



Health Level Seven® International

Unlocking the Power of Health Information

An ANSI accredited standards developer

March 15, 2010

Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Attention: RIN 0991–AB58
Hubert H. Humphrey Building
Suite 729D
200 Independence Ave., SW
Washington, DC 20201

RE: Interim Final Rule: Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology

The Interim Final Rule (IFR) on health information technology (HIT) standards marks a positive step forward in the nation’s efforts to improve health care by putting modern HIT tools at the fingertips of medical professionals and consumers alike.

We applaud the US Department of Health and Human Services for drafting an initial set of standards that, in general, support the goals of “Meaningful Use” of health IT and allow for sufficient flexibility in a heterogeneous marketplace. This was a very challenging and novel undertaking, and the result is an important contribution to the potential of information technology to improve the quality and efficiency of health care.

Health Level Seven members strongly support moving forward on the development of interoperable healthcare IT, including the Nationwide Health Information Network, which includes the maximum participation by all clinician categories across all healthcare delivery settings. A critical first step is ensuring that eligible professionals and hospitals can achieve adoption and meaningful use of qualified, certified, EHR technology. Clearly, the goal of such adoption and use is increased access, quality, and efficiency. Thus, while the Medicaid and Medicare incentive programs should emphasize improvement in these areas as an end result, we should also be mindful that adoption of the right technologies must precede its meaningful use.

Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organization (SDO) dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. HL7’s 2,300+ members represent approximately 500 organizations who represent more than 90% of the information systems vendors serving healthcare in the US.

The comments below propose reasonable and important modifications to the Interim Final Rule and represent input from Working Groups within HL7.

In General

Comment:

The published standards for EHR certification do not address standards for basic EHR functionality, but are targeted to specific functionality in certain areas such as content exchange, vocabulary, and transport for HIE. There was an EHR certification body (CCHIT) promulgating standards prior to the HITECH Act. Detailed certification criteria were developed for both inpatient and ambulatory EHRs. HHS made a conscious determination to not adopt previously recognized certification criteria developed in 2006 in their interim final rule. We believe that the new HHS standards leave a large gap between the previous standards, and the limited areas where standards are now proposed.

Two of the stated goals of EHR adoption are: “Improving quality, safety, efficiency, and reducing health disparities...Ensure adequate privacy and security protections for personal health information”. The regulations define standards for data integrity for data exchange activities, but not for underlying source system which produces the data that will be exchanged.

We are concerned that the standards will not adequately support the stated goals of health care improvement and adequate privacy and security because of missing foundational requirements for EHR systems and modules. Meaningful use will not be effectively achieved if the underlying data is not accurate, complete, and of unassailable integrity. The government has not identified any standards for underlying EHR systems or modules that support system and data integrity, authentication standards, and non-repudiation.

HL7 recommends:

Identify standard(s) for the underlying EHR functionality, such as those previously defined by CCHIT or those found in the HL7 Electronic Health Record System (EHR-S) Functional Model (FM). The fact that the first version of this EHR-S FM was created at the behest of HHS for just this purpose should be considered seriously. The standards should be detailed enough to support the goals of the federal government in the areas of user identification, access and validation; validity of data and data support structures, and supportive of fraud detection through a foundation that allows for validation and authentication of all system activities.

Comment:

HL7 notes that the existing Executive Order (EO) 13410 “Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs,” mandates that covered agencies (i.e. any Federal agency administering or supporting a Federal health care program) must support HITSP standards, as recognized by the Secretary. Although the IFR preamble states “[d]ue to our approach of aligning adopted certification criteria with the proposed definition of meaningful use Stage 1, the Secretary has decided not to adopt previously recognized certification criteria developed in 2006 as any of the certification criteria in this interim final rule” the IFR does not cover federal agencies.

We are concerned that there are several key standards which are required by the IFR to demonstrate meaningful use Stage 1 that potentially overlap and are inconsistent with the HITSP standards already recognized[i] and required as a result of EO 13410.

In sum, we understand that the intent of the IFR is to align “the initial set of standards, implementation specifications, and certification criteria adopted by this rule to focus on the 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 • Website: www.HL7.org

capabilities that Certified EHR Technology must be able to provide in order to support the achievement of the proposed criteria for meaningful use Stage 1 by eligible professionals and eligible hospitals under the Medicare and Medicaid EHR Incentive Programs.”[4] However, there are potential discrepancies between the requirements of the IFR and the more prescriptive requirements that exist under EO 13410. These contradictions could pose a dilemma for providers who are currently meeting the requirements recognized under EO13410, but would also like to demonstrate meaningful use for purposes of the CMS Electronic Health Records Medicare and Medicaid Incentive Programs.

HL7 recommends:

HL7 recommends that, prior to finalizing the set of standards in this interim final rule, ONC conduct a thorough review of the entire set of standards required under EO 13410 and provide clarification and assurances that any overlapping standards or inconsistencies do not undermine the stated intent and requirements of the IFR...

Comment:

The regulations lack specificity, particularly regarding implementation guidance. HL7 understands that the regulations were meant to be generic and areas requiring more specificity were to be addressed through a clearly defined and transparent process, which does not go through the Rule Making process. However some have heard that implementation guidance will not be mandatory. Our experience with previous regulatory efforts in a related area (HIPAA) tells us that there is a need for mandatory implementation guidance to reduce ambiguity and cost of implementation.

HL7 recommends:

HL7 recommends that the final rule clearly describe in detail how the implementation guidance necessary for true interoperability of health information will be mandated.

Detailed Recommendations

§170.202 Transport standards for exchanging electronic health information.

Adopts transport standard SOAP Version 1.2 and as an alternative, a stateless, client-server, cacheable communications protocol that adheres to the principles of REST for the exchange of content listed in Section 170205.

Comment:

Incorporation of HL7 2.3.1 in 170.205 and 2.5.1 by reference in 170.299 adds the normative transport mechanism, Minimum Lower Layer Protocol (MLLP), for those standards' messages. This is distinct from SOAP and RESTful choices.

We also note that the goals of interoperability and broad adoption of health information exchange mechanisms across diverse authorized stakeholders would be well served by employing existing administrative networks such as those utilized to convey NCPDP and X12 to support transactions required for Meaningful Use where efficient and compliant with applicable security and privacy safeguards.

HL7 recommends:

HL7 recommends removing section 170.202 altogether. Alternatively, MLLP could be included in the standard, although the security and interoperability functionality require significant pre-coordination, to avoid invalidating legacy HIT system investment.

§170.205 Content exchange and vocabulary standards for exchanging electronic health information.

(a) Patient summary record.

(1) Adopts content exchange standards HL7 CDA Release 2, Level 2 CCD and as an alternative ASTM E2369 CCR for the purposes of electronically exchanging a patient summary record or creating an electronic copy of a patient summary record.

Comment:

CDA CCD is an excellent choice for a standard. The CCD definition harmonizes HL7 CDA and ASTM E2369 in an XML structure that is intended for communication, persistence, and reuse beyond the initial intended purpose of the document to be shared. It is the work product of a joint agreement of HL7 and ASTM for those purposes. We appreciate your recognition of this harmonization effort.

However, ASTM E2369 is not an appropriate alternative. The CDA CCD specification already incorporates ASTM E2369. In addition, ASTM E2369 correctly excludes itself from being used for exchanging data, as a message, or as being a persistent copy of a patient summary record. Section 1.3.1 of the standard states “The CCR XML is not a persistent document, and it is not a messaging standard.” It also defines persistent document, in section 3.1.41, as “a document that remains as a document within a data structure or file system once it has been used for its original intended use.”

In addition:

- CCR lacks standard vocabulary data elements making selection and reporting of disclosure incidents difficult, especially for care episodes among providers who use semantically different vocabularies for data labels and values.
- CCR does not have appropriate elements needed to communicate relevant information such as 'hospital course.'
- CCR also creates ambiguities over certain types of information by removing important context. For example, CCR describes only one 'medication list' with no way to clarify which medication list is being referenced. In the hospital setting there are at least 4 different medication lists (the preadmission medications, the currently active medication orders in the hospital, the medications that have been administered in the hospital, and the medications to continue after discharge).
- CCR cannot provide input into clinical decision support beyond “for display purposes only” due to the lack of common definition of how data is structured.

For these reasons, we believe that CCR cannot realistically be used to convey information from an inpatient setting and is limited in its applicability to progress towards clinical decision support based on understandable, structured data.

HL7 recommends:

Adopt the HL7 CDA as the minimum standard version for exchange of documents and the HL7 CCD Implementation Guide as the starting point for the Patient Care Summary. Remove the redundant alternative ASTM E2369.

Comment:

Note that CDA is the standard and CCD is an implementation guide that constrains CDA by requiring section level templates. CCD is but one of a family of implementation guides against the CDA. (See recommendation regarding reference to these standards under section 170.299.)

The references to levels in the definition of the CCD standard are confusing. A Level 1 CCD does not exist. Under the CDA definitions, a Level 2 CCD would be one that contains section-level templates, and a Level 3 CCD would be one that uses some entry-level templates (although it might not use all entry level templates it is permitted to). The structured documents workgroup commonly uses the term level 1 to mean "the CDA specification with an unconstrained body", and allows a level 1 CDA to have a constrained header (as is the case in several recent implementation guides and draft standards for trial use).

Some confusion may have occurred because of confusion between how CCD represents information and how previous implementation guides using CDA for the Claims Attachment NRPM were structured. The Claims Attachment Implementation Guides used a different description of interoperable levels, the human decision variant and the computer decision variant. The computer decision variant corresponds most closely to CDA Level 3. The human decision variant was further subdivided into two subtypes, using a <nonXMLBody> (similar to CDA Level 1) and a <structuredBody> similar to CDA Level 2).

HL7 recommends:

HL7 recommends removal of references to levels. If that is not possible, then describe them as previously described in the claims attachment NPRM.

Comment:

Problem List, medication list, medication allergy list, procedures, vital signs and lab orders and results are commonly referred to as Sections of the CDA or CCD document, not "fields". These sections may contain narrative text using the CDA XML format for text, and need not contain level 3 entries. However, in order to use the specified clinical vocabularies found in the interim final rule in an interoperable fashion, the codes from these selected vocabularies must appear in level 3 entries. Units of measure are components of structured entries (CDA level 3) in these sections.

HL7 recommends:

HL7 supports specified clinical vocabularies; CDA level 3 is required to properly communicate that. Otherwise it is text level 2 (unstructured).

Comment:

Discharge summaries are clinical documents with their own sections with required content (specified by accreditation organizations), not sections of other clinical documents.

HL7 recommends:

HL7 recommends that the CCD not be used for this purpose. There are other HL7 document types (implementation guides or constraints) for CDA such as discharge summary that are better suited to this need.

§170.205 Content exchange and vocabulary standards for exchanging electronic health information.**(a) Patient summary record.**

(2) Adopts vocabulary standards ICD-9-CM and as an alternative SNOMED-CT for conditions and ICD-9 and as an alternative HCPCS for procedures included in a patient summary record.

Comment:

ICD-9-CM codes are used in billing systems for reporting diagnosis, problems, and conditions to payers. Providers are required to send ICD-9-CM to payers when they bill for services meant to eliminate a diagnosis. In HIPAA X12 837, the ICD-9-CM is accompanied by a flag that indicates whether this code is being used for that purpose. Neither the CCR nor the CCD support such a flag, so there is no way to know whether ICD-9-CM codes used in either report format accurately conveys the patient's problems. If EHR technology must be certified as supporting use of ICD-9-CM, then providers may populate the summary records, quality measures, discharge instructions, and referrals with billing ICD codes resulting in false positives about the patient's condition if these codes are used for analysis or decision support.

ICD billing codes have too little clinical detail to be used as the basis for clinical decision support, one of the major advances that HIT will bring to help improve the quality of healthcare. Since the CCD is more clinically focused, ICDs are not an appropriate vocabulary, and their use will impact the ability to implement CCD.

HL7 recommends:

HL7 recommends the use of SNOMED with CCD.

§170.205 Content exchange and vocabulary standards for exchanging electronic health information.**(a) Patient summary record.****Comment:**

In the preamble, HHS states that “[w]e believe that enabling the use of UCUM and SNOMED CT® for this exchange in the future would lead to improved interoperability.”¹ HL7 notes that

¹ Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule, Federal Register /Vol. 75, No. 8 /Wednesday, January 13, 2010 /Rules and Regulations 2033

conformance to the CCD standard requires the use of UCUM for results observation values where the result value is expressed as a physical quantity. If HHS stipulates the use of CCD and does not also require the use of UCUM as a standard in Stage 1, then EHR technology may be certified against a non-conformant CCD implementation.²

HL7 recommends:

HL7 recommends that HHS require use of the UCUM standard in Meaningful Use Stage 1.

(d) Electronically exchange administrative transactions.

Adopts content exchange standards and associated implementation specifications for administrative transactions.

Comment:

HL7 has several problems with this approach. First of all, most Medicaid and Medicare providers are already conducting these transactions using their practice management software or a third party. Practice management software is not typically included in, sold with, or maintained as part of an EHR system. Also, eligibility and claims are not part of the HL7 EHR Functional Model Direct Care functions and thus we don't consider this core to the EHR technology needed to support and improve healthcare outcomes.

HL7 recommends:

HL7 recommends that the X12 transactions be removed from the IFR totally so that providers can concentrate their efforts on implementing EHR technology required to improve health outcomes.

Comment:

CAQH CORE Phase 1 rules are intended for the ASC X12 4010A1 standard, however, the Interim Final Rule appears to require these operating rules for ASC X12 5010 transactions. If the administrative transactions are to remain in the final rule, HL7 recommends correcting this so that CAQH CORE operating rules are required only in conjunction with ASC X12 version 4010A1, or alternatively, by removing the CAQH CORE implementation guidance from the Final Rule entirely and advancing this requirement outside the regulation.

HL7 recommends:

HL7 recommends that ONC coordinate with CMS on the immediate release of the Final Rule for Claim Attachments following the Notice of Proposed Rulemaking (45 CFR Part 162 HIPAA Administrative Simplification: Standards for Electronic Health Care Claims Attachments; Proposed Rule, FR Doc. E9-31216) for inclusion in Stage 1 or Stage 2 standards for qualified EHR technology.

² HL7 Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD) at page 38: “CONF-244 **Observation / value** can be any datatype. Where **Observation / value** is a physical quantity, the unit of measure **SHALL** be expressed using a valid Unified Code for Units of Measure (UCUM) expression”; and at page 56: “CONF-417 Where **Observation / value** is a physical quantity, the unit of measure **SHALL** be expressed using a valid Unified Code for Units of Measure (UCUM) expression.”

Comment:

HL7 supports development of HL7 Financial Management message and service standards for the Medicaid Information Technology Architecture. For this reason, HL7 is concerned that a strict interpretation of the HIPAA-mandated ASC X12N 270/271 – Health Care Eligibility Benefit Inquiry and Response, Version 4010 (004010X092) and Addenda to Health Care Eligibility Benefit Inquiry and Response (004010X092A1) as well as ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, Version 5010 (ASC X12N/005010X279) requirements for the use of the AAA Segment to report errors in identifying the patient in the 271 Response transaction likely conflicts with established policies and procedures regarding phishing that many Medicaid agencies have established.

This will impede progress on the development of HL7 Financial Management Medicaid Beneficiary Registry messages and service specifications. The specific concern is that a strict interpretation of the 270/271 AAA specification requires the payer to inform the requestor exactly which fields in the search request caused the mismatch with the payer data providing an opportunity for phishing.

Further investigation is required to determine the impact of such a strict interpretation of the HIPAA-mandated transaction set and the use the AAA segment may have on privacy and other policies of Medicaid agencies and other governmental bodies. Although we support the inclusion of CORE Phase I, in Stage 1 of meaningful use, the requirement of the 4010 and 5010 HIPAA-mandated 270/271 eligibility transactions to use the AAA segment in a 271 eligibility response requires further investigation.

HL7 recommends:

HL7 recommends that ONC clarify the inherent conflict so that its work on MITA standards can progress.

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.**Comment:**

The Medicare and Medicaid Programs; Electronic Health Record Incentive Program NPRM preamble table 2 states that the Care Goal for EPs/Hospitals is to “Ensure privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law.”

But the objective is silent about either compliance with applicable law. This leaves the NPRM provision on this measure, and the certification criteria in the IFR open to interpretation about what is actually required. The NPRM only requires that the provider conduct a HIPAA Security Assessment, and is silent about compliance all the other laws that the provider needs the EHR technology to support.

HL7 Recommends:

We recommend that the Medicare and Medicaid Incentive Program final rule reflect the intent of the Care Goal to “Ensure privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law” [in table2]

in the objective by: Amending Table 2 Objectives for EPs and Hospitals to read “Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities *in compliance with applicable law*” and amending provision (17)(i) to read: “Objective. Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities *in compliance with applicable law.*” [1994 Federal Register / Vol. 75, No. 8 / Wednesday, January 13, 2010 / Proposed Rules]

In addition, we recommend that the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology final rule reflect the intent of the Incentive Program Care Goal to “Ensure privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law” by amending the title of § 170.210 to read: “Standards for health information technology to protect electronic health information created, maintained, and exchanged *in compliance with applicable law.*”

Comment:

We note that the qualifier “patient authorized” that is included in the preamble is dropped from the wording of the regulation

HL7 recommends:

We recommend that this qualifier be included in the actual regulation in order for this certification criterion to enable providers to meet multiple jurisdictional laws relating to patient authorizations and consents.

Comment:

Although we support HHS’ decision not to name a specific access control technology at this time because access control technologies are evolving and there is no need to stifle innovation in this area, we are concerned that the IFR did not include at least a functional standard for access control in 170.210 to reflect the access control certification criteria at §170.302 (o).³ In addition, while the regulatory language does include an access control certification criteria, we are concerned that the NPRM stipulation^[2] that providers must only meet certification criteria for which a standard has been named may preclude any actual certification of access control capabilities.

HL7 recommends:

HL7 recommends that ONC adopt a functional standard for access control and for the electronic capture, management, and conveyance of patient consents and authorizations afforded under

³ §170.302 (o) General certification criteria for Complete EHRs or EHR Modules. Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.

^[2] Federal Register / Vol. 75, No. 8 / Wednesday, January 13, 2010 / Proposed Rules, page 1846 "In a related proposed rule, the Department will propose the development of a certification program for health IT. Specifically, we have sought to ensure that the definition of meaningful use of certified EHR technology does not require EPs and eligible hospitals to perform functionalities for which standards have not been recognized or established" 3300 Washtenaw Ave., Suite 227 • Ann Arbor, MI 48104-4261 • USA 9 | Page
Office: +1 (734) 677-7777 • Fax: +1 (734) 677-6622 • E-mail: hq@HL7.org • Website: www.HL7.org

HIPAA, 42 CFR Part 2, state laws, Medicaid program confidentiality requirements^[1], and ARRA. These functional specifications should enable computable enforcement of patient authorizations and consents by means of access control technologies that use standardized role, permission, and purpose of use vocabularies in order to meet the criterion: “Capability to exchange key clinical information among providers of care and *patient authorized entities* electronically.”

Finally, we recommend that ONC include a comprehensive definition of access control to include the notion of object/operation pairs or “permissions” that can be assigned to roles and users under conditions, with obligations, and for specified purposes of use.

Comment:

We note that the qualifier “patient authorized” that is included in the preamble has been dropped from the wording of the regulation.

HL7 recommends:

We strongly urge that this qualifier be included in the actual regulation in order for this certification criterion to enable providers to meet multiple jurisdictional laws relating to patient authorizations and consents.

Comment:

We support HHS’ Cross-Enterprise Authentication and Authorization functional standard. However, naming SAML as an example is not helpful because interoperable use of SAML requires domain specific implementation guides such as the [OASIS Cross Enterprise Security and Privacy \(XSPA\) of Security Assertion Markup Language \(SAML\) for Healthcare SAML](#).

HL7 recommends:

“Table 2B-Adopted Privacy and Security Standards Row 5 should be modified to read:

“5...Cross-Enterprise Authentication and Authorization...Use of cross-enterprise secure transactions that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g., IHE Cross Enterprise User Assertion (XUA), and OASIS Cross Enterprise Security and Privacy (XSPA) of Security Assertion Markup Language (SAML) for Healthcare SAML

§170.210(e) and 170.302(v) Certification Criteria and Standard of Accounting for Disclosures

The standard specified in Table 2B stipulates a functional requirement that a recorded disclosure for treatment, payment or healthcare operations must include: the date, time, patient ID, user ID, and a description of the disclosure.

[1] [1] [The State Medicaid Manual Chapter 11 Section 11281.1 D. Safeguards](#)--You must insure that appropriate safeguards are in place to protect the confidentiality of eligibility information. The use or disclosure of this information is restricted to purposes directly connected with the administration of the Medicaid program.

Comment:

The IFR preamble lists the rationale for the limited set of data points for an accounting of disclosure based on the data that HHS considers available in a typical EHR audit log. The data points required are: the date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure. However, this list is only a subset of the data that a covered entity is required to provide to an individual requesting an accounting of disclosure under 45 CFR 164.528 (b) (2), and substantially undercuts the utility of that information.

For example, the user identifier from an audit log will likely not convey useful information to a patient about the entity to which the PHI was disclosed; contacting the disclosed to entity will be difficult without the address of that entity; and without a purpose for disclosure, a patient will have difficulty discerning the rationale for the disclosure, which may increase mistrust that could be alleviated had the patient know the purpose and uses for which the PHI was disclosed.⁴ This truncating of the disclosure data set does little to alleviate the accounting burden as the covered entity would be required to provide both an electronic subset of HIPAA required disclosure data points and a hard copy accounting for those data points that were not required of certified EHR technology.

HL7 recommends:

We recommend that the final rule stipulate that certified EHR technology be required to provide the full set of HIPAA accounting for disclosure data points per 45 CFR 164.528(b)(2).

§170.299 Incorporation by reference, and all language referencing this section:**Comment:**

HL7 suggests that by referencing multiple versions and not specifying implementation guidance, ONC is continuing the potential for varying interpretation on the content and vocabulary to be used for specific communication exchanges. HL7 recommends that the rules refer only to a minimum standard, which ONC may increase over time, and recognize a sanctioned structure and/or process with an open, consensus-based decision making process, where industry stakeholders can come together to agree on most current implementation guidance, agree on reasonable take-on target time lines, where decisions are well documented, voted on, and with full opportunity for any stakeholder to participate and voice their perspective. Appropriate implementation guidance is needed for standards to be successful.

⁴ http://edocket.access.gpo.gov/cfr_2003/octqtr/45cfr164.528.htm

(b) Implementation specifications: Content of the accounting. 2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of

this section, the accounting must include for each disclosure:

- (i) The date of the disclosure;
- (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
- (iii) A brief description of the protected health information disclosed; and
- (iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under Sec. 164.502(a)(2)(ii) or 164.512, if any.

HL7 Recommends:

A) For Stage 1, HL7 suggests that 170.299 uses

- HL7 V2.3.1 as the minimum standard version across all V2 based transactions.
- HL7 CDA R2 Level 2 as the minimum standard version for exchange of documents

B) For Stage 1, HL7 suggests that the rules recognize one or more organizations from the SDOs and those that harmonize the output from such SDOs, similar to HITSP, as the sanctioned organizations to manage evolution of the necessary implementation guidance, e.g.,

- EHR Lab Reporting using HL7 ELINCS as a starting point.
- Patient Care Summary using the HL7 CCD Implementation Guide as the starting point.

We should recognize that base standards allow for substantial optionality as they have to consider substantial variations in diverse use cases whereas implementation guides can significantly reduce interpretation variations. Encoding specific standards versions and implementation guides through rule making, beyond reference of the standards family (e.g., HL7 V2, X12, HL7 CDA), would inappropriately impede progress and take-up of more current implementation guidance that brings us closer to common interpretation and implementation of interoperable data exchange.

For Future Consideration

In General:

The following comments are not expected to be implemented in Stage 1 but should be considered when generating regulations for the following stages.

Comment:

It is recommended that the ONC specify standards in the following areas: Patient Identification, Disclosure Management for HIE, and Alterations/Amendments/Corrections. These three areas will be instrumental in support of health information exchange activities required for Meaningful Use Stage 2 measures. We recommend these three areas be addressed because there are currently gaps in existing standards which need to be developed, tested and then incorporated into certification criteria well in advance of 2013/2014. In order to accommodate that timeline, the standards or direction/priority for standards need to be addressed now to guide activities appropriately.

Patient Identification Standards Gaps:

Comment: Properly identifying an individual and their related records is the cornerstone of effective health information exchange activities. Current EHR standards lack patient identity management requirements for EHR systems to address the following:

- Ensure systems use best practices for matching algorithms.
- Ensure systems have functionality to support best practices for matching reliability based on key identifying information

Patient identity management is often a function of a master patient index application in hospitals or built into practice management systems for physicians.

The software and rules for identity management are often proprietary. Generally accepted principles and practices have not emerged to ensure in EHR standards and certification criteria the best practices in identity management to find and eliminate duplicate patients, link alias records (e.g. maiden name to current name), and find patients and their related records based on key identifiers.

Establish a foundation or establish a direction for standards related to patient identity management for EHR modules and complete EHRs.

- Patient identity techniques using key identifiers
- Matching algorithms
- Matching reliability
- Handling an alias
- Handling duplicates
- Handling incorrect matched identities

Health Information Exchange/Disclosure Management Standards Gap:

Comment: EHR system functionality and standards are not mature for management of disclosures that would support health information exchange activities. Standards are needed for the following:

- Automated query and disclosure process for “computer to computer” exchange of information in support of HIE
- Rules engine for disclosures that incorporates disclosure rules, limitations and restrictions.

Establish a foundation or establish a direction for standards related to disclosure management in support of HIEs for EHR modules and complete EHRs that include:

- Automated query and disclosure process for “computer to computer” exchange of information in support of HIE
- Rules engine for disclosures that incorporates disclosure rules, limitations and restrictions.

Alteration/Amendment/Correction for HIE Standards Gap:

Comment: A single accepted practice for alterations, amendments and corrections has not been established for EHR systems (modules or complete). The HL7 Records Management and Evidentiary Support Functional Profile has identified the required functionality, but that functionality is not recognized in certification criteria and not uniformly applied in EHR applications today.

EHR system standards and certification criteria must establish a uniform way of handling alterations, amendments and corrections across all modules and a uniform way of communicating those changes when information has been exchanged through an HIE Organization or with another entity (provider, payor, PHR, etc.).

Current EHR modules have differing business rules for handling amendments, corrections and alterations. The result is an inconsistent record available for exchange activities.

The inconsistency can reduce the reliability of the information particularly without a process for sending updates when changes are required.

HL7 RM-ES workgroup members have discussed this issue. Canadian representatives identify the handling of record changes as a problematic area that needs to be addressed to support health information exchange.

Standards for handling changes to the record are not consistently used by the industry. Standards for handling updates related to changes in support of health information exchange are currently not for EHR systems (module or complete).

- Identify the standard for properly amending, correcting or altering a record for all EHR modules and complete EHRs as outlined in the HL7 RM-ES Functional Profile.
- Establish a foundation or establish a direction for standards related to alterations, amendments or corrections in a health information exchange environment to ensure that information that has been updated is properly, timely, and uniformly communicated to receiving entities.

§170.302 General certification criteria for Complete EHRs or EHR Modules.

(r) Audit log

Record actions related to electronic health information in accordance with the standard specified in §170.210(b), provide alerts based on user-defined events, and electronically display and print all or a specified set of recorded information upon request or at a set period of time.

Comment:

Additional requirements are needed to support the intent and purpose of the audit log for record integrity purposes and ensure that a minimum set of audit logging procedures are completed.

Systems have the capability but system administrators routinely “turn off” audit logging processes to increase system performance and address storage capacity issues. As audit data is used to support record integrity, compliance activities related to breaches, and inappropriate access, is it critical that the audit logs are required during routine operations of the system, that the data be maintained in a secure manner, and be accessible in a human readable format. Many systems have logs, but they are difficult to access (or can only be accessed by the vendor through special processes and with expense). Not addressing accessibility and security in the requirement will result in a mandate that is critical, but may not be fully realized by the health care provider depending on the vendor that they select.

HL7 Recommends:

Audit logs must meet the following requirements:

- Logging must be on during normal production operation of the system for the minimum elements specified in 170.210(b).
- Maintain logs in a secure manner and track all modifications to the logs.

- Produce output in a human readable format.
- Retain logs for the retention period of the records.

170.302(v) and 170.210(e) Certification Criteria and Standard of Accounting for Disclosures

The standard specified in Table 2B stipulates a functional requirement that a recorded disclosure for treatment, payment or healthcare operations must include: the date, time, patient ID, user ID, and a description of the disclosure.

Comment:

The IFR correctly indicated that accounting of disclosure functionality is generally not a component of EHR systems today and not generally part of EHR standards today.

In reviewing the required elements for an accounting, it was noted that the rule missed requiring an important piece of information for an accounting of disclosures – to whom the PHI was disclosed.

The definition of a disclosure for treatment, payment, or healthcare operations includes providing access to information. The record action data does not require collecting “read/view/access” which would be necessary in supporting accounting of disclosure functionality in an EHR module/system.

The difference between a use and disclosure are not adequately defined by the rule to determine when an accounting is triggered.

The accounting of disclosure requirements utilize the record action data required in 170.210(b). The definition of a disclosure includes “access” to information. Without collecting “read/view” as a record action, the audit log is inadequate to support this requirement.

HL7 Recommends:

- A) Collect “who” the disclosure was made to as a required element to completely collect the information that is necessary for an accounting of a disclosure.
- B) Add “Read/View” as a record action in 170.210(b) to support the accounting of disclosure requirement expanding the record actions to include other types of output methods besides the limited and narrow method of printing.