

Health Information Technology Standards Committee Final Summary of the October 21, 2011, Meeting

KEY TOPICS

1. Call to Order

Mary Jo Deering, Office of the National Coordinator (ONC), welcomed participants to the 30th meeting of the Health Information Technology Standards Committee (HITSC), conducted as a virtual meeting. She reminded the participants that this was a Federal Advisory Committee meeting, with an opportunity for the public to make comments, and that a summary of the meeting would be available online. She conducted roll call, and turned the meeting over to HITSC Co-Chair John Halamka.

2. Overview of Meeting

Halamka characterized this meeting as an opportunity to polish and refine some of the materials that were presented in September. He reviewed the day's agenda, and introduced Dixie Baker, Chair of the Privacy and Security Workgroup.

3. HITSC Privacy and Security Workgroup

Dixie Baker commented that this presentation was being made in response to a request from the Implementation Workgroup relating to Meaningful Use Stage 2. She reminded the Committee of the Workgroup's process. The HIT Policy Committee (HITPC) presented Meaningful Use Stage 2 objectives and measures and other issues, including policy recommendations from its Privacy and Security Tiger Team. At the last HITSC meeting, the Implementation Workgroup presented work on Meaningful Use Stage 2, requesting input from the Privacy and Security Workgroup on privacy and security-related objectives and measures, and also on directives and measures having to do with patient/consumer communication.

The table of information that the Implementation Workgroup passed along had some work already done in the privacy and security area. The Privacy and Security Workgroup considered those suggestions in its work. Baker presented an overview of the Workgroup's recommended certification criteria, standards, and implementation specifications. Committee members received a complete copy of the recommendations in their meeting packets.

An issue that has been ongoing challenge is how to assess what security functionality should become certification criteria for an electronic health record (EHR) module. In looking at an enterprise, the most effective security measures and assurances are built into the infrastructure. They are not built into each application individually. Instead, they are part of the foundational architecture, in the application's operating systems, in the database management systems. There are a number of third-party services that applications typically use rather than doing everything themselves. Baker asked, how much of this should be criteria for EHR certification versus

assumptions of the infrastructure? The Workgroup does not want to simply assume that all of the necessary measures are in place, she said. It is a difficult challenge.

Baker then reviewed the team's general recommendations, as follows:

- Effective integration of EHR, infrastructure, and specialized security products and services is key to protecting electronic health information, care quality, and patient safety.
- Today every complete EHR and EHR module must meet all security certification criteria, which tends to encourage the implementation of security services within the EHR, rather than having the EHR use stronger mechanisms provided by the infrastructure or third-party services.
- To enable the certification process to more effectively address security integration, the Workgroup recommends that the ONC and National Institute of Standards and Technology (NIST) consider modifying the certification process so that each privacy and security certification criterion is treated as "addressable." To meet the criterion, each Complete EHR or EHR Module submitted for certification would need to either: (1) implement the required security functionality within the complete EHR or EHR module(s) submitted for certification; or (2) assign the function to a third-party security component or service, and demonstrate how the certified EHR product, integrated with its third-party components and services, meets the criterion.

Baker opened the floor for discussion of these general recommendations.

Discussion

- Wes Rishel indicated that it is not clear that every security or privacy recommendation should be addressable. He offered as an example the requirements for role-based access that seem to require a rather intimate relationship with the EHR software in order to be issued. Considering this case by case, he believes there might be a few instances where "addressable" isn't appropriate.
- Rishel also voiced concern that there are multiple products that have been adopted site by site to provide security, particularly anti-virus products. He questioned whether products would have to certify with all of the antivirus products that any of their clients could possibly use. Is this something that instead needs to be addressed in the required Health Insurance Portability and Accountability Act (HIPAA) site audit, rather than in recommendations for the certification of the EHR?
- With regard to the addressability question, Baker explained that even with role-based access control, it depends on how the EHR is integrated with the system. It could be integrated in multiple ways, and as the technology matures there will be more questions. The ONC and NIST should consider this as they consider these recommendations.
- Rishel suggested that the criteria be categorized into two types. There should be those types that are expected to have a certifiable solution—that is, the standard environment for the EHR that is used for the certification includes the modules necessary to provide those

security functions. Then, there should be other criteria such as intrusion protection and antivirus measures that are carried out at the site level. The vendors expect different sites to use different products. Those are Meaningful Use criteria rather than certification issues.

- Baker said if there is the assumption that the operating system is part of the certification, even that raises questions not easily solved by Rishel's suggestion.
- Cris Ross said that some of these comments may be familiar to those who have been through an SAS 70 or a Sarbanes-Oxley HIT audit, with respect to sorting out what things can be attested to by the vendor. He suggested that the group examine patterns from the best auditing processes to identify where to draw those lines.

Baker then presented the rest of the Workgroup's recommendations, including a series of consumer communications recommendations that are new for Meaningful Use Stage 2. She said that the Implementation Workgroup's table has some of these items listed under privacy and security, and some under patient portal recommendations. The Privacy and Security Workgroup considered all of the criteria relating to consumer communications together, and suggests that they all be considered together when the regulations are being constructed.

She again opened the floor for Committee input.

Discussion

- Halamka asked, when does a specificity become a certification criteria—as in, NIST would build test scripts and look at the detailed conformance—and when is it addressable on its functional characteristics? For example, is ASTM E2147 a set of best practices or is it something that would result in a script that NIST would build to test the functionality of an EHR? Baker explained that this is one of the outstanding questions for which the Privacy and Security Workgroup does not have an answer. They know that existing regulations include certification criteria and standards, and the regulations make it clear that in order for a product to be certified it must meet this criterion and use this standard. However, existing regulations do not include implementation specifications at all, and initially the workgroup thought that implementation specifications should be guidance documents on how to implement, but that they would not dictate a solution. So a user could reference a particular implementation guide, but would not necessarily have to use exactly the method it describes.
- Baker noted that outside of this meeting, she and Halamka had a discussion in which he informed her that the contents of the implementation guide are commonly used to derive test scripts for certification. If that is the case, then the Workgroup will need to make some changes to these recommendations. For example, ASTM E2147 has a list of auditable security-relevant events, some of which it describes as essential and others as optional. That is not always the case, though. Other implementation guides are less straightforward. The Workgroup is asking the ONC for clarification on how the implementation specifications are actually used and what they really should be. Are they really as strong as the standards, or are they intended to be guidance on how to implement?

- B.J. Lide noted that NIST has commented on this issue and is willing to continue this discussion with ONC.
- Rishel suggested that it would be better to recommend “SHA 1” or “SHA 2 *and* SHA 1.” Baker agreed with this amendment to the recommendations.
- Rishel discussed the Notice of Proposed Rulemaking (NPRM) for accounting for disclosure that carries with it an assumption of the level of auditing being done in the EHR. He asked if today’s recommendation is consistent with the NPRM. Specifically, it would require an audit log that includes the identity of the user, the patient, and some general information about the purpose for which the information was accessed. Baker said that is consistent with ASTM E2147. The Workgroup recommends not specifying exactly which data elements must be required in the certification criteria, because that is a policy that each organization would need to specify. The approach they recommend is that policy drives the enterprise’s decision as to what data elements to audit. Rishel pointed out that if they certify certain things, then they will know it is possible for an organization’s policies to require it. He suggested allowing for a wide suite of auditable events, but picking a minimum number that is consistent with privacy protection and requires certification.
- Rishel also pointed out that the definition of an EHR in the regulation and the definition being used Meaningful Use are different. It is clear that there is a requirement implied in the accounting for disclosure NPRM for merging audit logs produced by multiple systems to create a consolidated report.
- Baker commented that existing standards dictate that an organization must detect and record events, but say nothing about merging audit records. There is clearly a need for further work if they proceed into the area of merging records.
- Rishel said that good security and protection of private data requires correlation of information across multiple applications within an enterprise. The group should consider encouraging EHRs to produce their audit information in a mergeable format.
- Carol Diamond noted that she understands why using the certification process to ensure that there is capability to carry out these activities is important, and she understands the virtues of merging audit records. However, she indicated that she is confused about whether or not these recommendations and these standards are made on the presumption that there is interoperability of these capabilities across entities, and if so, why? Halamka pointed to the need to combine audit trails in his work, and Diamond concurred that this is necessary in a large, integrated system. But she wonders why a single office using an EHR would be required to have a system that has the capability of merging audit records, even though that office would derive little value from it.
- Baker clarified that the certification criteria that exist today say nothing about the merging of audit records, and they say nothing about the data format. Rishel has suggested that they be collected in a standard format so that they are auditable, but Baker questions that at this point because there are commercial products available that take information from multiple

platforms and bring it together. An entire industry does this without requiring that audit records be in a standard format.

- Rishel said that he reviewed those tools that are available for compiling security events from multiple systems for analysis. He found that those tools are characterized by a significant amount of custom code for major high-end application packages, and they do not by any means automatically or easily cover all of the applications in an enterprise. There is a great benefit to having at least a nucleus of the audit log that is important for accounting for disclosures, and a system that produces the data in some common format is not as high cost as changing the internal auditing of the system.

Action Item #1: The Committee approved by consensus the recommendations of the Privacy and Security Workgroup with Wes Rishel's amendment concerning SHA 1 and SHA 2 (i.e., it would be better to recommend "SHA 1" or "SHA 2 and SHA 1").

Action Item #2: The Committee approved by consensus the minutes from the September 28, 2011 HITSC meeting. Carol Diamond had a slight clarification to one comment, which she is forwarding to Mary Jo Deering.

4. S&I Framework Follow-up Discussion

ONC's Doug Fridsma provided an update from last meeting's discussion, and queued up questions that warrant future consideration. This week, the ONC completed the second of Standards and Interoperability (S&I) face-to-face meetings. They are 1 year into standing up the S&I Framework activities, so they are being somewhat reflective in about what is and is not working. The meetings were held October 18 and 19, and there were 234 attendees.

With about nine initiatives, there is a need to maintain synergy across the various programs. There are 885 registered users participating in the Framework, with approximately 400 active participants. The remaining registered users are tracking and monitoring progress and trying to stay connected. Fridsma commented that it is humbling to see such enthusiasm and expertise coming together to help solve problems. Of the 400 active participants, a significant number were able to attend the face-to-face meeting. At the next HITSC meeting, Committee members will be briefed with a more formal synthesis of that meeting.

With regard to the Nationwide Health Information Network (NwHIN) Power Team, Fridsma offered his thanks for their thoughtful work in evaluating standards readiness. He encouraged the group to continue to work on criteria for evaluation, as it provides transparency and allows people to understand the processes that occurred in peer teams and to translate for those not entirely steeped in standards nuances.

Fridsma heard at the October meeting that some people think the ONC needs additional feedback around the NwHIN. A number of participants did not have an opportunity to provide comments, and it would be helpful to identify a mechanism to allow this feedback to be obtained. Fridsma

also explained that there has been a lot of discussion about what to do with some of the radiology standards, both for imaging and reports. What would be helpful? What is the status of the relevant standards? What needs to be done to create an incremental path for those standards?

Fridsma discussed workarounds for transitions of care (ToC) and the Consolidated Clinical Document Architecture (CDA) Project. He reminded the Committee of the purpose of the Transitions of Care (ToC) Initiative. ToC has developed an agreement on a single standard of clinical summary documents for Meaningful Use. They are also working on implementation guidance on vocabulary mappings, and conversion tools that might be able to migrate existing implementations into a consolidated CDA standard.

As a reminder, Fridsma presented a slide from his last presentation, which shows the steps in the ToC evolution, and especially the path from C32 to templated CDA. He discussed the functional components supporting interoperability in the following areas: (1) use case/common information model (CIM), (2) consolidated CDA, (3) Computable Models, and (4) implementation guidance. He concluded the presentation by asking Committee members to consider how this information relates to previous activities and to think about what is the path to success and easier implementation.

Discussion

- In response to a question from Wes Rishel, Fridsma explained that the ONC was trying to test this approach of building blocks. They used transitions of care as a vehicle to focus that energy and ensure that the elements all worked and the approach was useful.
- Rishel offered remarks that he prepared before he heard the presentation. He said that the continuity of care document (CCD) is designed for a specific transition of care or a set of transitions of care that fall short of all transitions. There are several user stories for specific transitions of care, and then there are other stories that may not relate to transitions. It is important for industry to understand which ones, out of the Consolidated CDA, they should be gearing up on for Meaningful Use Stage 2. They can find ways to provide that guidance to the industry. At last week's Gartner Symposium, he heard from a number of people who worked on other C32 implementations. He was informed that there is a large amount of debugging that is needed at the time of implementation. In part, the problem is that current C32 requires simultaneous interpretation of a number of documents, and even an experienced programmer may have trouble deciding which piece of data refers to which.

There is also ambiguity as to where optional information may go. Testing tools tend not to comment if information is put in one place or another, as long as they both are valid paths for data. In looking at two CCDs created by the same document, data is displayed in different fields or is missing because the mapping was incorrect. There are also differences in handling text. For example, when text is a comment or when it is permissible to send either text or structured data for a given data item, important comments were stripped out.

Rishel noted that in general, people are very satisfied with result of Consolidated CDA. HL7, working with other organizations, has done a tremendous job of flattening specifications

into a specific document. He said that Fridsma and the ONC have done a tremendous job in cutting through organizational issues and making it possible to produce a Consolidated CDA. Many people at the Symposium felt that this specification alone will prevent as much as half of programming errors found in C32 and will cut staff time spent in debating specification interpretation down substantially.

Rishel pointed to the use of business names in the XML as another opportunity to increase the efficiency of programming and testing. This could take place through detailed clinical modeling work, or if Green CDA becomes an acceptable format. He sees some important opportunities for the ONC to further reduce the amount of bilateral testing required when trying to exchange a document containing some mixture of structured data and text among EHRs. It would be ideal if two certified EHRs interoperated and in fact, many user organizations probably expect this to occur. This is more than can be achieved in this round, but quantitatively they should be able to make a reduction in the amount of testing required.

Rishel recommended the following measures:

- Testing by not only passing schematron evaluation, but also examining the data in the system after a message is received and before a message is sent, to see that the correct data is associated with the correct business name.
 - Use multiple test trips. The only test for microbiology was “no growth detected.” There is no reason to believe that two implementations of microbiology, both of which handled “no growth” the same way, also handled other follow-ups the same way.
 - A public testing tool should be funded that uses the same testing rules that will be used for certification parsing and schematron testing, with post-processing tester showing business names. It should also provide sample messages with displays of the business data they contain.
 - Some manner of best practices council should be convened that can discuss those issues that have not been discovered in the standards process. The council would not be able to guarantee that HL7 would finally decide to implement the way they recommend, but it would help push through Meaningful Use Stage 2 and allow HL7 the time to do its work.
- David McCallie commented that CDA is still somewhat of a moving target and asked how consolidation to a moving target will be handled. Fridsma explained the need to identify what those individual templates will look like in Green CDA. HL7 is discussing having the community weigh in about the way that particular templates should work. Once that is accomplished, it will make CDA less of a moving target. The process will take a number of months. Meanwhile, it is important to have mechanisms to map between the current way of doing things and a more consolidated CDA approach.
 - Rishel’s understanding is that the Consolidated CDA was revised in the last iteration to include business names. This is helpful for the programmers and also seems like the basis for standard business names. If HL7 has already made progress on establishing standard business names, then it is a natural next step to establish a Green CDA standard based on those standard business names.

- Arien Malec suggested that in transition of care work, people were defining expectations for clinical semantics for items like medication lists, defining that it had to be an active medication list, and then whether the list had changed, and the associated CDA coding expectations. Those types of business rules on top of CDA would be useful for deeper interoperability.
- Tim Crummel noted that he agrees with the direction of Consolidated CDA. He added that 1 year from now there may be 50 or 60 eligible exchange partners with the Department of Veterans Affairs (VA) through the Virtual Lifetime Electronic Record (VLER) Project; whole states are now in the onboarding process. They are making decisions right now about their specifications for developing CDA or C32, for interoperability and for exchange with VA. If it is possible to take advantage of this current opportunity and escalate it, they can help those exchange partners to make the decisions so that in 6-12 months the VA will be able to bring these groups on and carry out interoperability more quickly. The VA would support accelerating the Consolidated CDA Project.
- Halamka said that future Committee activities will include continuing to drill down on the acceleration of Consolidated CDA. There is also the question of how to take additional NwHIN testimony, and how to examine areas that need enhancement in NwHIN and the RESTful approach. They must also begin to organize themselves to look at radiology and imaging results.
- Fridsma suggested that it might be useful to issue a public solicitation for written testimony. The Committee could review a summary of those findings, and that might be the most expeditious way to move forward. He also suggested that it may be useful to provide a demonstration of the existing tools developed, at a Committee meeting or in some other venue, to get input.

5. Update on Meta-Data ANPRM

ONC's Steve Posnack offered an update on the August Advanced Notice of Proposed Rulemaking (ANPRM) on meta-data, noting that the comment period closed less than 1 month ago. A series of 20 questions were asked to obtain specific input; the ONC received approximately 50 comments. Posnack showed a slide describing the breakdown of the types of commenters, and then presented some general analysis.

The commenters were largely supportive of the use of metadata generally. Some were opposed to federal regulation, and some thought standards development organizations (SDOs) should expand their reach. The ONC asked whether meta-data standards would be ready for Meaningful Use Stage 2 requirements. Nine respondents specifically indicated that they did not believe the industry would be ready. Regarding the CDA header, some respondents supported it; those who did not indicated that it should not be part of the regulation.

The ANPRM's 20 questions related to areas such as patient identity, provenance, privacy (including policy pointers and privacy categorization standards), implementation considerations/use cases, additional considerations, additional standards, and metadata

representation structure. Commenters generally supported the patient identity data elements listed in the ANPRM but suggested additional metadata elements within the patient category and identified others that they felt should be removed. Commenters also indicated that additional provenance elements are essential for accurate data linkage during queries. They indicated that the digital signature should not be included as part of the meta-data. A majority of commenters recommended that time stamp, actor, and actor's affiliation be expressed in XML syntax rather than including in a digital certificate.

It was also noted that metadata should only describe the data set. Privacy should be a separate layer from the metadata. Many commenters suggested looking into HITSP TP30. Many commenters had concerns that detailed privacy tags would inadvertently divulge sensitive information. A significant number of commenters stated that the use of policy pointers would be "problematic." Eleven commenters specifically stated that policy pointers should not be part of Meaningful Use Stage 2 certification requirements. Commenters were divided regarding the level of difficulty in designing EHR technology to assign metadata for Meaningful Use Stage 2.

Discussion

- David McCallie felt that the NPRM was unclear as to what problem was trying to be solved with the metadata. He suggested that the group focus on a small set of problems and develop a pilot rather than imposing it on a broad swath of data interchange. One concern is about when data leaves the control of an EHR or an HIE and passes to the consumer, and then the consumer takes that data and introduces it into another system with no contractual relationship with the first one. What is important is that there be some kind of assurance that data has not been tampered with. He suggested using that scenario as a use case to test.

6. Public Comment

There were no comments from the public.

SUMMARY OF ACTION ITEMS:

Action Item #1: The Committee approved by consensus the recommendations of the Privacy and Security Workgroup with Wes Rishel's amendment concerning SHA 1 and SHA 2 (i.e., it would be better to recommend "SHA 1" or "SHA 2 and SHA 1").

Action Item #2: The Committee approved by consensus the minutes from the September 28, 2011 HITSC meeting. Carol Diamond had a slight clarification to one comment, which she is forwarding to Mary Jo Deering.