that was previously stored in health IT certified in the Program. Alternatively, ONC is considering (2) whether developers and offerors of certified health IT should remain subject to the information blocking provision for an appropriate period of time after leaving the Program.

AMIA Response: AMIA recommends a combined approach that requires any health IT developer (or offeror) that continues to store EHI that was previously stored in certified health IT to remain subject to the information blocking provision, as well as require formerly certified health IT developers (or offerors) to remain subject to the information blocking provision for an appropriate time after leaving the Program. We recommend that an "appropriate period of time" be defined as no less than two years following the developer's departure from the certification program. This would allow former customers -- individuals and entities -- the opportunity to access EHI.

Networks
ONC proposes a functional definition of "health information network" (HIN) that focuses on the role of these actors in the health information ecosystem. ONC proposes that an actor could be considered an HIN if it performs any or any combination of the following activities. First, the actor would be an HIN if it were to determine, oversee, administer, control, or substantially influence

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

policies or agreements that define the business, operational, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities. Second, an actor would be an HIN if it were to provide, manage, control, or substantially influence any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.

AMIA Response: AMIA recommends ONC revise the definition of HIN to reduce the universe of actors that could be considered an HIN. We suggest that decision-making authority over governance and substantial influence of a technology or service that facilitates interoperability be the defining attributes of an HIN. Given the expansive definition of EHI, we also suggest that a HIN should enable interoperability of EHI predominantly. If the actor predominantly traffics in data not considered EHI, then they should not be considered an HIN. By emphasizing these characteristics ONC can better ensure that ancillary actors are not subject to compliance.

Exchanges

ONC proposes to define a "health information exchange" (HIE) as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes.

AMIA Response: We suggest that ONC revisit and ultimately narrow the scope of the definitions for "Health Information Network" and "Health Information Exchange", which appear to be too broad to be implemented effectively without significant collateral damage. The unintended consequences of exposing an unforeseen number of individuals and entities to the HIN or HIE designation is likely to create an immense undue burden on many participants throughout the healthcare industry. This burden is only exacerbated by the burden of proof that lies upon those classified as HINs and HIEs to demonstrate compliance with all regulations when accused of blocking information. Likewise, as a result of the current definition, any app or service even remotely related to the process of providing EHI access could arguably be considered an HIN or HIE, and the potential litigation bonanza that may reasonably ensue as a result could be overwhelming and would be best avoided.

Electronic Health Information definition

ONC proposes to define EHI to mean: (i) electronic protected health information; and (ii) any other information that:

- is transmitted by or maintained in electronic media, as defined in 45 CFR § 160.103;
- identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

AMIA Response: AMIA supports this definition. However, we note that the application of this definition across a host of proposed provisions will likely be variable. For example, the capability of various health IT developers to "produce and electronically manage (or retain)" EHI will differ greatly across systems. AMIA recommends that ONC monitor stakeholder experiences with this definition closely.

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.201 Exception – Preventing harm

ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.

AMIA Response: AMIA specifically comments on the patient harm risk, "Determination by a licensed health care professional that the disclosure of EHI is reasonably likely to endanger life or physical safety." While we expect health care professionals to practice ethically, we note that this exception may allow too much latitude to health care professionals who do not want to share or disclose information for personal reasons. For example, our members are aware of medical professionals who have unfounded concerns that the mere disclosure of health data directly to patients without their professional interpretation will routinely cause harm, despite existing evidence to the contrary. ONC should be cognizant of this and we urge them to further monitor this potential issue.

§ 171.202 Exception – Promoting the privacy of electronic health information

ONC proposes to establish a sub-exception that recognizes that an actor will not be engaging in information blocking if an actor does not provide access, exchange, or use of EHI because a necessary precondition required by a privacy law has not been satisfied.

AMIA Response: Exceptions such as this one must not be used to justify failure to perform public health reporting.

We reiterate our recommendation that ONC take concerted steps to support a secondary market of entities to promote the vetting and endorsement of 3rd Party API Users and their apps. A trusted vetting process for 3rd Party API Users would provide reasonable assurance to API Data Providers over the security of connecting with apps developed by such API Users. A standardized process for evaluating 3rd Party API Users would make routine blocking of data sharing less defensible by either API Technology Suppliers or API Data Providers. And in instances where these stakeholders performed their own vetting, the process might be more stringent than necessary, specifically intended to block data sharing. A secondary market for app endorsements would ensure the same

level of security and privacy protections are expected across 3rd Party API Users and their apps, and such markets would markedly diminish the cost of vetting by entities who are required to ensure data privacy and security.

§ 171.203 Exception – Promoting the security of electronic health information

ONC proposes to establish an exception to the information blocking provision that would permit actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions.

AMIA Response: We reiterate our recommendation that ONC take concerted steps to support a secondary market of entities to promote the vetting and endorsement of 3rd Party API Users and their apps. A trusted vetting process for 3rd Party API Users would provide reasonable assurance to API Data Providers over the security of connecting with apps developed by such API Users. A standardized process for evaluating 3rd Party API Users would make routine blocking of data sharing less defensible by either API Technology Suppliers or API Data Providers. And in instances where these stakeholders performed their own vetting, the process might be more stringent than necessary, specifically intended to block data sharing. A secondary market for app endorsements would ensure the same level of security and privacy protections are expected across 3rd Party API Users and their apps, and such markets would markedly diminish the cost of vetting by entities who are required to ensure data privacy and security.

§ 171.205 Exception – Responding to requests that are infeasible

ONC proposes a two-step test that an actor would need to meet in order to demonstrate that a request was infeasible. The actor would need to show that complying with the particular request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances.

AMIA Response: AMIA recommends adding an additional consideration for data format and manner in which exchange is demanded. If the actor can provide data to the requestor in a required format that differs from what the requestor wants, then this should be considered sufficient. The successful negotiation around format and manner should be the primary goal. If the requestor is prepared to pay for the different format they desire, that should be a conversation unrelated to this rule because EHI is being made available in another format. The requestor can choose to negotiate with the actor or convert the data themselves.

ONC further proposes certain circumstances that would not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether complying with a request would have been infeasible. They propose that it would not be considered a burden if

providing the requested access, exchange, or use in the manner requested would have (1) facilitated competition with the actor; or (2) prevented the actor from charging a fee.

AMIA Response: AMIA suggests adding a third circumstance, in which the actor fails to comply with other parts of this rule and/or other regulations that facilitate better information sharing and interoperability. For example, if a provider does not update their certified health IT, they should not be able to claim an exception under this provision.

Finally, ONC proposes that in order qualify for this exception, the actor must have timely responded to all requests relating to access, exchange, and use of EHI, including but not limited to requests to establish connections and to provide interoperability elements.

AMIA Response: AMIA requests a clearer definition of "timely," as the timeliness of the response can be affected by several factors. For instance, it may depend on the volume of requests that an actor receives, or whether the actor has the sufficient technology (that is not required by statute) to respond to the request. Further, there may be instances in which the actor's technology vendor has not yet provided an upgrade that is needed to respond to a data request. Thus, exceptions should also be made when the timeliness of the response is outside the actor's control.

Request for information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange

ONC is considering whether it would should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement. Such an exception may support adoption of the Common Agreement and encourage other entities to participate in trusted exchange through HINs that enter into the Common Agreement.

AMIA Response: AMIA supports the idea behind the Common Agreement for Trusted Exchange and generally believes that compliance with such should be exempted from the information blocking statute. We indeed support a future rulemaking, as details of the updated Common Agreement for Trusted Exchange are still forthcoming.

Request for information on new exceptions

ONC welcomes comment on any potential new exceptions they should consider for future rulemaking.

AMIA Response: At this time AMIA does not recommend additional exceptions.

Section IX – Registries Request for Information

Health IT Solutions Aiding in Bidirectional Exchange with Registries

ONC is seeking information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives. They also welcome any other comments stakeholders may have on implementation of the registries provisions under § 4005 of the Cures Act.

ONC is seeking comment on use cases where an API using FHIR Release 4 might support improved exchange between a provider and a registry.

AMIA Response: AMIA supports efforts to make registries more interoperable with clinical systems and certified health IT. We recommend ONC include in their consideration of the landscape various disease registries, not just clinical data registries.

Section X – Patient Matching Request for Information

Opportunities to Improve Patient Matching

ONC seeks comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability.

AMIA Response: AMIA and the informatics community has been a supporter and collaborator with the Pew Charitable Trusts on a range of issues and activities related to patient matching. This work has led to the creation of an evidence-base that ONC and other HHS agencies should heed when thinking about policy options to improve matching rates. One key area we recommend ONC investigate is in setting a minimum accuracy level for successful matching. Making this an aspect of the RWT CMC might provide a way to improve performance over time. Another option is for ONC to validate existing matching methodology the way it validates conformance to standards in its Certification Program. For example, the value of primary and secondary identifiers in increasing the likelihood of a match is well documented. ONC could utilize this information when selecting mandatory data elements for sharing to ensure that the most useful primary and secondary identifiers were collected at the time of every patient encounter.

Below we offer some findings and subsequent recommendations resulting from the research that Pew, AMIA and the broader informatics community has generated.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

May 23, 2019

Standardize certain demographic data already collected

First, ONC should require the use of standards for certain demographic data elements—an approach long recommended by many other organizations, including Audacious Inquiry in a report contracted by ONC.[25]

In Pew-funded research published recently in the *Journal of the American Medical Informatics Association*, experts at Indiana University studied whether the standardization of different data elements improves patient matching rates.[26] Researchers attempted to match records in four databases, standardized the data in those databases, and then retried matching the records to determine whether that standardization yielded better results. The researchers culled tens of thousands of records from the Indiana Health Information Exchange; a county public health registry; Social Security's Death Master file; and a newborn screening laboratory. Each of these databases had already been reviewed to ensure that the record matches were accurate, which allowed researchers to understand the number of correct and inaccurate matches both before and after the standardization of select demographic data.

The research revealed that the standardization of address to the standard employed by USPS, which details the preferred abbreviations for street suffixes and states, for example, would improve match rates by approximately 3 percent. One technology developer indicated that this would help their system match an additional tens of thousands of records per day. Separately, standardizing last name to the standard used by the Council for Affordable Quality Healthcare—while showing limited utility on its own—would further improve match rates up to 8 percent if standardized along with address.

As mentioned earlier, ONC's recent regulations already propose embedding address in the USCDI, but the agency could further improve match rates by requiring use of the USPS standard. To further promote the use of this standard, ONC should also coordinate with USPS to ensure that health care organizations can use the postal service's online, API-based tool—or another easily accessible mechanism—to convert addresses to the USPS standard. There may also be scenarios—such as for military personnel stationed abroad—where the use of the USPS standard is not feasible. ONC could restrict use of the USPS standard to domestic, non-military addresses if challenges arise in the broader use of the standard.

Adopt additional data elements for patient matching

Second, ONC should advance the use of regularly collected demographic data elements for patient matching. ONC currently requires EHRs to make some demographic data—such as name, birth

[25] Genevieve Morris et al., "Patient Identification and Matching Final Report" (2014), https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.
[26] Shaun J Grannis et al., "Evaluating the effect of data standardization and validation on patient matching accuracy," Journal of the American Medical Informatics Association 26, no. 5 (May 2019): 447–456, https://doi.org/10.1093/jamia/ocy191

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

date, and sex—available, and proposes to add address and phone number to the USCDI. However, health records contain other demographic data routinely collected that aren't typically used or made available to match records.

For example, research published in 2017 showed that email addresses are already being captured in more than half of patient records.[27] The documentation of email is likely higher today, given the adoption of patient-facing tools, like portals, that often require emails to register.

ONC could improve match rates by identifying and including in the USCDI readily available data elements—such as email address, mother's maiden name, or insurance policy identification number—that health information technologies should use for matching.

Specific responses to questions in patient matching RFI

ONC seeks input on various approaches to address patient matching, minimum data requirements, and measures to assess performance of different solutions.

First, ONC requests input on the potential effect that data collection standards may have on the quality of health data that is captured and stored. ONC also requests input on solutions that may increase the likelihood of accurate data capture, including the implementation of technology that supports the verification and authentication of certain demographic data. As mentioned above, use of the USPS standard for address would improve match rates, and does not require the capture of information in this format given the availability of online tools to conduct the conversion.

Second, ONC solicits information on additional attributes that could aid patient matching, and new data that could be added to the USCDI or further constrained within it to support patient matching. As previously mentioned, ONC should examine additional data routinely collected in EHRs to also use for matching—such as email address, health insurance ID, mother's maiden name, and others.

Third, ONC seeks comments on potential solutions that involve patients in the capture, update and maintenance of their own demographic and health data. Pew collaborated with the RAND Corporation to examine patient involvement in record matching.[28] The research revealed two key ways for patients to support record matching. For one, patients could validate their demographic information by verifying their mobile phone number and other data. In addition, EHRs could support smartphone applications that use standard APIs to allow patients to update their demographic data. ONC and the technology industry could pilot these patient-led approaches.

[27] Adam Culbertson et al., "The Building Blocks of Interoperability: A Multisite Analysis of Patient Demographic Attributes Available for Matching," Applied Clinical Informatics 8, no. 2 (2017): 322-336, https://doi.org/10.4338/ACI-2016-11-RA-0196.
[28] Robert S. Rudin et al., "Defining and Evaluating Patient-Empowered Approaches to Improving Record Matching," RAND Corp., accessed Aug. 27, 2018, https://www.rand.org/pubs/research_reports/RR2275.html.

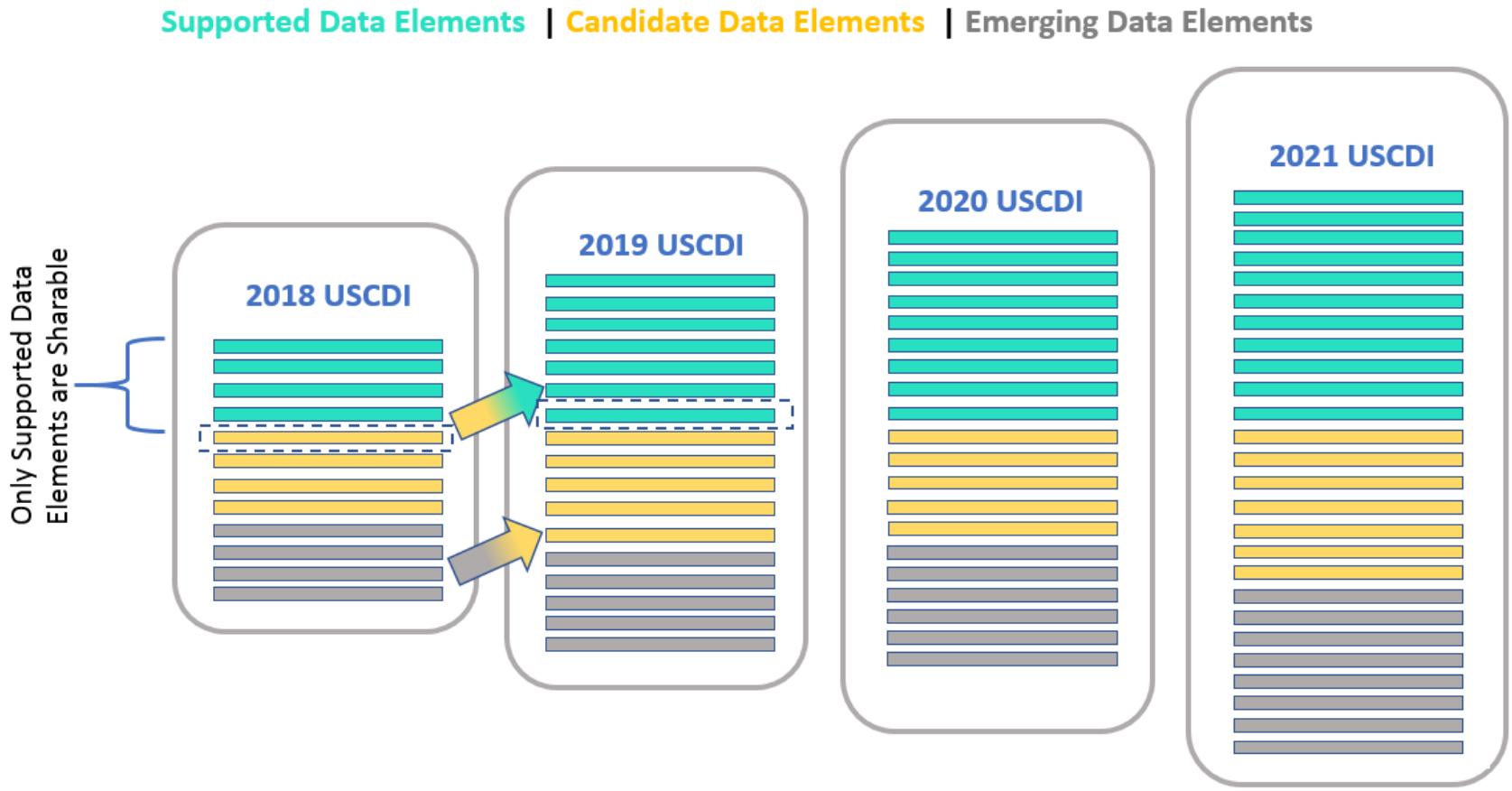
Fourth, ONC requests input on other innovative approaches to address patient matching. Pew research revealed a promising approach to patient matching that has not yet been widely used in health care: biometrics, such as fingerprint or facial recognition scans. In Pew-led focus groups on patient matching, patients overwhelmingly preferred the use of biometric over other options.[29] Patients in the focus groups indicated that they already use biometrics in other aspects of their lives—such as to unlock smartphones or board airplanes—and should be able to use the same approach for record matching. Pew intends to conduct further research on how the health care system could use biometrics to match records across different organizations while protecting patient privacy and the security of data.

Finally, ONC seeks input on performance measures and indicators that can be used to evaluate patient matching algorithms. Benchmarking different approaches would help shed a spotlight on matching deficiencies and the wide variation in quality across different algorithms. Technology developers could then use that information to improve their algorithms, and health care providers could adopt the most promising approaches. ONC should work with CMS to determine how to benchmark different matching approaches; this likely requires the identification of a large, real-world data set to test different algorithms. The use of real-world data, rather than synthetic data, is essential given that some innovative approaches—such as referential matching—use third-party databases to support their algorithms. ONC or CMS may be able to establish grantmaking authorities or other policies to obtain such a data set for benchmarking. This benchmarking could assess duplicate creation rates, the number of records correctly matched, and the frequency with which records are incorrectly merged.

*****

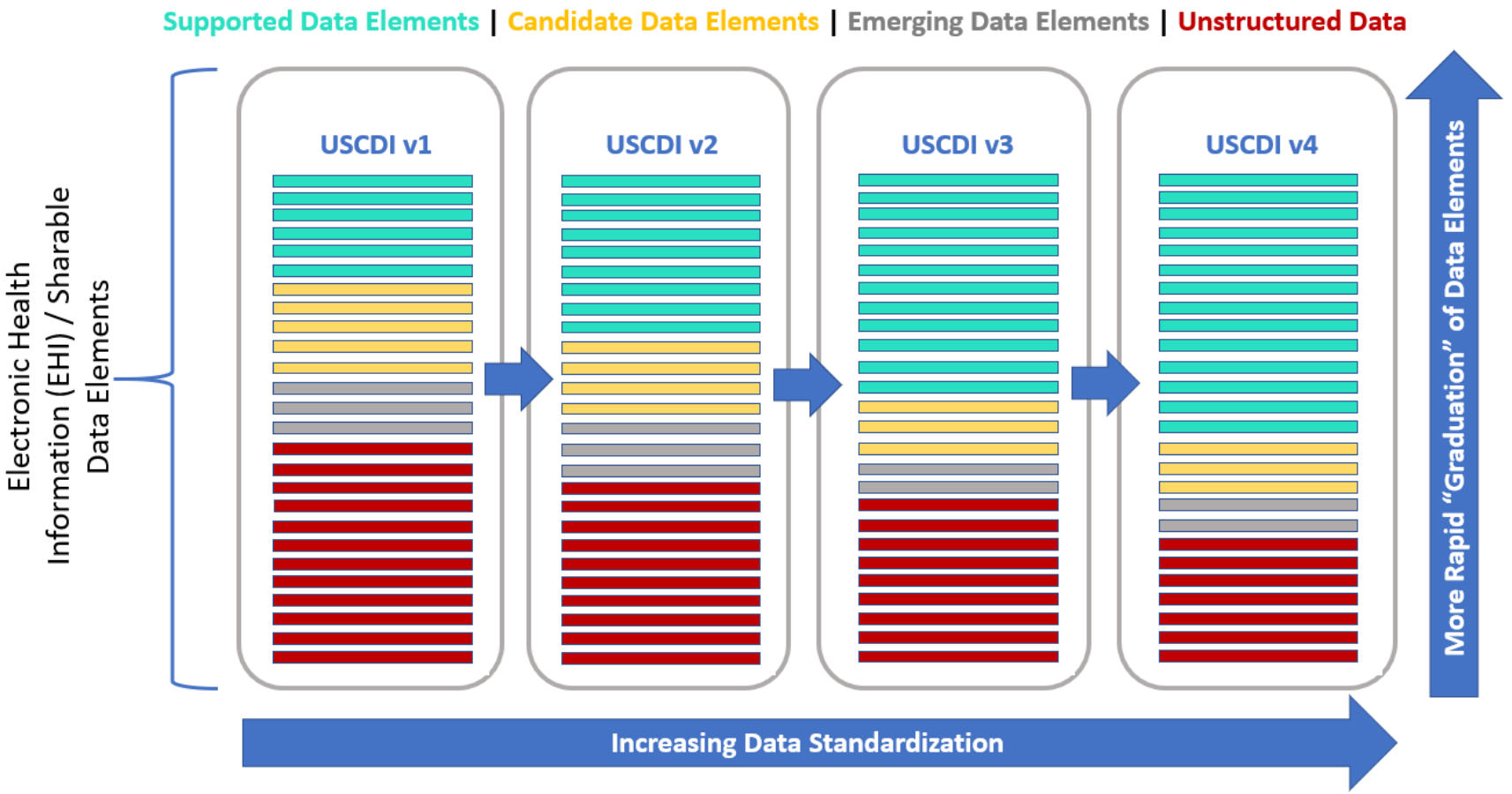
[29] Cite pew focus group brief

Appendix A: *Figure 1: ONC's Proposed USCDI Expansion Process (2018)*



This is the proposed data policy ONC developed in 2018. Grey "emerging data elements would graduate to candidate data elements and those candidate data elements would be included as part of the "supported" data elements over time. This approach literally requires data to be highly constrained and standardized before certified health IT would be expected to make EHI available for patient care, public health, and various kinds of research. AMIA recommends the approach outlined in Figure 2 below.

Figure 2: Share Now, Structure as Needed Approach using HL7 Unstructured Doc Template / FHIR Resources



The key differentiation between what ONC proposes in this NPRM and AMIA's recommendation is that certified health IT make "candidate," "emerging" and "unstructured" data elements available for access, exchange, and use as part of the USCDI v1 and in

subsequent versions of the USCDI, rather than only requiring certified health IT to make available "supported" data elements for routine access, exchange, and use. Including these additional kinds of data elements as part of the USCDI via this NPRM will require that certified health IT can support access, exchange, and use of these data from a technical perspective. The C-CDA "unstructured document" document-level template, the corresponding CCDA-on-FHIR Resource(s) or development of a "Get EverythingElse" API would ensure that ONC's policies are supported with technical specifications. This approach would also (1) enable users of data rather than health IT developers and standards development organizations to identify high-value EHI in need of standardization and (2) create market pressure for health IT to more quickly identify consistent standards to exchange emerging and candidate data elements.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

Appendix B: Sociotechnical Interoperability Stack