



33 W. Monroe, Suite 1700  
Chicago, IL 60603

Phone: 252-946-3546

Fax: 734-973-6996

E-mail: himssEHRA@himss.org

AllMeds, Inc.  
Allscripts Healthcare Solutions  
Amazing Charts  
Aprima Medical Software, Inc.  
Cerner Corporation  
CPSI  
CureMD Corporation  
Digital MD Systems  
eClinicalWorks  
e-MDs  
Epic  
GE Healthcare IT  
gloStream Inc.  
Greenway Medical  
Technologies  
Healthcare Management  
Systems, Inc.  
Healthland  
Lake Superior Software, Inc.  
MacPractice, Inc.  
McKesson Corporation  
MED3000  
MedcomSoft  
MEDHOST  
MediServe Information  
Systems  
MEDITECH  
NextTech Systems, Inc.  
NextGen Healthcare  
Information Systems  
Noteworthy Medical Systems  
Pulse Systems Incorporated  
QuadraMed Corporation  
Sage Software  
Sevocity, Division of  
Conceptual MindWorks Inc.  
Siemens  
Spring Medical Systems, Inc.  
SRS Software, LLC  
STI Computer Services  
Suncoast Solutions  
UNI/CARE Systems, Inc.  
Välant Medical Solutions  
VersaSuite  
Workflow.com LLC  
Xpress Technologies

September 23, 2011

Department of Health and Human Services  
Office of the National Coordinator for Health Information Technology  
Attention: Steven Posnack,  
Hubert H. Humphrey Building  
Suite 729D, 200 Independence Ave., S.W.  
Washington, DC 20201

Dear Mr. Posnack:

On behalf of the Electronic Health Record (EHR) Association we are pleased to provide these comments on the ANPRM on Metadata Standards to Support Nationwide Electronic Health Information Exchange. (RIN: 0991-AB78)

### General Comments

The Electronic Health Record (EHR) Association is pleased with the general direction of this Advanced Notice of Proposed Rule-Making (ANPRM) and its issuance by the Office of the National Coordinator for Health IT (ONC) as it starts to take steps towards realizing the vision described in the "*Report to the President: Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*" (the President's Council of Advisors on Science and Technology (PCAST) Report). We very much appreciate the fact the HIT Standards Committee and ONC have taken very seriously comments that the EHR Association and many others have made regarding the PCAST Report and its proposed approach to healthcare metadata. In particular, we recognize and are pleased that this approach focuses on documents and approaches to metadata based on existing standards. Our specific comments focus on the most appropriate metadata standards to use and the data elements that are appropriate for inclusion in metadata.

We would like to offer the following general observations, after which we provide specific answers to the questions the ANPRM raised.

- **Proceed to the next step with an open, transparent, and standards definition process**  
The EHR Association strongly supports taking an incremental approach toward enabling EHRs, health information exchange entities (HIEs), and health IT in general, to support enhanced query capabilities from defined and authorized providers and organizations, improving data liquidity. However, we believe that the process initiated by the HIT Standards Committee and followed by this ANPRM could be substantially enhanced by taking a broader approach to ensure that the 20 questions raised and the many other questions to be addressed and piloted will be resolved in the appropriate context. These steps must be taken before rules are issued that EHRs and other health IT are to be certified against.

ONC's Standards & Interoperability (S&I) Framework appears to be the ideal vehicle to manage the challenge at hand, from use case definition through pilot, as evidenced by the Direct Project that went through a similar process as well as other initiatives currently in process. We, therefore, would strongly encourage ONC to establish a metadata initiative that considers the feedback on this ANPRM and enables all industry stakeholders who have an interest in pursuing this challenge to openly participate. Moving to approaches with actual participation is in line with ONC's stated intent to fully engage all stakeholders through a transparent process that yields demonstrated value before it is mandated through the rule making process.

- **Clarify how the proposed metadata is supposed to be used in context of all components necessary to support the target use cases**

Although from the context of the ANPRM and the preceding discussions on the PCAST Report, the long-term intent is clear, it is not clear what the immediate intent of the proposed metadata standard is, particularly when considering the statements such as *"The HIT Policy Committee suggested that it would be practical to include this capability as part of the EHR certification requirements to support meaningful use Stage 2 under the Medicare and Medicaid EHR Incentive Programs."* Without clarity on all standards necessary to support the potential use cases and without having exercised those standards in at least one pilot with all other components and standards in place, it appears premature to consider requiring EHR systems to include this metadata in an upcoming meaningful use (MU) stage.

Additionally, exercising the proposed metadata in end-to-end pilots will help validate whether the metadata yields the desired data sets in terms of accurate patient matches and data set completeness.

- **Focus on loosely coupled, cross-provider use cases**

As the metadata are defined, we urge the project team to focus primarily on use cases that involve data exchange across loosely coupled provider organizations (large or small), or communities of organizations who do not have strong or consistent controls on patient identification methods, and lack consistent transport or clinical vocabulary. Metadata must be adequate to operate in this environment, with a long-term vision of cross-provider data liquidity. The EHR Association has proposed a framework of transport use cases and associated metadata requirements to address four of these transport use cases. Our detailed responses to the questions and recommendation to leverage the XDS metadata are based on this premise.

- **Extend the scope of use case examples**

The ANPRM uses a single use case example to clarify the suggested metadata. We believe that a reasonable range of intended uses needs to be defined before deciding upon the appropriate metadata set. We recognize that not all use cases can be described, but the following examples clarify the potential range that we believe must be satisfied.

- On one end of the spectrum is an example wherein dynamic queries can be performed on disparate systems (e.g., Query Health), across the Internet. Does the ANPRM envision its metadata supporting that scenario?
- At almost the opposite end of the spectrum is the simpler scenario given in the ANPRM of metadata-tagging a patient's electronic copy of his or her clinical summary.
- A third use case would be that of an emergency department assessing the current clinical state of a patient.

These use cases each have very different requirements and constraints. Other "in-between" scenarios may introduce additional considerations.

Our detailed answers will assume that a range of use cases, including the use cases described in the ANPRM for download and transmission, as well as the three described by the Power Team in slide 7 from their June 22<sup>nd</sup> presentation to the HIT Standards Committee (HITSC) are intended (patient pushes data from personal health record (PHR); simple query authorized by the patient; complex query based on policies). By considering a broader range of use cases, we introduce the critical perspective of a metadata framework that spans multiple use cases and avoids the risk of metadata fragmentation which would defeat the very purpose of metadata, particularly across diverse data sets. Of course, some use cases may only use a subset of the metadata defined by the framework.

We realize that the ANPRM rightfully does not try to specify the behavior of systems that query for metadata-tagged objects. We still caution that any aggregation, importing of data into EHRs, or clinical decisions based on the data must be done very carefully, unless performed from documents that offer a self-contained context.

- **Define metadata independent from the payload**

While the CDA Release 2.0 (CDA R2) header does contain the necessary data elements described in the ANPRM, and is appropriate for use along with summaries that are identified as relevant and simply need to be downloaded, it fails to support the broader use cases discussed by the HITSC. Indeed, if one is only looking to download patient summaries, the work of the S&I Framework CDA Consolidation Project and the Transfers of Care project recommend use of the same CDA R2 header standard to convey “implicitly” metadata in the summary document header, making “wrapping” potentially unnecessary. But this is a “payload dependent” approach that has several drawbacks:

- A number of data sets, including lab reports and immunizations, use HL7 Version 2 (HL7 V2) as the prevailing method to both create and exchange relevant data sets through EHRs and HIEs. It is unrealistic to assume that, in MU Stage 2 timelines, this data could move into CDA R2. We encourage the use of pilots to demonstrate the feasibility of CDA R2 for those purposes.
- Upon examining the broader perspective, it becomes apparent that the proposed metadata must transcend all data sets. There is, for example, extensive use of DICOM to support very rich data sets supporting imaging procedures. The CDA R2 standard is not appropriate to encapsulate these data sets. Awareness of such other data sets is helpful to minimize future changes of the proposed metadata set
- The CDA R2 header can serve as a definition for functional requirements for the metadata. In fact, this is what was done in the XDS metadata model, which considered functional requirements based on a wide range of standard exchange formats. This functional set of metadata is supported by numerous EHRs and HIEs. We believe that the XDS metadata model needs serious consideration. It has solid specification maturity, leverages HL7 CDA, HL7 V2, CCR, DICOM and many other standards for its functional definition.
- It has been implemented in production nationally, with significant piloting already performed in Beacon Communities, the NwHIN Exchange, and other HIE projects.
- And it is a design that has already been applied to several transport models, including XDS, Direct with XDM metadata, NwHIN Query/Retrieve, and others.

- **Separate metadata from privacy/security layers**

We are concerned with the potential propagation of privacy/security layers into the metadata, as well as metadata being so descriptive of the payload that a user can assert likely content that they are not supposed to see. Establishing an architecture through which one can apply privacy/security policies against the metadata without divulging to the requester the potential existence of certain data is a challenge. At a minimum, this approach requires clear separation of the metadata, sufficiently describing

the payload to return complete responses to a request for information, and the privacy/security policies that assert whether the requestor is qualified to know about and/or see the content. We, therefore, strongly suggest that any metadata being considered be carefully evaluated against this principle.

- **Carefully consider the patient identification conundrum**

When considering the metadata for patient identification, we recognize the challenge between having enough metadata to correctly identify and include data for the patient at hand from the various sources, while preserving the privacy of patients. We, therefore, urge the community to maintain realistic expectations about the accuracy of patient matches and data completeness.

### **Answers to Specific Questions**

**Question 1: Are there additional metadata elements within the patient identity category that we should consider including? If so, why and what purpose would the additional element(s) serve? Should any of the elements listed above be removed? If so, why?**

Please consider including the requirements for personal information as specified in section 1 of Version 2.0 HITSP C83 CDA Content Modules component, found on page 27. The optional elements for multiple birth indicator and multiple birth order are needed to distinguish between possibly unnamed newborns for patient matching. You should also require the vocabulary specified in Version 2.0 of the HITSP C80 Clinical Document and Message Terminology. This vocabulary ensures consistent representation of address information.

Note that not all metadata is required for every use case. This issue should be considered in establishing the requirements for metadata. The requirements for patient matching differ from those for download, transmission/registration, or query.

**Question 2: In cases where individuals lack address information, would it be appropriate to require that the current health care institution's address be used?**

No. The only time it is appropriate to use the institution address is when it is also the patient's residence.

**Question 3: How difficult would it be today to include a "display name" metadata element? Should a different approach be considered to accommodate the differences among cultural naming conventions?**

The use of a display name metadata element serves several purposes, as mentioned in the ANPRM. In one case, it is used as a "search name" in patient matching, to address issues in understanding cultural differences by personnel performing patient lookup. In other cases, it is used to appropriately display the name with the data.

The CDA Standard already includes a representation of the display name. This functionality is enabled because the order of the various name fields in the XML represents the display order, not a fixed order. If the patient's family name should be displayed first, it would appear first in the XML. It is certainly possible to include an "unparsed" name as one of the alternatives. Such a name would ideally be identified as being for that purpose, and HL7 provides the use XML attribute on the name for that purpose, as shown below:

```
<name use='SRCH'>John Q. Public</name>
```

Rather than adding metadata to support patient matching, we would simply note that an appropriate matching algorithm should be able to address search using names that have been entered in reverse order.

Addressing cultural issues, such as name order inversion, should be incorporated into patient matching best practices rather than including alternative name representations.

The approach found the most effective by NwHIN and IHE is to not mix the patient matching/identification into the metadata, but to leave it as a distinct workflow issue. For NwHIN where the community HIEs that are communicating are essentially “master person indices” systems (MPIs), the Cross-Community Patient Discovery (XCPD) is used. When centralized matching algorithms are implementable in a shared community MPI, patient identification (ID) cross-referencing (PIX) is appropriate. When patient ID is to be performed “manually”, Patient Demographics Query (PDQ) is used. Patient matching is not only about patient attributes. The patient matching Power Team reached a supporting conclusion that defining a set of matching attributes is a complex and unfinished challenge.

**Question 4: Are there additional metadata elements within the provenance category that we should consider including? If so, why and what purpose would the additional element(s) serve? Should any of the elements listed above be removed? If so, why?**

A CDA Document includes the document identifier, author, their specialty, and their affiliated organization. We would also recommend the type of service (found in the <code> element of the document) and date associated with the document (<effectiveTime> in <ClinicalDocument>). Also, the dates of service should be provided (<effectiveTime> in <serviceEvent> in <documentationOf> in the CDA Header). The dates of service, document creation date, and service performed are often used in search criteria to locate correct documentation (e.g., an EKG report for a specific patient). This capability is already supported in the XDS metadata.

Similar metadata also appears in the XDS family of standards (as it draws from CDA Release 2.0, DICOM, CCR, and other specifications).

The digital signatures are metadata that can be associated with documents, but should be supplied as a separate component, not as metadata.

Non-repudiation through digital-signature should be removed. It is very helpful standard functionality, but should not be incorporated into the metadata model. Digital-signatures are a layer that can be applied independent of the metadata. Such a layered approach that separates out the metadata needs from the technology used to specifically deliver non-repudiation is important for scalability and growth. More basically, not all uses of data require the very high level of assurance of non-repudiation that a digital-signature provides. Forcing digital-signatures as metadata will make the model very expensive. This is the same as your correct justification of separation of the confidentiality layer.

**Question 5: With respect to the provenance metadata elements for time stamp, actor, and actor’s affiliation, would it be more appropriate to require that those elements be expressed in XML syntax instead of relying on their inclusion in a digital certificate? For example, time stamp could express when the document to which the metadata pertain was created as opposed to when the content was digitally signed. Because this approach would decouple the provenance metadata from specific security architecture, would its advantages outweigh those of digital certificates?**

The CDA Standard already supports the time stamp, actor and actor’s affiliation (as well as additional metadata) in the CDA XML. Separating the digital signature from the downloaded summary is recommended above in our response to question four. Date of signature is less relevant than date of service and/or date of

creation. Signatures on a clinical document often occur days after the event occurred, and are not useful in clinical care.

We would suggest that metadata be defined functionally, rather than in a specific format, XML or otherwise. A functional definition enables broad application of this ANPRM to other exchange capabilities (e.g., public health reporting of immunizations, labs, and disease surveillance).

**Question 6: Are there additional metadata elements within the privacy category that we should consider including? If so, why and what purpose would the additional element(s) serve? Should any of the elements listed above be removed? If so, why**

The metadata model should describe the object (Document), not attempt to duplicate the privacy or security layers. Privacy and security policy and enforcement will leverage all of the metadata provided. Sometimes a privacy policy will request that a specific document be tightly controlled by referring to the document unique ID. Other times, a privacy policy will tightly control an episode of care, through the object's provenance and service time ranges. The privacy and security policies are part of the access control design layer. These do not need to be duplicated in a metadata model, but rather the metadata model needs to include sufficient metadata to enable access controls. The identified data type and sensitivity metadata elements are good examples.

Note that data type is useful for more than privacy management; it is useful for filtering data of interest at a fine-grained level (typically what CDA Document Type does). It is, however, not sufficient for filtering certain classes of data.

**Question 7: What experience, if any, do stakeholders have regarding policy pointers? If implemented, in what form and for what purpose have policy pointers been used (for instance, to point to state, regional, or organizational policies, or to capture in a central location a patient's preferences regarding the sharing of their health information)? Could helpful concepts be drawn from the Health Information Technology Standards Panel (HITSP) Transaction Package 30 (TP30) "Manage Consent Directives?"**

Having the data point at the policy level does not scale as objects age and policies are updated. Individual objects can be controlled through having a unique identifier for the object. This is a much more sustainable model. Note that the document already discusses using layers of functionality, such that a wrapping layer (security layer) can include the policies that would need to be met before that layer allows the data to be unwrapped. We strongly recommend separating the layers and keeping the metadata layer as attributes describing the object (document). We also strongly recommend the model defined in TP30 that separates privacy policies from access control and the objects they protect.

The use of policy pointers is not a mature technology and lacks standards that can be deployed in the healthcare environment. Specifically, the healthcare environment is made up of many independent authorities and multiple dimensions of controlling interests. The technologies available today to support policy pointers that emanate from the object require a single central authority with complete knowledge of all policies to be enforced. The most common of these technologies is digital rights management (DRM). DRM technology has also been shown to have significant weaknesses, and as such it has been abandoned by many of the industries that tried to use it. Of specific concern for healthcare use would be the failure modes that might make data completely unavailable during wide-spread disasters such as Hurricanes Katrina and Irene.

**Question 8: Is a policy pointer metadata element a concept that is mature enough to include as part of the metadata standards we are considering? More specifically, we request comment on issues related to the persistence of URLs that would point to privacy policies (i.e., what if the URL changes over time) and the**

**implication of changes in privacy policies over time (i.e., how would new policy available at the URL apply to data that was transmitted at an earlier date under an older policy that was available at the same URL)?**

See answers to questions six and seven above. Policy pointers are not appropriate at the object metadata layer. Policy is a different layer.

Having the data point at the policy level does not scale as objects age and policies are updated. Individual objects can be controlled through having a unique identifier for the object. This is a much more sustainable model. Note that the document already discusses using layers of functionality, such that a wrapping layer (security layer) can include the policies that would need to be met before that layer allows the data to be unwrapped. We strongly recommend separating the layers and keeping the metadata layer as attributes describing the object (document). We also strongly recommend the model defined in TP30 that separates privacy policies from access control and the objects they protect.

The metadata model should describe the object (Document), not attempt to duplicate the privacy or security layers. Privacy and security policy and enforcement will leverage all of the metadata provided. Sometimes a privacy policy will request that a specific document be tightly controlled by referring to the document unique ID. Other times, a privacy policy will tightly control an episode of care, through the object's provenance and service time ranges. The privacy and security policies are part of the access control design layer. These do not need to be duplicated in a metadata model, but rather the metadata model needs to include sufficient metadata to enable access controls. The identified data type and sensitivity metadata elements are good examples.

**Question 9: Assuming that a policy pointer metadata element pointed to one or more privacy policies, what standards would need to be in place for these policies to be computable?**

There is a lack of current standards for encoding privacy and security policy in an interoperable and computable form. In the mean time, we leverage vocabulary such as sensitivity (called confidentiality code by IHE XDS and CDA), and regional vocabulary for consent types (BPPC). The enforcement is thus done at multiple places along the exchange including at the data custodian, infrastructure, and data consumer. This type of federated security architecture is robust and can be enhanced incrementally.

**Question 10: With respect to the privacy category and content metadata related to “data type,” the HIT Standards Committee recommended the use of LOINC codes to provide additional fine-grained coverage. Would another code or value set be more appropriate? If so, why?**

If we correctly understand the HITSC recommendation to use LOINC, we assume that it is related to the LOINC “document types”. We believe that may be a reasonable starting point. However, there is much overlap and duplication among these LOINC document type codes. A USA Realm management of the codes used for metadata “data type” would be a good mechanism to build. This was a positive output from the HIT Standards Panel, but needs to be further refined and managed. The actual codes used will evolve over time, and there needs to be consideration of this evolution. However, the full LOINC vocabulary may be too fine-grained and present a privacy violation. We need to be careful to balance the needs to discover/describe with the needs to protect. IHE XDS proposed a triplet approach in addition to document type (fine-grained is useful for applying access control). It uses three different codes, each with a “small value set”, which when combined ensure a more flexible use of the metadata:

- Object-document class code. This is intended to be a coarse-grained (10-100 max values) data element that distinguish general classes of objects/documents (e.g., report, summary, care plans, patient input, etc.)

- Specialty code. This is intended to be a coarse-grained (10-100 max values) data element that distinguish the specialty that produced the object-document (e.g., cardiology, family medicine, neurology, etc.)
- Healthcare facility code. This is intended to be a coarse-grained (10-100 max values) data element that distinguishes the general type of organizational setting during which the documented act occurred (e.g., doctor's office, clinic, hospital, personal health record, etc.)

**Question 11: The HIT Standards Committee recommended developing and using coded values for sensitivity to indicate that the tagged data may require special handling per established policy. It suggested that a possible starter set could be based on expanded version of the HL7 ConfidentialityByInfoType value set and include: "substance abuse; mental health; reproductive health; sexually transmitted disease; HIV/AIDS; genetic information; violence; and other." During this discussion, several members of the HIT Standards Committee raised concerns that a recipient of a summary care record tagged according to these sensitivity values could make direct inferences about the data to which the metadata pertain. Consistent with this concern, HL7 indicates in its documentation that for health information in transit, implementers should avoid using the ConfidentialityByInfoType value set. HL7 also indicates that utilizing another value set, the ConfidentialityByAccessKind value set which describes privacy policies at a higher level, requires careful consideration prior to use due to the fact that some items in the code set were not appropriate to use with actual patient data. In addition, the HIT Standards Committee recommended against adopting an approach that would tag privacy policies directly to the data elements. What kind of starter value set would be most useful for a sensitivity metadata element to indicate? How should those values be referenced? Should the value set be small and general, or larger and specific, or some other combination? Does a widely used/commonly agreed to value set already exist for sensitivity that we should considering using?**

The data classification for sensitivity is an important metadata value. It needs to be sufficiently varied to allow for proper segmentation, but also sufficiently high-level so as not to expose the specific sensitive topic that privacy would protect. This is not to say that metadata be restricted to non-sensitive values, but rather that limiting the risk should be considered.

The ConfidentialityByInfoType value set should not be used. It is not intended for exposure outside a controlled environment. This value set was defined in HL7 for purposes of policy encoding -- for example to identify in a privacy policy (Consent Directive) the specific types of information that the specified patient considers most sensitive. As such, the value set is not intended to be used on objects as metadata values, but rather used by the EHR to determine which objects need to be identified as "R", restricted.

The metadata values in the ConfidentialityByAccessKind are defined for interoperability and should be used for that purpose. These values are defined to be used as metadata values in an object's confidentialityCode attribute. The HL7 Security and CBCC committees are in the process of correcting the HL7 documentation, by clarifying the proper uses of each value set and by differentiating the purpose of the confidentialityCode. This effort will also update the Security and Privacy Domain Analysis Model to help illustrate how the confidentialityCode along with other metadata attributes are used by privacy policy and access control enforcement. Included in this new model are metadata values such as author, time, unique identifiers, authentication, user-role, etc.

**Question 12: In its recommendations on privacy metadata, the HIT Standards Committee concluded that it was not viable to include the policy applicable to each TDE because policy changes over time. Is this the appropriate approach? Are there circumstances in which it would be appropriate to include privacy preferences or policy with each data tagged element? If so, under what circumstances? What is the appropriate way to indicate that exchanged information may not be re-disclosed without obtaining additional patient permission? Are there existing standards to communicate this limitation?**

We agree with the HITSC, privacy preferences should not be included in metadata. The privacy policy functionality should remain separate from the object metadata. These are separate domains and should function as layers for scalability. The standards are being developed to support more advanced privacy policy and obligations. These standards developments are not specific to healthcare, but are influenced by healthcare needs. These standards are implemented as an independent layer from the content they protect.

Considering that data and context changes, both data and policies can change rapidly as the provider and patient progress through the care process. For example, patient preferences tend to be negotiated at time of service/critical issue and thus can change rapidly. Age of data may be relevant such that the data set can be ignored or included.

**Question 13: With respect to the first use case identified by the HIT Policy Committee for when metadata should be assigned (i.e., a patient obtaining their summary care record from a health care provider), how difficult would it be for EHR technology developers to include this capability in EHR technology according to the standards discussed above in order to support meaningful use Stage 2?**

Providers using certified EHR technology to exchange patient summaries, using the HITSP C32 Version 2.5 Summary Documents using the CCD, already support the functional requirements of this ANPRM, although not necessarily all of the specifics proposed in the ANPRM.

The implementation challenge of metadata is dependent on the binding to transports and specific to their environment of use. The use of XDS metadata in the context of XCA is already in practice as part of the NwHIN-Exchange. The use of XDS metadata in the context of XDM (e-mail media) is already in practice as part of the Direct Project. The use of XDS metadata is common between these two nationwide projects, and is the basis of the common (NwHIN Document Submission) XDR protocol between these two projects.

Finally, depending on the specific metadata approach and associated transports ultimately chosen by ONC, there could be significant implications for providers and EHR vendors in terms of adding support for specific metadata elements, especially regarding privacy and provenance. We therefore recommend that, depending on the final approach chosen, CMS and ONC may wish to focus on meaningful use Stage 3 as opposed to Stage 2 in terms of addition of metadata certification requirements.

**Question 14: Assuming we were to require that EHR technology be capable of meeting the first use case identified by the HIT Policy Committee, how much more difficult would it be to design EHR technology to assign metadata in other electronic exchange scenarios in order to support meaningful use Stage 2? Please identify any difficulties and the specific electronic exchange scenario(s).**

Several EHR systems have demonstrated the ability to use CDA Release 2.0 to exchange laboratory results and immunization information. However, most laboratories are not yet prepared to exchange information in the CDA Release 2.0 format, nor is public health yet ready to receive it in that format in most locations. Some state HIEs (e.g., Vermont) are considering using CDA Release 2.0 to deliver Immunization data from public health to the EHR. We would encourage use of CDA Release 2.0 in future pilots, but would not recommend this as the *only* way to exchange information for MU Stage 2.

**Question 15: Building on Question 14, and looking more long term, how would the extension of metadata standards to other forms of electronic health information exchange affect ongoing messaging and transactions? Are there other potential uses cases (e.g., exchanging information for treatment by a health care provider, for research, or public health) for metadata that we should be considering? Would the set of metadata currently under consideration support these different use cases or would we need to consider other metadata elements?**

Different use cases will generate different requirements and constraints, so there is no assurance that metadata selected for a few initial simple use cases will be adequate for future use cases that have not yet been analyzed. For example, the ambitious PCAST assemblage of a virtual patient record from diverse sources poses much greater challenges in all three categories of metadata than the simpler use case of giving an electronic copy to the patient.

Yes, we believe there are other use cases that should be considered. Exchanges for clinical trials and disease registries, in addition to transitions of care, patient engagement, and population health, are worth considering. We are not saying that complete analysis of all future use cases is required before starting with proofs-of-concept, but we believe design must be based on much more than one limited example. Metadata should be designed for the long-term. Failure to ensure sufficient breadth would require extensions or redesign to metadata. By definition, missing metadata cannot be created in many cases – that is, even if it is technically feasible, no one is often willing to assume this responsibility. Redesign of metadata creates major discontinuity and is very costly to deploy.

**Question 16: Are there other metadata categories besides the three (patient identity, provenance, and privacy) we considered above that should be included? If so, please identify the metadata elements that would be within the category or categories, your rationale for including them, and the syntax that should be used to represent the metadata element(s).**

Metadata categories are better described as uses of metadata. This is to say, different needs (such as use cases) will drive a set of metadata. Each metadata attribute tends to have many uses. A good example of this is the use of protecting privacy, which leverages almost all metadata values.

The table below lists the XDS metadata elements, and identifies extensions with new categories and more effective structuring of the dataType category:

- Other categories such as:
  - o Data encoding (mimeType) and data structure (e.g., CDA R2 with implementation specifications)
  - o Service time (start and end) associated with the data object content
  - o Language used, when displayable document
  - o Data management (hash and size)
  
- Increase structure for certain categories in order to enable structured searches:
  - o dataType with a fine-grained coded value (e.g., LOINC Document Type)
  - o A three axis" dataType" so that deterministic clinical searches are supported:
    - ClassCode (the high-level class of object)
    - PracticeSettingCode (the high-level clinical specialty produced the class of object)
    - HealthcareFacilityTypeCode (the class of source institution as known by the patient)

<b>XDS Metadata Attribute</b>	Required(R), if available(R2), Optional (O)	Related to ANPRM concepts
<b>uniqueId (document)</b>	<b>R</b>	TDE ID
author	R2	
authorInstitution	R2	Provenance Affiliation
authorPerson	R2	Provenance Actor
authorRole	R2	
authorSpecialty	R2	
<b>patientId</b>	<b>R</b>	
sourcePatientId	R	Patient ID – ID
sourcePatientInfo	O	Patient ID -- name, gender, DOB, address
<b>contentType</b>	<b>R</b>	Content Data Type (encoding)
<b>formatCode</b>	<b>R</b>	Content Data Type (e.g. CDA R2+ CCD+C32 summary)
<b>classCode</b>	<b>R</b>	Content Data Type (high-level class: e.g. summary, report, care plan, patient input, etc.)
<b>healthcareFacilityTypeCode</b>	<b>R</b>	Content Data Type (sources: hospital, clinic, office, etc.)
<b>practiceSettingCode</b>	<b>R</b>	Content Data Type (Specialty)
<b>typeCode</b>	<b>R</b>	Content Data Type (fine grained LOINC document type)
serviceStartTime	R2	
serviceStopTime	R2	
<b>languageCode</b>	<b>R</b>	
<b>confidentialityCode</b>	<b>R</b>	Content Sensitivity
<b>creationTime</b>	<b>R</b>	Provenance timestamp
<b>size</b>	<b>R</b>	Size of data object
<b>hash</b>	<b>R</b>	

**Question 17: In addition to the metadata standards and data elements we are considering, what other implementation factors or contexts should be considered as we think about implementation specifications for these metadata standards?**

The S&I Framework, with its inclusion of reference implementation and pilots, would provide a good way to discover these additional factors. It is not possible to anticipate every issue in advance without actually having to implement and test a standard or specification.

There are still some functional requirements missing from the ANPRM. While CDA Release 2.0 supports the metadata described in the ANPRM, it is not required by the specification. CDA can support multiple names and name parts, but it does not require a name to be provided in a clinical document (and there are some use cases for CDA where this capability might be needed). Some vocabulary is also required to ensure that information exchanged is commonly understood.

The current MU requirements for standards for patient summaries offer a path to a solution. It specifies the

*HITSP C32 Version 2.5 Summary Documents* using CCD as the implementation guide for using CDA for accessing patient summaries. That document in turn utilizes the *HITSP C83 CDA Content Modules (version 2.0)* and *HITSP C80 Clinical Document and Message Terminology (version 2.0)*. It suggests that the patient identifier, name, address, telephone number, gender, date of birth, and marital status be required in the personal information communicated in the *CDA Header* (see *section 2.2.2.1 of Version 2.0* of this document, found on page 27). The *HITSP C154 Data Dictionary* describes the various uses for this data (see *section 2.1.2.1 of version 1.0* of that document, found on pages 10-11).

The *HITSP C80 Clinical Document and Message Terminology* component addresses vocabulary applicable to patient metadata, as well as other metadata used for provenance. *Section 2.2.1 General Information Value Sets* specifies the vocabulary that would be appropriate for patient metadata. This could be found starting on page 26 of version 2.0 of that document. This fills another important gap in the metadata specification by ensuring agreement on a common vocabulary.

Provenance metadata also needs vocabulary, and can be found in the *Document Metadata* section, starting at the bottom of Page 80 of that specification. Note that much of this vocabulary has already been adopted in NWHIN exchange specifications, and is used in both CONNECT and Direct Project implementations. Sections of note are *2.2.3.15.1 Document Class*, *2.2.3.15.2 Document Type*, *2.2.3.1.15.3 Healthcare Facility Type*, *2.2.3.15.4 Clinical Specialty*, and *2.2.3.15.6 Author Role*.

Digital signature would be difficult to implement since the target audience is often not known in advance.

**Question 18: Besides the HL7 CDA R2 header, are there other standards that we should consider that can provide an equivalent level of syntax and specificity? If so, do these alternative standards offer any benefits with regard to intellectual property and licensing issues?**

Yes, the XDS metadata should be considered as a framework for more extensive use cases. It has been defined for many other use cases. Despite some perceptions that it is complex, its number of required data elements is close to the number proposed in the ANPRM, and its required metadata elements are closely aligned with the provenance, patient identity, and privacy, with just a few variations. Its use would also leverage work already done in previous ONC-sponsored work – NWHIN Exchange, CONNECT, and the Direct Project (where XDR metadata was simplified and mapped to SMTP). The following table shows the subset of XDS document entry attributes that are **required** and/or related to the ANPRM’s proposed metadata.

<b>XDS Metadata Attribute</b>	Required(R), if available(R2), Optional (O)	Related to ANPRM concepts ( <i>may not be exact or 1:1</i> )
<b>uniqueId (document)</b>	<b>R</b>	TDE ID
author	R2	
authorInstitution	R2	Provenance Affiliation
authorPerson	R2	Provenance Actor
authorRole	R2	
authorSpecialty	R2	
<b>patientId</b>	<b>R</b>	
sourcePatientId	R	Patient ID – ID
sourcePatientInfo	O	Patient ID -- name, gender, DOB, address

<b>contentType</b>	R	Content Data Type (encoding)
<b>formatCode</b>	R	Content Data Type (e.g. C32 summary)
<b>classCode</b>	R	Content Data Type (high-level class: e.g. summary, report, care plan, patient input, etc.)
<b>healthcareFacilityTypeCode</b>	R	Content Data Type (sources: hospital, clinic, office, etc.)
<b>practiceSettingCode</b>	R	Content Data Type (Specialty)
<b>typeCode</b>	R	Content Data Type (fine grained LOINC document type)
serviceStartTime	R2	
serviceStopTime	R2	
<b>languageCode</b>	R	
<b>confidentialityCode</b>	R	Content Sensitivity
<b>creationTime</b>	R	Provenance timestamp
<b>size</b>	R	Size of data object
<b>hash</b>	R	

XDS metadata encoding leverages OASIS ebRegistry service XML structure as the overall framework, while complex and healthcare-specific data elements rely on HL7 V2 encoding made semantically compatible with HL7 CDA data elements semantics. There no licensing issue beyond those of HL7 V2. So, it is compatible in most respects with the ANPRM recommendation for CDA R2, but is more inclusive of considerations for other documents in addition to CDA, and was based on analysis of many transport scenarios, whereas CDA R2 header by itself was more focused on a CDA document and less on the transport “envelope.”

**Question 19: The HL7 CDA R2 header contains additional “structural” XML elements that help organize the header and enable it to be processed by a computer. Presently, we are considering leveraging the HL7 CDA R2 header insofar as the syntax requirement it expresses relate to a metadata element we are considering. Should we consider including as a proposed requirement the additional structures to create a valid HL7 CDA R2 header?**

No, we do not think the metadata should be equal to a full CDA R2 header, though it is valid to derive metadata elements from a CDA header if it exists. A set of metadata, even associated to a CDA document, will never match the specification of the CDA header (the present ANPRM proposal attempts several non-compatible changes).

A CDA header has been designed with a different purpose than health information exchange metadata. The CDA header is designed for the purposes of a clinical document header; in other words, “inward looking metadata” related to the information contained in the body of the document.

The metadata for information exchange is *not* an object or document header. It is “outward looking metadata”, focused on the sharing and access to the object-document to which it is associated. It may have been created by another system, at a different time than when the object document was created. Of course, when the “HIE metadata” is created, some information contained in the object/document may be used (including from the header if the object is a CDA document), but not necessarily.

**Question 20: Executive Order (EO) 13563 entitled “Improving Regulation and Regulatory Review” directs agencies “to the extent feasible, [to] specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt;” (EO 13563, Section 1(b)(4)). Besides the current standards we are considering, are there performance-oriented standards related to metadata that we should consider?**

We agree with the intent of EO 13563. Taken literally, it implies that this ANPRM should not have proposed a specific standard (no matter how valid), but should have just stated a performance objective of demonstrating that certain EHR data sets can be exposed using industry standard methods, and let the industry figure out which standards to use within a reasonable timeframe. We recommend starting small, and increasing complexity over time through pilots. Per EO 13563, ONC or any agency should “propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs” – in this case the benefits of information liquidity, etc. The cost/benefit comparison is a reason to lean towards metadata standards (such as XDS metadata used in Direct, NwHIN, and HIEs) that are already widely supported by many vendors and deployed for the intended purpose, rather than standards that have not been deployed for that purpose, or rather than proposing a new/modified standard such as the ANPRM does. The only missing element for enabling wide and consistent use of the XDS metadata is the establishment of a USA Realm management of the codes used for XDS metadata to further refine and manage the value sets defined by HITSP. These codes will evolve over time, with pilot projects and careful consideration of this evolution process.

Sincerely,

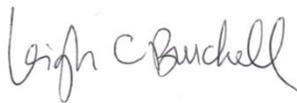


Carl Dvorak  
Chair, EHR Association  
Epic



Charles Jarvis  
Vice Chair, EHR Association  
NextGen Healthcare

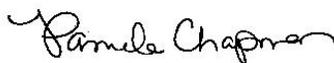
**HIMSS EHR Association Executive Committee**



Leigh C. Burchell  
Allscripts Healthcare Solutions



Rick W. Reeves  
CPSI



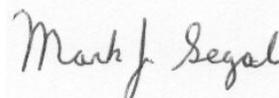
Pamela Chapman  
e-MDs



Jason Colquitt  
Greenway Medical Technologies



Michele McGlynn  
Siemens



Mark Segal  
GE Healthcare IT

cc: Steve Lieber, HIMSS  
Gail Arnett, HIMSS  
EHR Association Executive Committee

#### About HIMSS EHR Association

*HIMSS EHR Association is a trade association of Electronic Health Record (EHR) companies that join together to lead the health information technology industry in the accelerated adoption of EHRs in hospital and ambulatory care settings in the US. Representing a substantial portion of the installed EHR systems in the US, the association provides a forum for the EHR community to speak with a unified voice relative to standards development, the EHR certification process, interoperability, performance and quality measures, and other EHR issues as they become subject to increasing government, insurance and provider driven initiatives and requests. Membership is open to HIMSS corporate members with legally formed companies designing, developing and marketing their own commercially available EHRs with installations in the US. The association, comprised of more than 40 member companies, is a partner of the Healthcare Information and Management Systems Society (HIMSS) and operates as an organizational unit within HIMSS. For more information, visit <http://www.himsehra.org>.*