Health Level Seven® International
Unlocking the Power of Health Information

An ANSI accredited standards developer

April 3, 2015

Dr. Karen DeSalvo, MD, MPH, MSc
Coordinator
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
Hubert Humphrey Building, Suite 729
200 Independence Avenue SW
Washington, DC 20201

Dear Dr. DeSalvo:

HL7 appreciates the opportunity to provide feedback on the ONC's Draft Version 1.0 *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*. Health Level Seven International (HL7) is the global authority on interoperability for healthcare information technology (IT) and the organizational home and link for Fast Healthcare Interoperability Resources (FHIR) and Consolidated Clinical Document Architecture (C-CDA), both of which are cited in the Version 1.0 *Interoperability Roadmap* as foundational for critical interoperability wins in the near-term.

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 members represent approximately 500 organizations that comprise more than 90% of the information systems vendors serving healthcare in the U.S.

Given the importance of issues in Version 1.0 *Interoperability Roadmap* and HL7's core relevance to supporting the development of an interoperable health IT infrastructure that supports a broad scale learning health system over the next ten years, HL7's leadership, Policy Advisory Committee and Work Groups contributed notable time and effort to these comments. We would be happy to answer questions or provide further information to you and thank you for your continued efforts to put interoperability at the heart of the national HIT conversation and a robust, patient-centered healthcare infrastructure.

Sincerely,

Charles Jaffe, MD, PhD
Chief Executive Officer
Health Level Seven International

Stanley M. Huff, MD
Board of Directors, Chair
Health Level Seven International

Sincerely,

HL7 Responses to ONC Draft Version 1.0 Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap

Overall, HL7 appreciates the comprehensive listing of relevant Roadmap principles, objectives and the resulting system and standards structure. HL7 offers the following observations and recommendations in response to the proposed Roadmap and the specific questions.

Governance

General: HL7 recommends that the roadmap better and more fully articulate the architectural and governance components for interoperability. There is a need to understand more holistically what interoperability is and what to focus on when. We suggest that a focus on high-value priority use cases will help put the various suggested calls for action into context and allow identification of the various gaps we collectively must address to fulfill use case goals. HL7 is ready to assist with the definition and/or refinement of the various standards and implementation guidance to support necessary interoperability. We suggest a collaborative governance framework as essential to coordinating the activities across the various stakeholder communities to ensure that foundational interoperability components are addressed and available (e.g., standards/implementation guidance, trust framework, infrastructure, and incentives.)

The roadmap should address the underlying challenges that lead to interoperability not having been achieved to the level to which HITECH aimed. Fundamental not incremental adjustments are needed or we will end up with yet another differently detailed document and process but the same inadequate outcome. HL7 suggests careful assessment of the successes and challenges of the past governance structures such as those related to HITSP, AHIC, CCHIT, the HIT-PC/HIT-SC/S&I Framework, and HL7/NCPDP efforts. We suggest part of the challenge has been to focus on too many capabilities at once. As also indicated in the Roadmap, it is important that we start small and simple and focus on being able to complete something concrete before moving on.

Governance Framework: We suggest that governance should be approached as a framework of related processes across various governance entities. It is essential that there are two areas of focus:

- Identify high-value priority use cases that can gain the most by fully enabling them with nationally defined interoperability capabilities.
- Coordinate the completion of all relevant components, including trust framework, principles of privacy and security “by design”, directories, standards/implementation guides, pilots, initial deployments, incentives, sustainable infrastructure, cost-benefit analysis, before the capabilities are rolled out at a national level.

Stakeholder Participation: For governance to be effective, representative participation in the governance processes across the various governance entities is essential. To establish the high-value priority use cases, key stakeholders involve providers, patients, payers, and regulators. To coordinate the completion of all relevant components, key stakeholders involved should include SDOs, software developers, providers, professional societies and others.

Timelines and Scope

Timeline and Migration: Regarding the action timeline and overarching vision for standards transition, HL7 is pleased to see flexibility in the roadmap that allows change over time and a practical, necessary look to the future with references to FHIR and the querying of a common clinical data set. However, we believe the roadmap appears limited with its focus on FHIR and C-CDA as the primary means of interoperability while other standards and implementation guides are equally important to achieve the variety of use cases being considered in Appendix H.

Assumptions on C-CDA and Common Clinical Data Set: Regarding the one common clinical data set referenced in the roadmap, HL7 is concerned because in practice there is no one common clinical data set. Different data sets are needed for different purposes. For example, having a common data set for when a patient presents at a general practitioner, an emergency room or a pharmacy is not effective. Trying to define everything for everybody in an overly simplistic fashion is unworkable and unmanageable. Current deployment of C-CDA documents has demonstrated a one-size fits all document does not achieve the interoperability desired. We note on this issue, the European Union's success when focusing on specific use cases such as problems, medications and allergies. HL7 has a few more specific concerns with the content/scope of common clinical data set which are: (1) extending vital signs beyond a common understanding is challenging; and (2) limiting allergies to medication allergies is problematic. We encourage further defining the common clinical data set based on settings, including other elements and a plan to convene clinicians for their perspectives on this issue.

While HL7 is pleased with focus on the utility of C-CDA 2.0, we believe the roadmap articulates an overly simplistic view of interoperability in this area. Roadmap text leaves the impression that if a common clinical data set is exchanged with the C-CDA2.0, we are all set and interoperability is largely achieved. But this limited view of interoperability is misleading. A combination of document and discrete data exchange, using push and pull methods, is essential to achieve the necessary interoperability to support typical use cases. For example, sending a targeted C-CDA document type for a specific transition of care using Direct transport that can be followed by a FHIR based RESTful service to request additional information, would be suitable for many transition of care use cases, rather than sending one large C-CDA document for every transition. Similarly, using V2 messaging to support Lab orders and results is more suitable than transitioning this to C-CDA or FHIR in the short/mid-term.

FHIR Framework and Profiles: The notion of profiling as we move towards a FHIR framework will be critical. As FHIR is emerging, profiles are currently ad-hoc without wide industry endorsement. This is understandable in the early stages of defining a standard, but we cannot sustain that long-term if we aim to support consistent interoperability implementations at a national level. It is therefore critical these profiles created for certain use cases gain industry support and endorsement to enable consistent interoperability across systems. HL7 is pleased to work with the Argonaut project to help establish such profiles for an initial set of use cases.

Additionally, to meet its full potential and best support national interoperability goals, FHIR will need to have increasing input from clinical experts about clinical FHIR Resources. These experts will have three distinct but closely related responsibilities. The first role would be to provide the subject matter and knowledge experts necessary for the creation of FHIR profiles. The second role or responsibility for the clinical experts is to agree to the set of profiles that will be used for truly interoperable services. The final responsibility for the clinical experts is to say what data is important to share. These issues create a compelling need to have greater involvement of clinical experts in FHIR. HL7 urges ONC to think through ways to incentivize

such collaboration from clinical experts to allow them to effectively contribute their part in making FHIR a truly interoperable solution.

Limited Workflow Scope: We are concerned that the Roadmap initially states that workflow is out of scope for the first iteration, yet offers a number of actions that involve interoperability in support of workflow. This perception is further evident by the emphasis and focus on the exchange of a common clinical data set that also seems to favor a document push approach. We suggest that workflow support is integral to interoperability and should be included in the first iteration. As indicated earlier, interoperability needs to be considered in the context of specific high-value priority use cases, and consider push and pull, document and discrete data, service and direct and message based exchange, to enable the appropriate exchange to provide the user with the right data at the right time.

Device Informatics Plan: Though there are references to personal health devices and the need to advance usage of the FDA Unique Device Identifier (UDI), this roadmap largely ignores the vast amount of information that can be acquired from healthcare devices and used for care delivery, including decision support systems and optimization of clinical workflow. Many products exist today that implement HL7 and IEEE standards-based interfaces. Semantic standards exist for core sets of device-acquired information, especially physiologic monitoring. The Roadmap should be updated to explicitly include a plan for advancing incorporation of device informatics over the next 10 years.

Privacy and Security Protections for Health Information

Response to Roadmap Question: What security aspects of RESTful services need to be addressed in a standardized manner?

Both Security and Privacy infrastructure are critical to RESTful services used in healthcare. HL7 has from its inception placed special emphasis on the mission critical Security and Privacy aspects for conveying health information using any type of platform or protocol it has developed including: HL7's RESTful FHIR Content and Services Draft Standard for Trial Use [DSTU], and its predecessor content and protocol product lines such as Version 2 and Version 3 Messaging, Version 3 Clinical Document Architecture [CDA] and its multidisciplinary CDA Implementation Guides, various model such as the Reference Information Model, SAIF Architecture, various Behavioral, Conceptual Information, Domain Analysis, and System and Service Functional Models.

This is well summarized in the HL7 Version 3 Guide: "It is expected that the healthcare application systems that implement V3 will be required to have significantly more functionality to:

- To protect the confidentiality of patient information than has been common in the past. The new functions may include, but are not limited to, limiting the right to view or transfer selected data to users with specific kinds of authorization and auditing access to patient data. V3 will seek out and adopt industry security standards that support conveying the necessary information from one healthcare application system to another, so that these systems may perform the confidentiality functions.
- To authenticate requests for services and reports of data than has been common in the past. The new functions may include, but are not limited to, electronic signature and authentication of users based on technologies more advanced than passwords. V3 will

seek out and reference standards such as X.500 and RFC 1510 to support conveying the necessary information from one healthcare application system to another, so that these systems may perform the authorization and authentication functions.

- That the technological platforms upon which V3 information systems developers implement applications that use HL7 will be required to have significantly more capability to protect the confidentiality and integrity of patient information than has been common in the past. The new functions may include, but are not limited to, public- and private-key encryption, and correspondent system authentication and non-repudiation.

That is, HL7 either develops, leverages, or collaborates with other SDOs such as OASIS, ISO, ASTM, and IHE to cover all aspects of security and privacy for all of its product lines including authentication, authorization, identity verification and directory standards; ontological, vocabulary, and content models for conveying privacy, security, trust and provenance policies, agreements [such as consent directives], forms [such as patient friendly consent directive templates and other consumer facing user interfaces], security labeling, role-based and access-based access control, integrity, and digital signature.

A cornerstone to the content models used to drive access control systems is the HL7's Healthcare Privacy and Security Classification System [HCS], which specifies standardized vocabulary and formats with which to convey security and privacy requirements on all HL7 protocols, and in particular for Restful interchanges as part of HTTP header, Security Label metadata in e.g., FHIR Resources or in OAUTH Claims Tokens. HCS is based on NIST, ISO, and Intelligence Community specifications, and has influenced or been influenced by OASIS XSPA and the NHIN Authorization Framework and Access Policy specifications.

HL7 FHIR's Security and Privacy Aspects, which meet and exceed HL7's historic high bar for Privacy and Security, are detailed as implementer guidance in the DSTU FHIR Security Section. FHIR specifies the use of Security Labels, and has Resources for Audit Event (based on IHE ATNA) and Provenance. In addition, there is a FHIR ConsentDirective (based on v.2, v.3, and the CDA Consent Directive Implementation Guide) and the associated FHIR Consent Directive Questionnaire/Questionnaire Answer profiles (under development) using the soon to be balloted Patient Friendly Language for Consumer Facing Interfaces Implementation Guide. These are interoperable because they are all coded with HCS vocabulary. We urge ONC to review these specifications.

Ubiquitous, Secure Network Infrastructure E.1 Cybersecurity and E.2 Encryption

HL7 strongly supports additional guidance from Federal Agencies charged with disseminating standards on cybersecurity and encryption of data at rest if these are part of a coherent and comprehensive framework of coordinated standards that are mandatory where necessary. This may require additional regulatory action.

HIPAA set an addressable bar for protection of data at rest that has not proven effective in driving the industry take advantage to the HITECH section 13402 breach notification safe harbor by investing in NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices compliant safeguards when the cost of securing consumers PHI is less than the cost of a security breach. At this juncture, the lack of a framework leaves HL7 and other SDOs at a loss on how to specify sufficient safeguards within their own standards that will form cohesive security and privacy specifications in which to deploy their content and exchange standards. Developing public APIs that cannot assure patients and providers that their information can be safely exchanged as authorized is premature until the prerequisite security layer has been ubiquitously deployed.

However, relying on casualty insurers to incentivize payers to do the right thing as recommended on page 57 Table 5 E2.4: "ONC will work with payers to explore the availability of private sector financial incentives to increase the rate of encrypting" does not seem like a plan with much traction given the number of providers and payers, which are likely already insured against the risk of breach, that are experiencing major breaches at increasing frequency and magnitude. Until the cost of mitigating security gaps in health systems outweighs the cost of mitigating a breach, it's unlikely that this pattern will change. Unfortunately, case law favors the plaintiffs in breach class action suits, and patients and their families are the ones who bear the undue cost of identity theft and disclosure of their sensitive information, which unlike a credit card or bank account, can never be mitigated.

Verifiable Identity and Authentication of All Participants

HL7 concurs with the Roadmap acknowledgement that there is a critical lack of uniform identity proofing and authentication protocols, which impedes interoperability due to Trust issues. HL7 supports the Roadmap suggestion that the US establish common identity proofing practices at the point of care; require multi-factor authentication for all patient and provider access to health IT systems in a way that aligns with what is required in other industries; leverage existing mobile technologies and smart phones to provide efficient, effective paths for patient or provider identity authentication; and integrate the RESTful approaches to authentication in anticipation of that vision of tomorrow.

HL7 is addressing Identity and Authentication as a key part of what would be an interoperable trust framework for healthcare. While HL7 does not make policy, a common trust framework may provide mechanisms to negotiate trust, replacing Data Use and Reciprocal Support Agreements, one-off Memoranda of Agreement, and transport method specific industry governance groups. Some work in this area has already been undertaken by the US Federal Governance Council and NIST and others that is forming the basis of the HL7 work.
HL7 is already working with ONC on demonstrating approaches that fully leverage HL7 standards and include mobile devices, including those owned by the patient themselves, within a technical trust framework. For example, HL7 and ONC will be demonstrating mobile device interfaces with CE using FHIR and restful interfaces during HIMSS 2015.

Consistent Representation of Permission to Collect, Share and Use Identifiable Health Information

Until as recently as the July 15, 2014 HIT Privacy and Security Tiger Team Data Segmentation for Privacy [DS4P] Transmittal Letter HL7 privacy protective technologies have been characterized as still immature, especially at the granular level. HL7 very much appreciates the Roadmap's recognition that:
Technological advances are creating opportunities to share data and allow patient preferences to electronically persist through an interoperable learning health system. Technology provides a means for electronically identifying, capturing, tracking, managing and communicating an individual's choice preferences regarding the use and disclosure of health information from the originating source to other technical systems. Health IT enables not only the capture of a documented choice, but also the capture of what permissions apply, even when there is no documented choice. Health IT can enable users to comply with relevant use and disclosure laws, regulations and policies in an electronic health information environment. [page 63]

However, while recognizing advances in privacy protective technologies that enable policy bridging, ONC asserts that the variance in privacy laws and policies is impeding nationwide

interoperability, and therefore must be harmonized under HIPAA so that non-sensitive health information can be shared without consent for TPO:

Despite efforts to address potential technology standards and solutions for individual choice across this complex ecosystem, it has become clear that the complexity of the rules environment will continue to hinder the development and adoption of a consistent nationwide technical framework (e.g., data elements, definitions, vocabularies) for electronically managing individuals' basic and granular choices until the complexity is resolved. Reducing variation in the current legal, regulatory and organizational policy environment related to privacy that is additive to HIPAA will help facilitate the development of technical standards and technology that can adjudicate and honor basic and granular choices nationwide in all care settings, while ensuring that special protections that apply as a result of deliberative legislative processes remain conceptually in place. Through the course of harmonization, however, individual privacy rights as specified in state and federal laws must not be substantively eroded. For example, where a law protects reproductive health or behavioral health information (to name but two sensitive conditions), harmonization would not mean the substantive weakening of such protections. [page 67]

Over the last ten years, ONC has led, participated, or leveraged numerous policy, policy, and technology initiatives, which have developed, tested, standardized, demonstrated, and deployed privacy and security capabilities that enable patients to control how their information is shared across multiple US jurisdictions and organizations *despite of the variability of laws and policies governing those exchanges.* These initiatives include the deliverables from the HITPC and HITSC Privacy and Security Workgroups, the Health Information Security & Privacy Collaboration [HISPC], State Health Policy Consortium, the Standards and Interoperability Framework Data Segmentation for Privacy initiative, the Behavioral Health Data Exchange Consortium ONC State Health Policy Consortium Project, and the various SDO Privacy and Security Workgroups within ISO, HL7, IHE, ASTM, and OASIS.

Of note: The RTI Report on State Law Requirements for Patient Permission to Disclose Health Information concluded that the very solutions to basic and granular consent being proposed by the Roadmap" would be subject to much debate".[1] And the findings of the HISPC Consent

[1] RTI Report on State Law Requirements for Patient Permission to Disclose Health Information

4.2.1 Possible Federal Solutions

One means for harmonizing or simplifying state laws that has been suggested is one federal standard that uniformly preempts state law.84 Some stakeholders have suggested that the HIPAA Privacy Rule should fill this role.85 The findings of our review indicate that adopting this approach would effectively eliminate many state laws that impose greater restrictions on the disclosure of health information for treatment purposes.86 This approach would require the enactment of federal legislation and would be subject to much debate.

Another federal approach to harmonizing state laws has been proposed by the National Committee on Vital and Health Statistics (NCVHS), a federal advisory committee to the Secretary of the United States Department of Health and Human Services. NCVHS has recommended that the federal government adopt a national policy to allow individuals to have limited control, in a uniform manner, over the disclosure of designated categories of health information […]

Overall, our research indicates that the NCVHS approach with respect to patient control and role-based access aligns with existing laws in many states. However, adopting the NCVHS approach would impede the ability of health care providers to disclose health information for

Options Collaborative, which was charged to identify and evaluate "factors that affect the balance between consumer privacy interests and affordable provider access to reliable health information through HIE. […] Ultimately, the Collaborative did not identify a single consent model that all participants considered acceptable across all scenarios.[2]

The HIT industry has supplied the technology used by organizations and jurisdictions to support patient control over exchange such as Access Control and Consent Directive Management Systems with standards-based policy adjudication engines, and supportive enforcement capabilities such as role and attribute based access control provisioning, and Security Labeling and Privacy Protective Systems. The emerging Healthcare Internet of Things is leveraging authentication and authorization standards such as OpenID Connect, OAuth2, and UMA to provide similar capabilities for RESTful exchanges.

Recommendation 1: Standardize the technical consent framework, not policy which is inherently variable and changing.

We see Provider, Payer, and Research organizations as well as HIEs adopting various types of Consent Directive Management Systems to enable regional and national federated exchange via NwHIN and Direct, throughout CaBIG, with Query Health, and emerging Restful APIs such as Structured Data Capture, Data Access Framework, and the Argonaut project. Adoption of such technologies enable HIEs to enter into Qualified Service Organization agreements with SAMHSA for the exchange of 42 CFR Part 2 protected information.

For these reasons, HL7 believes that "consistent representation of an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s)" is achievable with the current policy enabling and policy agnostic computable and adjudicate-able consent directive standards developed by HL7. If ONC considers HL7 Consent Directive CDA and the FHIR Consent Directive, which leverage the same Healthcare Privacy and Security Classification System codes used for HL7 Data Segmentation, Security Labeling, and Privacy Protective Service standards and FHIR Security Labels and AuditEvent Resource are robust enough to support the uniform and inflexible[4] computational consent regime envisioned in the Roadmap, then these Consent Directive standards are also robust enough to enable jurisdictional and organization flexibility in designing the consent regimes deemed appropriate for the healthcare exchange ecosystems .

---

treatment in many states that permit disclosure of some (or all) of these categories of health information for treatment without patient permission. As the Committee has acknowledged, the NCVHS proposal would also be subject to much debate, particularly with respect to liability issues arising from incomplete information being available to providers.

[2] NGA State and Federal Consent Laws Affecting Interstate HIE p.18 – 19.

[4] OCR touts the flexibility and variance that HIPAA allows covered entities in deciding whether and how to enable patient consent for disclosure of PHI through HIEs in **Individual Choice: The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment [PDF - 168 KB]**

Recommendation 2. Provide patients with a patient friend and easily understandable Consent Directive Framework.

With respect to the following statement on page 63: "As a result, states have created a "patchwork" of health information privacy laws and protections that address individual choice and are not uniform across state lines or care settings/encounters. This patchwork is also not easily understood by individuals."

HL7 as well as many others in the patient empowerment community realizes that patients cannot be full partners in their Health Internet of Things unless they are afforded intuitive, patient friendly user interfaces for all their interactions in the healthcare domain, not just consent.

There are a myriad of online resources specifically tailored to provide detailed and accurate health information to lay persons about complex and variable topics such as health conditions, procedures, medications, and enrolling in health insurance coverage. ONC has amassed a wealth of Meaningful Consent resources specifically designed to assist covered entities with conveying important legal concepts in patient friendly terms.[5]

For these reasons, HL7 has established the Patient Friendly Language Project to develop policy agnostic implementation guidance on standardized language and structures for consumer facing interfaces such as consent directives.

Summary Privacy and Security Comment:

With Respect to the following assertion:
Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s). [p. 61]

HL7 concurs that consistent representation of an individual's consent directive is key for nationwide interoperability through the use of standardized formats and vocabularies, it remains committed to its foundational principle that the standards should always be policy agnostic and policy enabling. To that end, HL7 embraces privacy and security by design and encourages both its stakeholders, standards developers, and implementers to let business requirements, such as jurisdictional, organizational, and patient privacy policies, drive the use of the standards and technologies and not the other way around. Now that interoperable consent directives and security mechanisms for their enforcement have matured, as the Roadmap points out, it is not

[5] Meaningful Consent for providers-professionals search results on www.healthit.gov

clear why consistent representation requires a one size fits all privacy policy and consent directive regime.

Core Technical Standards and Functions

Vocabulary and Code Sets: Regarding vocabulary and code sets (semantics), there is a gap in the standards listed in the Draft Version 1.0 *Interoperability Roadmap* for non-medication orders. This is an important gap to close because clinical decision support (CDS) cannot become interoperable without semantic standards that represent orders and order details. It was a gap that was identified in two S&I Framework initiatives: Health eDecisions and Clinical Quality Framework. However, to HL7's knowledge it is not a gap currently being addressed through any standards development efforts. From a CDS perspective, great progress is being made on syntax/data models (e.g. FHIR, QUICK) and expressions (eg, CQL), but if a CDS system outputs a recommendation (e.g. to order an intervention), there is currently no way for the CDS system and an EHR system to exchange that information in a standards-based interoperable manner.

A scenario that can illustrate this is where a patient with acute pancreatitis is having severe abdominal pain despite initial therapy, and a CDS system identifies the need to obtain an abdominal CT scan to rule out abscess. Today there are no national standards for the representation of an abdominal CT order, so implementation of this recommendation would require a point-to-point exchange with mappings to local terminologies, thereby limiting the scalability of the CDS. A related example is an abdominal CT scan order that resides on an order set. Organizations currently use widely disparate terminologies with different degrees of pre-coordination and post-coordination to express the same concept. For example, one organization might consider "Abdominal CT with contrast" to be the order item, whereas another organization might consider "Abdominal CT" to be the order item, with "contrast" being specified as an attribute of the order.

These examples are focused on imaging, but the same concept applies to laboratory orders, nursing orders, and other non-medication categories. Given such heterogeneity, a scalable and interoperable system for sharing CDS artifacts and services will not be possible without closing the gap in standards for non-medication orders.

Standards Activities Additions: On page 83 of the roadmap there is a list of "…standards activities that are being worked on …"

HL7 recommends adding to this list: laboratory related ONC S&I Initiatives – Laboratory Implementation Guides (Orders [LOI], Results [LRI], electronic Directory of Service [eDOS] and Electronic Laboratory Reporting [ELR]), until the Normative edition of these Implementation Guides are published at the completion of the draft standard for trial use period. The EHR-S Functional Requirements for Lab should also be added.

Measurement

Measures and Interoperability: There is a need to get and use measures as supporting information to track overall use case improvements. Measuring interoperability volumes on their own does not yield any good information on whether interoperability contributed to the improvement to the use case.

HL7 has important work in progress on measuring standards maturity beyond current practices. We are happy to share this with ONC and work together exploring this issue.

Priority Use Cases (Appendix H)

1. Appendix H lists the priority use cases submitted to ONC through public comment, listening sessions, and federal agency discussions. The list is too lengthy and needs further prioritization. ***Please submit 3 priority use cases from this list that should inform priorities for the development of technical standards, policies and implementation specifications.***
    a. We do not have specific high-value priority use cases to contribute, but as they are being established, HL7 is ready to work with the community to ensure that gaps and missing standards / implementation guides are addressed to ensure there is appropriate support for the use cases.

Standards Advisory

Responding to the call for comments under the standards advisory section, HL7 offers the following observations and recommendations:

A number of important items should be added to the Standards Advisory document including:

- Methods for indicating standards' maturity and availability of test tools;
- Measures of standards adoptability in terms of maturity and implementability;
- Notations of which standards in the advisory are also required for eHR certification in regulation and context about where they are required; and
- Examples of real world implementations in each category and an expert implementation contact.

Other specific HL7 recommendations include:

- The Standards Advisory states that "Sex" references the HL7 V3 Value Set, but the hyperlink currently goes to CDC PHIN website. We would suggest this link be correctly clarified.

- There is a Value Set Authority under the auspices of the National Library of Medicine. This may be a better 'source' for standards vocabularies (http://www.nlm.nig.gov/hit_interoperability.html)