



# Health Level Seven® International

*Unlocking the Power of Health Information*

*An ANSI accredited standards developer*

September 23, 2011

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

**RIN 0991- AB78**

## **Metadata Standards to Support Nationwide Electronic Health Information Exchange Advance Notice of Proposed Rulemaking (ANPRM)**

Dear Dr. Mostashari:

HL7 welcomes the opportunity to comment on the Metadata Standards to Support Nationwide Electronic Health Information Exchange ANPRM recently published by ONC. We are honored by ONC's selection of the CDA Release 2 header for the metadata to be used to describe patient information in Health Information Exchange. While we appreciate the selection of CDA Release 2.0 for the purposes specified in the ANPRM, we have several concerns.

### **GENERAL COMMENTS**

The process for arriving at the appropriate metadata set to attach to a variety of data sets that may be of interest to the use cases envisioned is challenging. From our experience developing standards. It is critically important to consider a reasonable range of use cases and anticipated data sets before establishing an initial set of requirements (metadata in this case) for an initial subset of use cases and data sets.

While documents provide a reasonable and industry accepted starting point, metadata beyond documents such as images and other data sets that may not (yet) have been reported should be considered. Health Information Exchange encompasses exchange of summary documents, laboratory reports, immunization and population health data, and imaging reports and data.

Additionally, the full flow from query/search to response must be understood and preferably piloted before such metadata set can be finalized as a standard, thus before it can be referenced in a regulation that systems must incorporate.

In the broader case of exchange, we believe that the metadata captured by the CDA Release 2.0 header is certainly functionally suited for many of these purposes. However, the CDA Header XML is only one of several mechanisms through which metadata can be obtained for exchanges. Laboratory reports, immunizations and other population health data are currently exchanged in several HIEs in the US using HL7 Version 2.0. Imaging data is exchanged in other cases using DICOM.

The HL7 EHR Work Group is developing a functional definition for metadata based on CDA Release 2.0 and other mechanisms used for exchange today. We anticipate release of this document in early Q1 of 2012. We understand that regulatory timelines may not allow ONC to wait for such a model to be developed. Therefore, we would hope that ONC would modify the ANPRM to define metadata functionally, and allow for adoption of the HIE Metadata Functional Model in the final rule. An HIE

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA  
Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

Metadata functional model developed by HL7 can subsequently be used to help guide the industry in implementation of the necessary functional requirements.

We would encourage participation in the development of this specification. Interested parties need not be members of HL7 in order to contribute or vote on the specifications. We would offer that HL7 can work closely with the S&I Framework initiative, and other related organizations such as IHE to further develop this functional profile. We would also welcome participation from organizations piloting exchange metadata to participate in this process to validate the efficacy of the proposed guidance before it is incorporated into regulations.

**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?**

In addition to the ONC identified Patient identification metadata, additional data items may be needed to identify newborns, including indicators of multiple birth, and position in birth order. Newborns may not have sufficient demographics (e.g., names may not have been selected by the parents yet). This metadata should be present in exchanges when it is relevant, but should not be required in all cases.

**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?**

It is inappropriate to use the address of the institution where a patient receives care unless the patient is also a resident at that institution.

**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 case for display name as described in the ANPRM is to identify the patient. In the cases described by the ANPRM, download by a patient from an HIE/EHR/PHR or Portal of data already in the system, and transfer to a patient's PHR, this step has already occurred. Transport protocols such as those found in the NwHIN and in the DIRECT specifications can ensure that the patient is already identified. In the case of NwHIN, these protocols have a common patient identifier. In the case of DIRECT, pushing the content to the patient's PHR requires knowledge of the patient's PHR DIRECT address, which effectively identifies the patient.

The utility in search provided by the "display name" is not necessary for those cases. In wider exchange use cases, we note that most Health Information Exchanges also deal with identification of the patient in a separate step before initiating exchange. In the few cases where this is not performed (e.g., point to point push via DIRECT), a "display name" capability might be useful. However, we note that in the case where these are received by an automated system that, the use of a master patient index to identify the patient would be likely, and that these systems are already optimized to deal with the issues of culturally appropriate name orders. In other cases, the use of the metadata in a manual search might be aided by a "display name". However, here we note that a better aid would simply be to encourage the use of automated name matching.

We note that existing standards used in Health Information Exchange provide several different mechanisms to include display name. HL7 Version 3 and CDA R2 provide a display name capability, as the name components are already in display order. There is also the capability in CDA Release 2 to provide a search string for the display name, as shown in the example below:

```
<name use='SRCH'>Henry Levin the 7th</name>
```

In HL7 Version 2, the Patient Identifier segment offers another approach, which is to allow for a code to specify the order in which name parts are assembled using the XPN data type. Multiple name representations are also permitted in that standard, which allows a name to be used in a search context to be specified along with the usual representation divided into given and family name components.

As display name is used in only a small number of use cases, but does have value, it might be included as an optional piece of metadata for Health Information Exchanges, but should not be required in all cases.

**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?**

Metadata regarding the date of signature is less relevant in clinical care than the dates during which the individual received the care. Documents created during emergency care or discharge are often signed after the patient has left the institution where they received care. The dates of service are much more useful to enable information to be found with regard to the health event requiring care. The type of service provided is also important. This enables providers to identify relevant documentation based upon the particular service received, e.g., emergency department encounter, chest X-ray, et cetera. Healthcare information can be associated with multiple digital signatures for many different purposes. We believe that these should be separated from the document because the use cases for access to content and verification of the signature of the content are different.

**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 a specific security architecture, would its advantages outweigh those of digital certificates?**

The metadata described above is already functionally supported in CDA Release 2.0 and other information standards. As recommended in question 4, we believe the date of service is much more valuable than date of signature.

We recommend separation of the digital signature from the metadata as it:

- A) Requires greater technical infrastructure to validate digital signatures (e.g., certificate access and deployment),
- B) Has different and more limited purposes than the clinical content of the information being exchanged,
- C) Need not be present depending upon the policies of the HIE, EHR and/or portal in use.

**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?**

There are multiple levels of metadata in Health Information Exchange transactions, and that metadata varies by use case. Some metadata applies to the information being retrieved and doesn't change over the lifetime of the data being exchanged. Other metadata, such as purpose of use, requestor identity and credentials, and applicable consents are applicable to, and only associated with the specific transaction or request for which the data is returned, and can change from transaction to transaction.

In the use case described by the ANPRM, and in broader use cases, we would recommend that the regulation only specify the metadata that is static with respect to the information being retrieved. This includes the "sensitivity classification" of the information contained within the patient summary, as this remains static. But it does not include metadata supporting further layers involved within the security, privacy and access control layers supporting information access policies. Rather than have the metadata point to the policies, there should be separate pointers linking appropriate policies to the data being protected. This allows for dynamic control of data as privacy policies, consents, et cetera, change over time. For example, the recent NPRM allowing patients access to laboratory data illustrates the issue. Had laboratory data been marked with metadata that said it was protected under a policy addressing CLIA requirements, all of that data would have to be remarked with new metadata to support new policies after that regulation became final.

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA  
Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

In use cases beyond those identified by the ANPRM, additional data may be needed for particular kinds of transactions (e.g., queries for data to facilitate determination of disability benefits, treatment, payment, operations). However, we note that metadata is appropriate based on the kind of transaction being performed, rather than being a static property of the data being exchanged.

**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?"**

The HITSP TP30 transaction package has been used in several exchanges that are live in several operational health information exchanges. This includes exchanges in Massachusetts and Vermont. The State of Connecticut has recently proposed policies<sup>1</sup> supporting this technology for their Health Information Exchange. Numerous vendors have both demonstrated support at IHE Connectathons (see testing results<sup>2</sup>) and deployed it (see vendor integration statements<sup>3</sup>).

We note that policy pointers are from policies to the data that they protect in these cases, rather than from the data protected to the policies applicable. Metadata associated with the information being retrieved is simply classified according to the risk of exposure to patients (e.g., normal, restricted, very restricted). HL7 strongly recommends the model defined in TP30 that separates Privacy Policies and Access Controls from the objects they protect. Individual objects can be classified according to the risk of exposure to patients (e.g., normal, restricted, very restricted). These values can be used by the access control layer to facilitate determination of appropriate risk-based control policies, and where necessary, the inclusion of purpose of use in the exchange. We note that in the use cases described by the ANPRM, the purpose of use is fixed (patient access), but in broader use cases, it could be more dynamic (e.g., disability benefits determination, treatment, payment, operations, et cetera). Separation of layers ensures that the security layer can include the policies that would need to be met before the access control layer allows data to even be unwrapped.

The separation of the Privacy/Security layers from the data and metadata layers is not inconsistent with the use of privacy pointers, and as the standards and implementation of these standards recognize the needs of Healthcare they can be leveraged. This evolution is enabled by the separation of the layers.

**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 answer to 6 and 7. Policy pointers should not be stored in the object metadata layer due to the dynamic nature of both policies and consents. Policy is a different layer in information exchange. Having the data point at the policy does not scale as objects age and policies are updated. Individual objects can be controlled through having a unique identifier for the object to which a policy is applied. This is a much more sustainable model over time. We strongly recommend the model defined in TP30 that separates Privacy Policies from Access Control from the objects they protect.

The metadata model should be describing the object (Document), not trying to duplicate the Privacy or Security layers. Privacy and Security policy will leverage all of the metadata provided. Sometimes a privacy policy will request that a specific document be tightly controlled, it will do this by referring to the

<sup>1</sup> Available on the web at

[http://www.ct.gov/dph/lib/dph/state\\_health\\_planning/hit/policies\\_and\\_procedures/hite-ct\\_access\\_control\\_policy\\_09.04.2011.pdf](http://www.ct.gov/dph/lib/dph/state_health_planning/hit/policies_and_procedures/hite-ct_access_control_policy_09.04.2011.pdf)

<sup>2</sup> Available on the web at <http://connectathon->

[results.ihe.net/view\\_result.php?rows=company&columns=actor&title=integration\\_profile&integration\\_profile=BP](http://results.ihe.net/view_result.php?rows=company&columns=actor&title=integration_profile&integration_profile=BP)

<sup>3</sup> Same page as above. Integration statements are available by clicking on the folders on that page.

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA

Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

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?**

See previous responses to questions 6-8. As previously noted, metadata should be captured about the information being stored that is static over the lifetime of that information, rather than that which can be dynamically updated. Many of the policies are specific to the kinds of transaction and use, and to the receiver of the information in the transaction, et cetera, rather than being properties of the data being stored.

Work in this space is actively being pursued by HL7 and other related organizations such as OASIS (e.g. XSPA). This work is leveraging the lessons learned through more stepping stone standards such as IHE BPPC, and the more advanced HL7 CDA Consent Template DSTU<sup>4</sup>.

**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 granularity. Would another code or value set be more appropriate? If so, why?**

If we understand properly the HIT Standards Committee 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 LOINC document type codes. HITSP provided a US Realm value set from LOINC for use by Health Information Exchanges, but it needs to be further refined and managed. The actual codes used will evolve over time, and there needs to be consideration of this evolution.

The full LOINC vocabulary may be too fine-grained and presents risks to data with respect to privacy violations. 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 with each 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 elements that distinguish data based on the type of service that generated it (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 data being exchanged (e.g. cardiology, family medicine, neurology, etc.)
- HealthCare Facility code. This is intended to be a coarse grained (10-100 max values) data elements that distinguish general type of organizational setting during which the documented act occurred (e.g. doctor 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**

---

<sup>4</sup> Available on the web at

[http://www.hl7.org/documentcenter/public/standards/dstu/V3DAM\\_MR\\_CPCD\\_DSTU\\_R2\\_2010APR.pdf](http://www.hl7.org/documentcenter/public/standards/dstu/V3DAM_MR_CPCD_DSTU_R2_2010APR.pdf)

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA

Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

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 to not 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, but not for transmission in patient identifiable documentation. For example, in a privacy policy (Consent Directive) the specific types of information that the specified patient considers most sensitive could be encoded using such a value set, but these values would not be applied to patient identifiable documents. 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 Restricted.

The metadata values in the ConfidentialityByAccessKind are defined for interoperability and should be used for the purposes described by this ANPRM. These values are defined to be used as metadata values in an object's confidentialityCode attribute.

The HL7 Security and CBCC Work Groups are in the process of updating the HL7 documentation, by clarifying the proper uses of each value set and by documenting the differentiation of the purpose of 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 HIT Standards Committee, privacy preferences should not be included in Metadata. The Privacy Policy functionality must remain separate from the metadata for the information being exchanged. These are separate domains and function as layers for scalability. 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.

**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?

For the use case of transfer of data to a PHR or download from an HIE, EHR's have demonstrated the capability to capture demographics that include gender and date of birth in Meaningful Use Stage 1. EHRs routinely store the patient's name within the record. However, we note that the "display name" is often not stored separately. The process of capturing the patient's name is normally done during patient

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA  
Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

registration. The use of a “display name” may be useful at registration time in order to match the patient to existing records in the master patient index, but would not be used subsequently. This is often a function provided in a patient registration system or practice management system separate from the EHR. The “display name”, if present in the metadata, should not be a required field that is supplied by a complete EHR, as the name parts are usually resolved in the correct order before they are communicated to it.

Systems which are routinely used for newborn care commonly capture information about multiple birth and birth order, but systems which are not used in this context do not. We would therefore suggest that metadata about multiple birth and birth order be supported but not required in the metadata.

**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).**

Most systems routinely separate the security, privacy and access control layers from the EHR technology. The requirement to support digital signatures is challenging, especially to small providers due to the requirements to manage and obtain access to certificates used in exchanged data.

Other electronic exchange scenarios, e.g., immunization reporting, electronic laboratory reporting, or disease surveillance, use different standards required under meaningful use Stage 1. To require these systems to supply a CDA Header would be very challenging, as the mechanism for exchange does not readily support wrapping the HL7 Version 2 content inside a CDA Header. We note that functionally, these exchanges already support the metadata requirements, simply in a different format. We would suggest that the metadata be defined functionally. HL7 is engaged in development of a functional profile in support of this ANPRM, and would encourage the participation of others in its development. We anticipate balloting of this specification in December of 2011.

**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?**

While this ANPRM focuses on patient access to information, the other use cases described are for different purposes. The extension of metadata into use cases such as those described would need to accommodate purpose of use in the transactions used for those use cases.

**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).**

Beyond those metadata elements we have already suggested in our response, we do not have any additional metadata elements to consider at this time. We believe that description of the syntax used to support metadata elements is premature, given the number of different ways that health information is exchanged. While we would welcome the goal of convergence to a single standard (e.g., such as CDA Release 2.0), we do not believe that it is feasible in the current time frames.

Metadata elements we have suggested include:

- Multiple Birth Indicator and Birth Order
- Dates of Service
- Type of Service
- Confidentiality Code (Normal, Restricted, Very Restricted)

3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA  
Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: [hq@HL7.org](mailto:hq@HL7.org) • Website: [www.HL7.org](http://www.HL7.org)

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?

We believe that ONC should consider existing Health Information Exchange implementations and pilots to discover the appropriate contexts for specification of metadata standards.

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?

Focus on syntax is premature, as functional requirements for metadata exchange should be delivered first. A number of standards provide a similar level of syntax and functionality, including HL7 Version 2, Version 3, CDA, and the IHE Cross Enterprise Sharing family of profiles.

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?

While CDA Release 2.0 does contain a great deal of structural metadata, we recognize that not every piece of information exchange used for clinical care is delivered in the CDA format. For example, the recent NPRM harmonizing the CLIA and HIPAA regulations will now allow patients greater access to their laboratory reports. This material is often transmitted to many HIE in production using HL7 Version 2. Because CDA Release 2, like all HL7 Version 3 standards is based on the existing models in HL7 Version 2, those messages have many of the same functional capabilities.

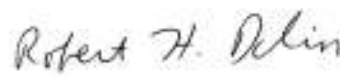
Question 20: Executive Order (EO) 13563 entitled “Improving Regulation and Regulatory Review” directs agencies “to the extent feasible, [to] specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt;” (EO 13563, Section 1(b)(4)). Besides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

As previously stated, HL7 is developing a performance-oriented functional profile directly related to this ANPRM, and is expecting to ballot this document in December of 2011. We would encourage the use of functional definitions rather than syntactic definitions for the purposes described in this ANPRM, and would encourage participation of interested parties in the development of this resource.

Sincerely,



Charles Jaffe, MD, PhD  
CEO, Health Level Seven International



Robert H. Dolin, MD  
Chair, HL7 International