HIT Standards Committee
FINAL
Summary of the December 10, 2014 Virtual Meeting

ATTENDANCE (see below)

KEY TOPICS

Call to Order

Michelle Consolazio, Office of the National Coordinator (ONC), welcomed participants to the meeting of the Health Information Technology Standards Committee (HITSC). She reminded the group that this was a Federal Advisory Committee (FACA) meeting with an opportunity for public comment (3-minute limit), and that a transcript will be posted on the ONC website. After calling the roll, she instructed members to identify themselves for the transcript before speaking.

Opening Remarks

Acting Deputy National Coordinator and Chairperson P. Jon White reported that he has been detailed to ONC from AHRQ. He was excited about the draft Strategic Plan. AHRQ recently released the new JASON report, for which some HITSC members had served as briefers (names not stated). This report builds on the previous one.

Remarks and Review of Agenda

HITSC Vice Chairperson John Halamka welcomed White and expressed his hope for the removal of the acting in his title. He summarized the importance of each of the items on the previously-distributed agenda. He acknowledged the December 8 release of the draft HHS HIT Strategic Plan. He announced that two HITSC members will be appointed to the HITPC Strategy and Innovation Workgroup, which has responsibility for commenting on the Plan. He reported that he had recently assisted in raising funds so that HL 7 could work on realization of the JASON recommendations.

Federal Health IT Strategic Plan

Seth Pazinski, ONC, explained that the National Coordinator has statutory authority for updating the HHS Plan. The Federal Health IT Advisory Council, Health IT Strategy and Innovation Workgroup, and the public will provide input, along with a long list of federal agencies. Strategic direction consists of the following: expand adoption of health IT; advance secure and interoperable health information; strengthen health care delivery; advance the health and well-being of individuals and communities; and advance research, scientific knowledge, and innovation. The Plan contains a mission statement, vision, and principles, all of which were shown on the slides. In its final form, the Plan will delineate 3-year and 6-year outcomes that mix metrics and milestones and identify the relevant participating federal agencies. The public comment period ends February 6. This is a federal plan for federal activities. ONC released the *Federal Health IT Strategic Plan 2015-2020* for public comment December 8. He said that the FACAs can be helpful in identifying priorities and indicating opportunities for private sector involvement.

Q and A

Halamka told the members to read the Plan, especially p. 8. Leslie Kelly Hall said that interoperability is necessary to make informed decisions. Implementation of the Plan will impact many federal agencies. Eric Rose announced that he had read the Plan and found it to be substantive. He wondered whether usability and workforce development were covered. Pazinski referred him to p. 10 for workforce development and said that the safety section includes usability. Halamka reminded everyone that the Plan is strategic, not tactical, and is not restricted to meaningful use. Consolazio indicated that the HITSC Steering Committee has responsibility for membership appointment. She suggested that interested HITSC members volunteer for the Strategy and Innovations Workgroup via e-mail. Then the Steering Committee can select among volunteers.

Dixie Baker asked how the Roadmap and the Plan are related and suggested that people who participated in the Roadmap review respond to the Plan. Pazinski acknowledged the overlap among contributors. The Plan's focus is broader and contains more on adoption. The Plan is more directed to federal agencies while the Roadmap takes into account the private sector. Halamka said that the intent was for the Roadmap to follow the Plan.

Approval of Meeting Summary

Halamka apologized for overlooking an expected action item—the acceptance of the summary of the November meeting. He asked for objections, corrections or additions to the summary of the November meeting as circulated with the meeting materials. None were heard and he declared it accepted by consensus.

> **Action item #1: The summary of the November 2014 meeting was accepted as circulated in advance of the meeting.**

Identity Management Recommendations

Transport and Security Workgroup (TSSWG) Chairperson Dixie Baker began by reviewing the HITPC Privacy and Security Tiger Team Recommendations regarding authentication (2012, 2013). In addition to the review of those recommendations, the workgroup heard several presentations from technical experts. The TSSWG recommendations are based on the HITPC recommendations and strengthen and reduce gaps in the current certification requirements. She showed slides and presented these recommendations:

- To strengthen the authentication currently certified in EHR technology, the TSSWG recommends adding the following criteria: continuously protect the integrity and confidentiality of information used to authenticate users, using the standard specified in §170.210(a) (1) of the 2014 Edition EHR Standards, Implementation Specifications, and Certification Criteria. If passwords are used for user authentication, accept only passwords that meet the guessing entropy guidelines set forth in Appendix A of NIST 800-63-2
- To enable EHR technology to be certified for having implemented multi-factor authentication, the TSSWG recommends adding the following certification criterion: restrict access to the system, or to one or more individual functions within the system (e.g., prescribing controlled substances), to only those individuals who have presented at least two of the following three forms of authentication -- knowledge of a secret (e.g., password), possession of a physical object (e.g., hard token or smartcard), or a biometric (e.g., fingerprint)

- Support the NIST effort to revamp NIST Special Publication 800-63-2 (Electronic Authentication Guideline); closely follow the move from LOA to componentized trust; and recommend appropriate identity-proofing for query-based access
- Consider Data Segmentation for Privacy (DS4P) for authorizing access to behavioral data (TSSWG will address later in the work plan)
- Track development and piloting of User Managed Access (UMA) profile of OAuth 2.0 as potential standard for consumer consent

Discussion

Halamka brought up revoking biometric authentication in two-factor authentication. Baker recalled that a biometric cannot be the second form of authentication. What is removed is what is stored in the cache, or the system is instructed not to accept that particular biometric. Halamka said that only living tissue can be used for a biometric. It is more difficult to revoke biometrics than a token or password.

David McCallie asked whether multi-factor authentication was being recommended for every authentication, including remote. Baker emphasized that the recommendations did not pertain to policy; they apply to technical standards. So when an entity decides to require multi factor authentication, these are the recommended technical standards. If a function within a module requires multi-factor, the vendor could so implement. The system must be capable of multi-factor authentication for either the entire system or modules. For example, if the EHR technology's sole purpose is to do prescription of controlled substances, or the module does nothing but prescription of controlled substances, everyone who uses the system or the module might be required to authenticate using multiple factors. But if the module that is presented for certification includes a function within that module for prescription of controlled substances, then that EHR vendor might choose to just require the multi-factors when the user tries to prescribe a controlled substance. McCallie had other questions and comments, including one on re-authentication. He and Baker agreed to discuss them off-line.

Andy Wiesenthal inquired about forced password rotation and greater entropy. Baker responded that frequency of password change is a password policy issue. It is not captured in entropy requirements. Co-chairperson TSSWG Co-chairperson Lisa Gallagher concurred. Wiesenthal suggested that research findings may be available to express a standard for rotation because this is one of the most aggravating tasks for users. Gallagher reminded him that the recommendation pertains to certification only. Several members described their own practices in complying with the letter of their organizations' password change policies, while circumventing the intent of the policies. Gallagher suggested bringing password policy to the HITPC's attention. Perhaps funding research on the optimal time for rotation should be recommended. Baker said that the committee could comment that passwords should be addressed in NIST 800-863. Wes Rishel referred to testimony received 3 or 4 years ago. He observed that drawing a distinction between what is technology and what is policy is a continuing problem in enhancing security. He disagreed with Baker pertaining to a hardline distinction. According to Arien Malec, the NIST passport entropy scheme does not hold up well in practice. There are better ways of addressing risk. McCallie agreed with Malec. Halamka approved of moving to a risk based approach, but wondered how it would be certified against. Baker said that the first recommendation (beginning with continue) covers it. Malec seemed to agree. Baker said that guidance could be developed, but risk management is the responsibility of the implementer. Halamka observed that risks are continually changing. Rishel reiterated that the password issue is of extreme importance to EHR users, who are under great time pressures. What are the levers that the committee can recommend since the password problem is not particularly amenable to certification? Referring to so-called best practices is not advisable because they are not evidence based. According to Baker, 800-863 is the framework with which to influence best

practice. There is research on maximizing effectiveness of passwords. The TSSWG can work with ONC staff on the best ways to express concerns and influence the industry. Halamka restated the recommendation for action: If, in the future, certification for two-factor authentication is called for, the meaning of two-factor will be defined. Secondly, TSSWG, ONC staff and NIST staff will work together on a risk mitigation strategy to be used in place of certification. Baker indicated that she was not opposed to Halamka's restatement. In response to her question, Halamka confirmed that he was suggesting removal of the following: If passwords are used for user authentication, accept only passwords that meet the guessing entropy guidelines set forth in Appendix A of NIST 800-63-2.

Rose observed that no one was necessarily looking to the HITSC or ONC to define the number of days for setting passwords. The focus should be on certification. Halamka asked whether anyone objected to the approval of his restatement of the TSSWG authentication recommendations. Hearing none, he declared them approved and said that a transmittal letter could go forward.

Action item #2: The HITSC approved the recommendations on authentication:

- **To strengthen the authentication currently certified in EHR technology, the TSSWG recommends adding the following criteria: continuously protect the integrity and confidentiality of information used to authenticate users, using the standard specified in §170.210(a)(1) of the 2014 Edition EHR Standards, Implementation Specifications, and Certification Criteria**
- **To enable EHR technology to be certified for having implemented multi-factor authentication, the TSSWG recommends adding the following certification criterion: restrict access to the system, or to one or more individual functions within the system (e.g., prescribing controlled substances), to only those individuals who have presented at least two of the following three forms of authentication -- knowledge of a secret (e.g., password), possession of a physical object (e.g., hard token or smartcard), or a biometric (e.g., fingerprint)**
- **Support the NIST effort to revamp NIST Special Publication 800-63-2 (Electronic Authentication Guideline); closely follow the move from LOA to componentized trust; and recommend appropriate identity-proofing for query-based access**
- **Consider Data Segmentation for Privacy (DS4P) for authorizing access to behavioral data (TSSWG will address later in the work plan)**
- **Track development and piloting of User Managed Access (UMA) profile of OAuth 2.0 as potential standard for consumer consent**

Standards and Interoperability (S&I) Framework Updates: Prescription Drug Monitoring Program (PDMP)

Initiative Coordinator Jonathan Coleman and Jinhee Lee, SAMHSA, gave a slide presentation on PDMP. Lee began with slides describing well-known trends in prevalence of prescription drug use and overdose. They described the White House Prescription Drug Abuse Prevention Plan, which focuses on education, PDMPs, proper medication disposal and enforcement. PDMPs are state-run databases that collect information on controlled substances dispensed by pharmacies. Authorized users can query PDMPs through portals to determine appropriateness of prescriptions for a particular patient. The goal of the S&I Framework project is to integrate query within HIT systems to streamline PDMP data to health care professionals. But there are challenges. Health care workers are burdened by separate logins and separated workflow. Complex data workflows involve HIEs, PDMP hubs, pharmacy networks, and HIT systems. PDMP data structures are based upon existing NIEM architectures for PDMP-to-PDMP data sharing and are not typically natively supported by EHR systems. There are no widely adopted standards

for the flow of data from a PDMP to a HIT system. A technical community comprised of representatives from PDMPs, pharmacies, and EHRs reviewed technical architecture across actors and system functions, and provided recommendations. The goal is to integrate use of the PDMP with the EHR. Pilot programs are being conducted in six states. The pilots are identifying gaps in standards and their mitigation. This information will be used to update the implementation guide. For information: http://wiki.siframework.org/PDMP+%26+Health+IT+Integration+Homepage

Q and A

Halamka asked White about the S&I Framework and the many implementation guides that the HITSC has yet to see. They likely involve standards that the committee has discussed, for instance, patient identification and matching. How does the PDMP project solve that one? White indicated that it may fall under the next agenda item.

McCallie expressed dismay that nothing on FHIR and smart-style plug ins is being considered as a potentially simpler solution. He urged their consideration. Coleman explained that due to financial constrains in states, the group decided to focus on standards currently used by PDMPs. More advanced technology can be considered at a later time. McCallie went on to say that the integration with physician work flow would be difficult and brittle with the current standards. Plug-ins with FHIR could solve the problem. Coleman indicated that McCallie's suggestion is consistent with the approach being used. Multiple systems can use the interface. There are remaining concerns regarding security involving patient matching. Some of the pilot projects are using pick lists. McCallie observed that they may be using web services and APIs in different ways. He suggested consideration by the Architecture, Services and APIs Workgroup, which he chairs. Arien Malec, who co-chairs that workgroup, said that PDMP could serve as a potential use case. Coleman said that the goal is to be synchronous. Halamka told Coleman that the HITSC members can provide useful expertize: The pick list is not a good idea. Rishel observed that experience in rolling out standards demonstrates that new standards have a significant impact upon work flow. He wondered about the current status of ASAP. What is the experience to predict how it will scale up? In response to a question about stakeholder representation, Coleman, saying that there is participation from care delivery organizations, offered to send the participant roster to Rishel. Further probing suggested that few, if any, direct users, such as clinicians, were involved in the project. Halamka wondered about the application of the standards readiness scheme developed by Baker and her group to these standards. Lee pointed out that some of the pilots are SAMHSA grantees and are providers of care. Halamka summarized, saying that he applauded the progress with PDMPs, but the project should look for experience with easier solutions.

Standards and Technology Updates

Steve Posnack, ONC, noted the tension between what needs to be done immediately for PDMPs to work better versus preparing for the future. He went on to present these two interdisciplinary questions as the rationale for convening two new task forces:

- S&I Framework: In what ways can ONC evolve the S&I Framework to support current industry needs and those anticipated by the 3, 6, and 10-year milestones included in the interoperability roadmap? Final recommendations are due March 2015.
- Data Provenance: Given the community-developed S&I Data Provenance use case, what first step in the area of data provenance standardization would be the most broadly applicable and immediately useful to the industry? Final recommendations are due January 27.

Moving to another topic, Posnack described the outcome of the certification open test method pilot. The goal was to design new test methods through an open community-led, development process.

Stakeholders selected two certification criteria from the 2014 Edition to focus on during the pilot—E-prescribing and CDS. A workgroup for each was established. There were more than 100 participants initially. Stakeholders suggested that the test method templates for the criteria and drafted test method content for each of the two criteria. Final stakeholder-driven test procedures were released. However, the output of the pilot was not significant. New test procedures did not significantly differ from current or original ones. Participants indicated that they preferred to react to test procedures rather than create new ones. They appreciated the transparency and requested that such a transparent approach be put in place with longer public comment periods. They expressed a desire for eRx to be scenario based.

Q and A

Halamka noted that although stakeholders may not be able to write scripts, they can react to scripts designed by others.

Referring to plans for the formation of a data provenance task force, McCallie noted that the question defined a specific use case. A task force could be formed with representatives from several of the existing workgroups. Halamka questioned the reasonableness of expecting recommendations by January 27, which implies meeting over the holidays. Posnack responded that only two or three meetings would be required. The January deadline is driven by fiscal year budged considerations and planning. Halamka announced that the HITSC Steering Committee will consider the request. Gallagher reported that data provenance is an item on the TSSWG workplan. However, the workplan does not include a specific question. And the item was scheduled to be taken up later in 2015.

Malec and Stan Huff volunteered for the Framework Task Force. Halamka observed that there is great interest in evaluating and making changes in the Framework. The task force structure is intended to deal with relatively narrow questions. Learning will occur in process.

Public Comment: None

SUMMARY OF ACTION ITEMS:

Action item #1: The summary of the November 2014 meeting was accepted as circulated.

Action item #2: Recommendations on authentication (identity management) standards were adopted for forwarding to ONC.

Meeting Materials:

- Agenda
- Summary of November 2014 meeting
- Meeting presentation slides and reports

Meeting Attendance					
Name	**12/10/14**	**11/18/14**	**10/15/14**	**09/10/14**	**08/20/14**
Andrew Wiesenthal	X				X
Anne Castro	X	X		X	
Anne LeMaistre	X	X			X
Arien Malec	X	X		X	X
C. Martin Harris	X	X		X	
Charles H. Romine					
Christopher Ross				X	X
David McCallie, Jr.	X	X		X	X
Dixie B. Baker	X	X		X	X
Elizabeth Johnson	X	X		X	X
Eric Rose	X	X		X	X
Floyd Eisenberg	X	X			
James Ferguson	X			X	X
Jeremy Delinsky		X			
John Halamka	X	X		X	X
John F. Derr	X	X		X	X
Jon White	X				
Jonathan B. Perlin					X
Keith J. Figlioli	X			X	
Kim Nolen	X	X		X	X

Leslie Kelly Hall	X	X		X	X
Lisa Gallagher	X	X		X	X
Lorraine Doo	X	X		X	X
Nancy J. Orvis				X	
Rebecca D. Kush		X		X	X
Sharon F. Terry				X	X
Stanley M. Huff	X	X		X	X
Steve Brown	X			X	
Wes Rishel	X	X			X
Total Attendees	**22**	**20**	**1**	**22**	**21**