

**HIT Standards Committee
DRAFT
Summary of the December 19, 2012 Virtual Meeting**

ATTENDANCE

The following members attended the meeting:

- Dixie Baker
- Anne Castro
- Christopher Chute
- John Derr
- Lorraine Doo
- Floyd Eisenberg
- James Ferguson
- John Halamka
- Leslie Kelly Hall
- C. Martin Harris
- Stanley Huff
- Elizabeth Johnson
- Rebecca Kush
- Arien Malec
- David McCallie Jr.
- Nancy Orvis
- Jonathan Perlin
- Wes Rishel
- Christopher Ross
- Walter Suarez
- Sharon Terry
- James Walker

The following members did not attend this meeting:

- Tim Cromwell
- Kevin Hutchinson
- J. Marc Overhage
- Charles Romine

KEY TOPICS

Call to Order

MacKenzie Robertson, Office of the National Coordinator (ONC), welcomed participants to the 43rd Health Information Technology Standards Committee (HITSC) meeting. She reminded the group that this was a Federal Advisory Committee (FACA) meeting being conducted with an opportunity for public comment, and that a transcript will be posted on the ONC website. She called the roll and reminded members to identify themselves for the transcript before speaking.

Remarks

David Muntz, Principal Deputy National Coordinator, remarked on the opportunity to celebrate the many accomplishments in HIT. He thanked the HITSC, the public, workgroup members, implementers and everyone.

Review of the Agenda

Jonathan Perlin, Chairperson, commended the hard work completed by ONC staff. He reported that he had been unable to attend the ONC annual meeting due to his travel in the United Kingdom. Although there is tension regarding EHRs, much progress has been made in the United States. This is a time of transition from closing out Stage 1 to initiation of Stage 2 and planning for Stage 3. The work on the test scripts indicates remarkable progress. Workgroup activities are interdependent. The use of the test scripts will improve EHR internal consistency. He acknowledged the significance of the recommendations to be presented, recognizing that the recommendations on module certification were a result of Dixie Baker's insistence at the September meeting that privacy and security be considered in modular certification.

He inquired about objections, corrections, improvements or additions to the meeting summary distributed with the meeting materials and, hearing none, announced the acceptance of the summary of the November meeting as distributed.

Action item #1: The summary of the November 2012 HITSC meeting was approved as circulated.

Comments

John Halamka, Vice Chairperson, reported that the ONC annual meeting was a high-energy event of celebration of progress. HITSC's work was well represented. He emphasized the importance of test scripts, saying that a bad script is harmful to the industry. For example, in Stage 1, a certification test of e-prescription used a medication banned by the FDA years ago. He also noted the importance of the other recommendations being made, saying that the HITSC was facilitating the road from paper to action.

Implementation Workgroup (IWG) Comments on the Test Scripts

Liz Johnson, Implementation Workgroup Co-chair, reported that the workgroup had reviewed all of the public comments and added to them as determined to be necessary. The ONC and CMS staffs have already incorporated much of the workgroup's work. The test procedures were released (and reviewed by the workgroup) in four waves. The members reviewed 36 of the 47 test procedures, excluding the privacy and security tests. Then they reviewed the staff summaries of the public comments and recommended concepts not captured in the public comments. The workgroup report did not include the public comments, and the workgroup made no additional recommendations if the members determined that the public comments were comprehensive. Many comments have already been implemented.

Recommendations were as follows:

Computerized provider order entry: Although an order change can be accomplished by cancelling an order and entering a new one, we recommend that the criterion allows the user to change an existing order without cancellation. Recommend listing medication by generic name in addition to brand or trade name.

Vital signs, BMI, and growth charts: Recommend changing the growth charts test data so the EHR will plot a chart for a late pediatric patient, not an adult. Although the CMS meaningful use objective's age range is 0-20 years old, growth is usually complete between 16 and 18 years (this is reflected in test procedures). For Stage 3, recommend lowering the upper age boundary for plotting of growth charts.

Smoking status: Recommend clarifying that an EHR can map to the eight smoking statuses based on a more granular level of data entered by the user (e.g. cigarettes per day, pack-years, etc.)

Patient-specific education resources: Recommend clarifying that an EHR function, not Infobutton, selects a patient (this is reflected in test procedures). Recommend disallowing certification testing in which the three data categories (problem list, medication list, laboratory tests and values/results) can be tested in combination to identify education resources (i.e. this test would only allow the identification of resources based on one category at a time) (this is also reflected in test procedures).

Immunization information: For Stage 3, the test procedure and data assume that the provider documenting an immunization is the provider who administered the immunization. Recommend allowing physicians the ability to record immunizations administered by other providers. Since this information would likely be supplied by the patient, the test data set would differ as the patient may not know the immunization specific information such as lot number, expiration date, and/or manufacturer.

Demographics: Recommend clarifying how to test that all languages, as defined by the standard, can be recorded within the EHR, if display of each language is not required. For Stage 3, recommend capturing birthplace in future iterations of this certification criterion.

Family health history: For Stage 3, recommend accounting for adopted individuals in future iterations of this certification criterion.

After recognizing the staff work on the test scripts, Cris Ross, Co-Chair, continued the presentation of recommendations.

Drug-drug, drug-allergy interaction checks: The test procedure should include CPOE as described in the certification criterion. Before a medication order is completed and acted upon during CPOE, interventions must automatically and electronically indicate to a user drug-drug and drug-allergy contraindication based on the patient's medication list and medication allergy list.

Clinical decision support: Recommend that demographics and vital signs be tested in combination with the other listed data elements, as the test procedure allows, to trigger an intervention.

Image results: Recommend clarifying that the vendor can determine the format and structure for images and results test data (e.g. DICOM is permitted but not required). Recommend clarifying how to test that the image and results are complete and accurate (i.e. clarify definition of complete and accurate).

Electronic medication administration record: Recommend clarifying how assistive technology can and will be used and requiring that the test be directly observable by the tester. Recommend defining acceptable methods in which a tester can and will observe the use of assistive technology during the certification testing process (i.e. ensuring a real scenario in a test environment). Recommend clarifying specifically how all the rights will be tested especially the right route.

Clinical summary: Recommend clarifying if historical data (e.g. vital signs) should be included in the ambulatory clinical summary. Recommend clarifying the Care Plan Section as it does not align with the certification criterion (e.g. the criterion describes the care plan as a narrative of goals and instructions; however, the test data define specific elements with structured data including LOINC, SNOMED CT and CPT codes) (this is reflected in test procedures).

General: Recommend industry support to assist with C-CDA adoption. This could include an ongoing forum, led by an ONC or industry group, where vendors and users can continue to improve and enhance the adoption of C-CDA throughout its evolution. For Stage 3, recommend allowing a user to import individual elements of a C-CDA into an EHR and including past history (e.g. surgical, illnesses, etc.) in clinical summary and the C-CDA.

Data portability: Recommend not certifying for the severity of medication allergy. Note that this also applies to the transitions of care certification criterion (this is reflected in test procedures).

Transmission to public health agencies: For syndromic surveillance, the testing should mimic a real scenario in a testing environment; however, the testing will be limited by the ability of the public health agency (or testing representation of this agency, such as a test tool) to receive the data. For Stage 3, recommend exploring transport standards or facilities specific to syndromic surveillance.

Discussion

Arien Malec inquired about 314 B, clinical information reconciliation of active medications and problem and medication allergy lists, and the creation and display and updating of a single list and incorporation of data in the clinical summary in Stage 3. Johnson said that the recommendations did not pertain to the clinical summary; they pertained to bringing in past history. Rishel reminded Malec that the recommendations were not a restatement of the public comments. That importing the enumerated data elements from C-CDA was not mentioned in the recommendations does not imply that the workgroup is opposed. Halamka clarified that problems of medications and allergies are expected to be reconciled; the recommendation is suggesting that the contents of the C-CDA should be incorporated as structured data and not just free text in Stage 3.

Jamie Ferguson suggested that for language, the character encoding according to a standard that would support the indicated languages be specified. He explained that a commonly used standard for that purpose is ISO 8859-15, which supports essential character encoding for all of the commonly used Western European languages. An alternative standard is ISO 88571, Latin alphabet number one versus Latin alphabet number nine, which supports French names as well as transliteration of Russian, which would limit the way the languages have to be captured according to the standard. ISO 8859-15 is supported by Windows software in the United States. Johnson responded that the suggestion can be entertained by ONC.

Halamka related an example from his organization on image results. Since EHRs currently in use generally do not store or manipulate images, separate PACs or imaging management systems are required for viewing. With the GE vendor neutral archived version 4, when the EHR shows a report or study results, a link appears in the report. Clicking on that link results in a single sign-on patient context transaction that calls the PAC system or the vendor neutral archived and it invokes the viewer that is provided by GE and shows the clinician the image as it would be shown to a direct user of the PAC system. He went on to say that more detailed guidance on testing and guaranteeing the integrity of the image would be helpful. Perlin concurred that language qualifying the intent without micromanaging the architecture would be valuable. Malec noted that literal interpretation of the certification requirements could result in hardwiring the actual component used to display the image as a certified EHR technology as opposed to allowing providers to swap in and out other image viewers.

Regarding drug – drug interaction, Leslie Kelly Hall commented that in the new edition the patients' identification of their drugs should be incorporated into reconciliation. Ross responded that the requirement includes such data. With regard to image results, he reported that the workgroup's recommendation is only supplementary to the pages of public comment being reviewed by ONC staff. The whole issue about the relationship of the EHR to other systems in some ways is included in the phrase about complete and accurate image and results. What is complete and accurate from the standpoint of the EHR and the patient record is not the same as what is maintained in the systems external to the EHR.

Rishel recommended a wording change to: Recommend clarifying that the vendor can determine the format structure and access method for images and results test data so that tests have to be written so that someone using a viewer in within the terms of the requirement.

Jim Walker observed that guidance on the relationship between medical history and past medical history in the clinical summary would be helpful, though he acknowledged that composing such guidance would

be difficult. Ross informed him that the recommendation represented consensus; he realized that the recommendation could be a stronger one. The conceptual boundary between medical history and past medical history is porous; there will probably be processes that are automated that will need to be distinguished. What is useful for capture will vary by professional discipline. Johnson observed that in gathering a current history, past events are included. The topic warrants continued exploration.

Perlin asked whether, pending incorporation of the spirit of comments made during discussion, members had objections to transmitting the test scripts recommendations to ONC. He said that Robertson should prepare and send the transmittal memo before the holidays. No objections were heard. Perlin declared approval of the recommendations.

Action item #2: The test script recommendations were approved.

Ross described the 2014 test scenario development, an alternative to unit-based testing. The approach reflects a typical clinical workflow in multiple care settings, allows persistence of data elements (i.e. model for data threading), and maintains testing flexibility (e.g. add/remove —unit test). The workgroup's process is to design a clinically plausible workflow based on the 2011 Edition Certification Criteria and then to reevaluate the scenarios against the 2014 Edition Certification Criteria. The test scenarios work requires development of: specific test scenarios (e.g. interoperability, CQMs); test scenario scripts; and test scenario data for implementation early in 2013. Work in preparation for Stage 3 includes distribution of the workgroup's assignment among the members, feedback and recommendations and the consideration of a recommendation for asynchronous adoption of standards. The workgroup will submit recommendations to the HITSC in January 2013. A public hearing to solicit feedback on the progress of Stage 2 is planned for February.

Halamka indicated that the time frame fit with what he was hearing from certification bodies. McCallie responded that Cerner Corp. will begin testing in March. He asked about an expectation that all certification bodies will use the scenarios. Ross responded that he hopes the scenarios will be adopted by all bodies. Johnson noted that the use of scenarios will be optional but workgroup members representing vendors have indicated their enthusiasm and acceptance. Halamka repeated his offer for an early pilot testing site. Ross acknowledged that a better result could have been expected with more time between script release and implementation. Malec reported that his company has completed products ready for testing. He advocated for being realistic about Stage 3 expectations. He expressed concern about the HITPC-HITSC interplay and the Stage 3 time frame.

Baker reported that in its work on modular certification, the Privacy and Security Workgroup found that many of the certified modules are actually subsets of certified complete EHRs. Efficiencies could be gained by taking this into account. Test results could be reused. Johnson admitted that the workgroup had not considered that idea, but since the idea is a good one, it will be placed on the workgroup's agenda. Wanting to be sure she had understood the point, Johnson repeated, asking about a correct interpretation: If I have done a complete testing for my EHR and all modules are included, can I use that same testing result to get certification at the modular level? Is that a correct interpretation? Baker said bi-directionality may be possible. She clarified that in such a situation, the product would not necessarily be exempt from certification, but relevant test results could be reused for certification. McCallie interjected his endorsement: it would be great to avoid having to retest something that has already been certified as a complete EHR just because it is represented as a module. Johnson and Ross indicated that they planned to consider Baker's idea.

Trusted Identity of Patients in Cyberspace Report Out

Dixie Baker, Chair, Privacy and Security Workgroup, reported on the public hearing on trusted identity convened November 29. She explained the difference between identity proofing and authentication. Identity proofing is the process of collecting and verifying information about a person for the purpose of

proving that a person who has requested an account, a credential, or other special privilege is indeed who he or she claims to be. It may include, for example, driver's license, passport or birth certificate. Identity proofing is performed before the account is created (e.g., portal, email), the credential is issued (e.g., digital certificate) or the special privilege is granted. Authentication is the process of establishing confidence that an individual who uses a credential that is known to the system (e.g., login name, digital certificate) is indeed the person to whom the credential was issued. The three types of authenticators are: something you know (e.g., password); something you have (e.g., smartcard, hard token, mobile phone); and something you are (e.g., fingerprint). Multi-factor authentication requires more than one type. Authentication is performed each time a user logs into an account (e.g., portal, email) or otherwise uses a credential. Baker explained that the purpose of the hearing was to aim toward "best practices" for Stage 2 and forward-looking practices for Stage 3. The Privacy and Security Tiger Team will present policy recommendations to the HITPC in January.

Panelists described several ID proofing methods. In-person proofing is performed by the provider where a relationship/trust exists. The providers' employees need to be trained on the basics of identity proofing. Some use methods that rely on third parties (such as notaries public). Remote proofing may be based on: the reuse of existing credentials; third party, knowledge-based questions; or demographic matching on practice management or other provider systems. The latter should be accompanied by out-of-band confirmation (e.g., letter). Much education of both consumers and providers may be required. Dissemination of "best practices" rather than certification is the preferred approach. Regarding authentication methods, Baker explained that the Tiger Team had previously recommended a minimum of user name and password. The team questioned whether a higher level of assurance was needed. It appears that no single level of assurance is right for all purposes, but "best practices" that move in the same direction as online banking are suggested. Transparency regarding risks and benefits for download and transmit should be adhered to. Practices should move toward the National Strategy for Trusted Identities in Cyberspace (NSTIC) approach. Other observations by the workgroup were made. The required level of assurance should be defined, not how it is to be accomplished. Providers need a higher level of assurance than do patients. Best practices rather than certification is recommended.

Baker continued. The 2014 Edition of Standards and Certification Criteria require the capability to use Direct to transmit health information to patients and third parties. CMS has made clear that transmission using transport standards other than Direct (SMTP, FTP, REST, SOAP, etc.) will still count toward the patient-action (5%) measure. The HITPC has raised questions regarding the use of Direct for transmissions to consumers, given perceived complexities associated with the issuance, use, and management of digital certificates. It is anticipated that PHR service providers will provide Direct addresses and associated digital certificates, to consumers. As a measure of identity proofing, providers will need to obtain Direct addresses directly from patients requesting record transmission.

Discussion

Halamka talked about the many consumers who use PHRs and do not understand the need for new credentials at each doctors' offices. He wondered about ever reaching the point where physicians can get out of the authentication credential-issuing business. Some kind of trusted identity management behind the Open ID should be recognized. Baker said that trust of Open ID may be a good idea. However, the health care industry is extremely regulated and providers need to feel protected.

Privacy and Security Workgroup Recommendations on Certification of Modules

Dixie Baker presented recommendations for the 2016 Edition. She began by thanking Will Phelps, ONC, for his work. She provided the back story for the recommendations. The HIT Certification Program certifies two types of EHR technology: complete EHR and EHR module. To qualify for a meaningful use incentive payment, an EP, EH or CAH must adopt and meaningfully use Certified EHR Technology (CEHRT). They can select either a certified Complete EHR, or a set of certified EHR modules that

collectively meets the CEHRT definition. The responsibility for assuring that a set of certified EHR modules can successfully and securely be integrated together is left up to the adopter, who is also responsible for assuring that the operational environment is HIPAA compliant. The 2011 Edition certification process requires that all EHR technology presented for certification meet all privacy and security certification criteria unless the presenter can demonstrate that required security capabilities are inapplicable or technically infeasible. If EHR technology relies on additional software to meet the criteria, then that external software must be included in the EHR technology's testing and certification and disclosed to customers, and is listed with the primary EHR technology on the Certified HIT Products List (CHPL). Applied to EHR modules, this approach has led to product developers' implementing security functions that will never be used in actual operations, or having to generate documentation explaining why the requirements were inapplicable or technically infeasible, but providing no real value beyond the certification process. This approach discourages developers and implementers from taking advantage of external security services available from the enterprise in which the certified EHR module is implemented. The 2014 Edition introduced changes aimed at streamlining the certification process and reducing regulatory burden. It eliminated the requirement for EHR modules to be certified to the privacy and security certification criteria. It also introduced Base EHR definition – a set of core attributes, including privacy and security, that each CEHRT adopted by an EP, EH or CAH must meet. The workgroup was asked to consider whether it might be possible to require that each EHR module be certified against some minimal set of privacy and security criteria, without imposing unreasonable regulatory burden, for the 2016 Edition. The workgroup was instructed to: provide recommendations for certifying EHR modules under the 2016 Edition; identify the minimal set of privacy and security standards and certification criteria; and anticipate future broad adoption of NSTIC-based authentication, with which the recommendations should be compatible.

The workgroup found that EHR certification regulations do not explicitly define Modular EHR although it is interpreted as software that meets “less than all” EHR certification criteria. If a vendor presents for certification a module that meets the requirements of one or more security criteria but does not address any non-security criteria, that module can be certified under the ONC HIT Certification Program. However, only one EHR module has been certified against only privacy and security criteria. It is very difficult to define a rigid test approach for certifying the broad range of possibilities that EHR modules could present. Most certified modular EHRs are subsets of products certified as Complete EHRs, specialty software (e.g., anesthesia, critical care), and special purpose applications (e.g., e-prescribing, meaningful use reporting). For the strongest security protection, each EHR module integrated within an enterprise would use a common set of enterprise-wide security services. Baker reported that the Privacy and Security Workgroup agrees that having each module implement its own security is not an ideal approach. She reminded the group that the recommendations for the 2016 Edition reflect comments on the preliminary recommendations discussed at the previous HITSC meeting.

She stated and showed slides on the recommendations: For 2016 Edition EHR certification, each EHR module presented for certification should be required to meet each privacy and security criterion using one of the following three paths. The first path is to demonstrate, through system documentation and certification testing, that the EHR module includes functionality that fully conforms to the privacy and security certification criterion. The second path is to demonstrate, through system documentation sufficiently detailed to enable integration, that the EHR module has implemented service interfaces that enable it to access external services necessary to conform to the privacy and security certification criterion. The third path is to demonstrate through documentation that the privacy and security certification criterion is inapplicable or would be technically infeasible for the EHR module to meet.

The minimal set of security functionality that every EHR module should be required to address via one of the three defined paths is: authentication, access control, and authorization; auditable events and tamper

resistance; audit report(s); amendments; automatic log-off; emergency access; encryption of data at rest; and integrity.

Baker noted that as new privacy and security certification criteria are adopted, this minimal set will need to be revisited. For example, the optional accounting of disclosures criterion will need to be evaluated as a potential addition to this minimal set once the final rules are issued. She then presented slides that delineated implications and needs for certification.

Discussion

Malec asked about calling for standards for modules and what might they be. Baker reminded him that at the November meeting, HITSC members instructed the workgroup not to recommend standards but rather to recommend documentation. If standards were used in the module, the documentation would provide that information. Additional documentation should not be required. The first and second paths should already have included the documentation so that the module can be integrated. Detailed documentation would identify the expected parameters, the data structure and give other information.

Doug Fridsma, ONC, said that interfaces can be defined either by a standards-based approach or a proprietary approach: What if someone brings two modules together and says that there is an interface between them that satisfies the requirements and wants to have them certified together? Or is this more like attestation based on the documentation? Baker reminded him of the discussion at the previous meeting in which the members said that two paths should be combined as the second path. For the second path, the standards in the interface are not specified, but the documentation would be required. The first path is one in which two modules are brought together.

Halamka declared his support for the recommendations, saying that their implementation would enhance privacy and security. Additionally, they address the complaint of entrepreneurs who said that Stage 1 did not allow for innovation with modules. It is important to facilitate innovation in consumer-generated data.

Perlin asked for any objections to approving the recommendations and sending them in a transmittal letter. No objections were voiced.

Action item #3: The recommendations from the Privacy and Security Workgroup on certification of EHR modules were approved for transmission to the National Coordinator.

Vocabulary Task Force Recommendations on Dental Vocabularies

Jamie Ferguson, Chairperson, reminded the group that two Stage 2 CQMs require dental vocabulary beyond SNODENT, which is now included in SNOMED. He explained that a National Committee of Vital and Health Statistics (NCVHS) letter from September 2012 cited testimony in which concerns about stakeholder representation and maintenance processes of Current Dental Terminology (CDT), a HIPAA mandated code set, were raised. NCVHS subsequently determined the issue is managed appropriately and it fully supports adoption of CDT for CEHRT and meaningful use. The HITSC Vocabulary Task Force considered these issues in meetings with representatives of the American Dental Association, NIST, and NCVHS and recommends that CDT be adopted immediately as a standard vocabulary for certified EHR technology to support stage 2 meaningful use.

Discussion

Both SNODENT and CDT would be acceptable standards, similar to SNOMED and CPT. Betsy Humphreys, Co-Chair, Vocabulary Task Force, explained that CDT is used to record the procedure. Without the addition of CDT, dental procedures are not entirely covered. SNODENT would not cover both measures. The Value Set Authority Center will have to include both.

Nancy Orvis announced that her organization is concerned with the slowness of SNODENT development. She asked about funding for continued development. Humphreys said that she would inquire and

communicate directly with Orvis. Ferguson indicated that although there may be a desire to accelerate development, it does not necessarily have any impact on the two CQMs. There may be concern regarding interoperability of dental data. Someone said that CDT is already listed in the requirements as an optional standard. If the recommendation is implemented, CDT would become mandatory.

Floyd Eisenberg asked about CDT being an interim vocabulary. Ferguson said that it depends on the content development of SNODENT within ICD-10 and the U.S extension, which is currently not sufficient for purposes of meaningful use.

Halamka clarified that the recommendation was to move CDT from an optional to a mandatory standard.

Jim Walker asked whether it would be appropriate to recommend the incorporation of CDT into SNODENT. Humphreys announced that she had received messages from Steve Posnack, ONC, which led her to rethink the recommendation. Posnack had reminded her that by making CDT mandatory, it would have to be included in products that will never be used for reporting on the two oral health CQMs. She acknowledged the need for more work on the recommendations. Halamka asked if Posnack could suggest language. Rishel asked about the cost of CDT. Orvis said that there is a nominal cost.

Halamka summarized: The notion of CDT being the appropriate vocabulary to represent structured data in the quality measures is not controversial. The recommendation needs to be worded in such a way that it recognizes that CDT should be used in the quality measure. But the HITSC does not want to impose a cost or burden on those vendors or those applications that do not include the two dental quality measures.

Orvis described a use case in which civilians who are called up for military duty are required to report both their medical and dental status. When discharged, the DoD reports their medical and dental status.

Halamka suggested that Ferguson and Humphreys confer with Posnack for language and revise the recommendation for members' approval. Ferguson responded that ONC staff could certainly work out the details. However, he asked for agreement on the intent of making CDT an adopted standard vocabulary to enable the CQMs when they are used.

Halamka asked for objections to the approval of the intent of the recommendation. Hearing none, he announced approval.

Action item #4: The intent of the Vocabulary Task Force's recommendations on CDT was approved.

Halamka announced that the Vocabulary Task Force would be consolidated under the Clinical Operations Workgroup.

ONC Updates

Doug Fridsma showed slides and talked about an overview of the S&I Framework and the current status of various projects. In the coming months staff will begin to transition the portfolio from development to maintenance. ONC has contracted for advice on how best to maintain the products, which will involve coordinating with SDOs. Eventually, he expects that products will be packaged and the artifacts made available to the public.

Q&A

Some products will be turned over to other organizations for maintenance. Due to an 80% decline in funding, it is necessary to streamline and be efficient in the use of remaining funds. Very limited development will continue. The HL7 community will have to take over maintenance of C-CDA. Rishel talked about the aggressive timelines for meaningful use and pointed out that the ability to manage to a deadline is different under a more distributed approach. He expressed his hope that ONC can negotiate

the necessary support from organizations with multiple missions. Maintaining control over focus and deadlines will be difficult.

John Derr noted the importance of S&I projects as facilitators. McCallie cautioned that S&I's ongoing work has important implications for stage 3 that vendors themselves often miss and cannot keep up with, for example, Health eDecisions. Fridsma promised to do his very best for the most value. Staff is currently identifying priorities.

Baker asked about ONC's plans for standards readiness work initiated through the efforts of the NwHIN Power Team. Fridsma acknowledged that the identification of standards and their readiness will be increasingly important. ONC will rely on the workgroups to a great extent.

Kelly Hall requested that guidance be provided for patients' contributions of their data. Fridsma advised that since SDOs are voluntary organizations, those who participate influence the adoption of standards. The NwHIN Power Team recommended characteristics of good standards for meaningful use. Engagement by organizations that are willing to test is essential.

Fridsma, Cont.

Following the request for comments (RFC) on Meaningful Use stage 3, assignments to the HITSC workgroups were made on December 14. Fridsma said that some items were assigned to more than one workgroup with the primary and secondary workgroup designated. Should members of a workgroup wish to take on items in addition to those assigned, they may contact Robertson. And some items have yet to be assigned. Workgroups will report on their assignments at the January 16 meeting. He instructed them to use these questions in their assignments:

- What are the existing standards that we have to support the goals and objectives of MU3?
- How mature are those standards? How many people use them?
- How much time would it take to get to the next incremental step?
- What is needed to get to that next step? Pilots and experience? Refinement of the standard? Development of consensus across different approaches?

Fridsma said that since not all topics had been assigned to workgroups, the chair and co-chair must decide how to handle the remaining items. Halamka responded that since the Clinical Operations Workgroup had done work on several of the remaining topics, most of those topics will be so assigned. Ferguson announced that he had already started to review the items.

The RFC period closes January 14. Workgroups will report their comments at the January 16 in-person meeting. The health information exchange in-person hearing is scheduled for January 29, 9a.m. – 4p.m.

Robertson requested that the record show that three members had joined the call after roll call—Floyd Eisenberg, Nancy Orvis and Martin Harris.

Public Comment

None

SUMMARY OF ACTION ITEMS:

Action item #1: The summary of the November 2012 HITSC meeting was approved as circulated.

Action item #2: The test script recommendations were approved.

Action item #3: The recommendations from the Privacy and Security Workgroup on certification of EHR modules were approved for transmission to the National Coordinator.

Action item #4: The intent of the Vocabulary Task Force's recommendation on CDT was approved.

Meeting Materials

- Agenda
- Summary of November 2012 meeting
- Presentations and reports slides