Collaboration of the Health Information Technology Policy and Standards Committees

Final Summary of the October 5, 2016, Joint Meeting

KEY TOPICS

Call to Order

Michelle Consolazio, U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC), welcomed participants to the Health Information Technology Policy Committee (HITPC) and Health Information Technology Standards Committee (HITSC) joint meeting. She reminded the group that it was a Federal Advisory Committee Act (FACA) meeting being conducted with two opportunities for public comment (limited to 3 minutes per person) and that a transcript will be posted on the ONC website. She called the roll and told members to identify themselves for the transcript before speaking.

Review of Agenda

HITPC Co-chairperson Kathleen Blake noted the importance of each of the agenda items. The agenda was distributed in advance of the meeting. She asked for a motion to approve the summary of the September 13, 2016, meeting as circulated with the meeting materials. A motion was made and seconded. The summary was approved unanimously by voice vote. (A correction of a name submitted by a member was announced and accepted by Consolazio.)

> **Action item #1: The summary of the September 13, 2016, joint meeting was approved unanimously by voice vote.**

Health IT Playbook Overview

Lauren Richie, ONC, described the online, dynamic and interactive playbook of provider-level tools and resources with feedback features. Available to anyone, it is intended to serve these audiences:

- Care teams in small and medium ambulatory practices, particularly those serving underserved areas
- Providers who have not adopted or are not using certified health IT
- PCPs, specialists, PAs, NPs, RNs, and LTPAC providers

The first section, Patient Engagement, was described at the previous meeting. Topics covered in the second section are:

- Electronic health records
- Certified health IT
- Health information exchange
- Patient engagement
- Value-based care
- Privacy and security
- Quality and patient safety
- Care settings

- Population and public health
- Specialists
- Transformation support

Richie demonstrated a navigation of the *HIT Playbook*. Staff invites feedback. Visit https://www.healthit.gov/playbook/

Q&A

HITSC Co-chairperson Arien Malec praised the *Playbook*, saying that it is an excellent resource. Eric Rose informed the staff that the site contains many broken links. Rose wondered about any plans for how to deal with one's specific vendor. Richie said that this is the first release; feedback will be used to design future releases. Staff will work with professional associations. Vindell Washington, ONC, requested suggestions for what would be useful regarding working with specific vendors.

Josh Mandel asked about the plans for updating the *Playbook*. Richie referred to an early 2017 update. Periodic updates will be made as needed, for example, when a new rule is published.

Patricia Sengstack said that the content assumes that the provider has all of the resources to implement the *Playbook*. The *Playbook* should delineate implementation steps.

Leslie Kelly Hall noted that staff did a good job of getting and using input. She requested a section on open APIs. Richie said that there is a section on APIs; perhaps it will be expanded in the future.

Karen van Caulil asked about a dissemination plan. Richie talked about a public webinar and use of listservs and stakeholder engagement contacts. Although the webinar was not recorded, staff plans to add a voice-over guided introduction.

Anjum Khurshid asked about integration of patient consent with work flow. Richie responded that the integration is covered in the patient engagement section. Khurshid said that the topic should also be referenced in the IT section.

HITPC Co-chairperson Paul Tang praised the *Playbook*, saying that it is exceptionally accessible. The information is relevant to the Medicare and CHIP Reauthorization Act (MACRA). The hearings on health information exchange revealed that providers had to reach out to other organizations to set up providers with whom to exchange. Providers do need information on working with their specific vendors. Malec said that the Centers for Medicare & Medicaid Services (CMS) has made funds available for education for MACRA implementation.

Someone suggested allocating a space for vendors to add commentary about their products. Floyd Eisenberg observed that the glossary is very good. Eisenberg suggested adding information on how consumers can get involved. Eisenberg noted a reference to PSA, which is not defined. He acknowledged that he did not know what PSA is. Richie informed him that PSA stands for public service announcement.

Donna Cryer said that the Consumer Task Force recommended the inclusion of information on patient consent in the patient engagement section. Kelly Hall suggested the use of communication channels that were established for Part D education. A member suggested having a space to add information on specialty association resources.

Aaron Miri wanted information and guidance on medical devices. Blake asked for coordination with CMS efforts in developing a tool to assist physicians with MACRA value payments.

Lorraine Doo reported that CMS has convened focus groups with providers on information dissemination. A few small providers mentioned their difficulty in reviewing contracts due to the time

required. ONC needs to have a plan for testing ongoing use. Richie said that ONC also used focus groups to design the *Playbook*. A staff person assured members that there is close coordination between ONC and CMS.

EHR Contract Guide

Elise Anthony and Karson Mahler, ONC, showed slides, demonstrated the *Guide* site, and explained that the 2013 *Guide* has been updated and released. It was prepared for ONC by private sector attorneys who have extensive experience negotiating EHR contracts. The *Guide* is intended to serve different audiences. Anthony cautioned that it should not be construed as legal advice and does not address all possible issues. It may help health IT purchasers to:

- Understand the "fine print"
- Consider contract provisions that impact whether the technology they are contracting for will meet their needs and expectations
- Ask the right questions when selecting an EHR and better communicate their requirements to potential vendors
- Consider and manage expectations and offer a framework for negotiating reasonable contract terms that reflect best practice contracting principles

Part A focuses on planning. It describes:

- Types of EHR products and service models
- Researching and comparing EHR products and vendors
- Identifying and prioritizing technical and operational requirements
- Understanding certification and regulatory requirements
- Procurement strategy, planning and resourcing

Part B focuses on the negotiation and contracting phase of acquiring an EHR. It describes strategies and recommendations for negotiating best practice EHR contract terms; addresses the practical issues important to providers; and illustrates how legal issues might be addressed in a contract by providing example contract language.

Areas covered in Part B are:

- EHR safety and security
- System performance
- Data rights
- Interoperability and integration
- Intellectual property issues
- Managing risks and liability
- Dispute resolution
- Switching EHRs

Q&A

Tang said that vendors typically wait until the last minute to offer contracts. Purchasers need advice in dealing with vendors, such as a set of questions to ask before signing a contract.

Blake referred to safety and security and her experience in contracting for educational services. It is very difficult for purchasers to know what controls are in place and maintained, such as vendor audits, reporting cycles, and a primary responsible person. It ends up being everyone's responsibility. Patients

believe that safety and security are their providers' responsibilities. Blake suggested the inclusion of a checklist with the recommended frequency of audits and reports.

Malec observed that the authors of the *Guide* seem to have decided to present several very strict and narrow interpretations, for example, regarding data use and ownership rights. The *Guide* may not be sufficiently sensitive to different types of technologies. Many technology models facilitate data sharing with patients and between providers: Why did staff pick one point on the entire spectrum and decide to present very specific recommendation on certain topics? Mahler replied that the *Guide* does not take a specific position on granting rights. The approach is that, as custodian, the provider should be in charge of how much access to grant. There are many considerations to take into account. Malec said that he will send suggestions for specific language to use to resolve his concerns.

Mandel commented that although its scope and depth are impressive, the *Guide* will probably be used primarily by larger organizations: What about giving a list of standard functions for vendors to use to indicate what they provide? Anthony reported that staff strove for a balance between suggesting resources and offering a model contract. Mahler added that provider organizations should add information to the *Guide* for their specific audiences.

Noting that the meeting was running behind the allocated times for agenda items, Tang asked members and staff to be brief. David Kotz asked about safety and security, noting that EHR contractors often impose gag orders: What does the *Guide* do to push vendors to be more open? Anthony replied that providers can play an important role in advocating for transparency during the contracting process. The certification process deals with several transparency factors.

A member talked about the need for a helpful list of functionalities for which providers should look. Another member said that there are three important issues: (1) a gag rule is against public policy; (2) understanding the cost of data exchange; and (3) continuity of services.

Wanmei Ou pointed out that multiple contracts are typically required to implement an EHR. Providers need information on how to tackle these multiple contracts. Another member said that information on the revenue cycle should be included, and security certification should be maintained during the contract.

Kyle Meadows declared that the next iteration should go deeper into health information exchange. Kelly Hall referred to APIs and apps endorsed by providers. Overly specific contracts should be avoided because they add to the current confusion.

Carolyn Petersen referred to intellectual rights and patient-generated health data (PGHD), saying that the topic is included in the *Playbook,* but not in the *Guide*. Although Aaron Miri voiced approval of the reference to the NIST framework, he noted that missing elements are costs of interoperability, consolidation across providers, and hosting versus on-premises. Mahler reminded the members that the presentation was an overview. If one actually reads the *Guide*, he/she will find that many of the topics raised during Q&A have been covered. Anthony requested members' help in informing potential users of the *Guide*. Tang said that the Q&A suggests areas for future HITPC consideration.

Remarks

A change was made in the order of the agenda to recognize Washington. Washington thanked the members for their work. The purpose of the *Playbook* and the *Guide* is to give providers resources for their empowerment. Not all providers realize that the purchase of an EHR does not result in filling all technology needs. He referred to several recently announced awards to support interoperability and

sharing information on cyber threats. Officials are working on making a smooth transition to the next administration.

Zika Update

James Daniel, ONC, showed slides and described how health IT is being used to respond to Zika and, more generally, to develop an all-hazards approach. Building on learnings from the responses to Ebola and Middle East Respiratory Syndrome (MERS), algorithms, vocabulary sets, order sets, and vendor outreach have been used. He showed a flow chart depicting the guidance for clinicians published in a recent *Morbidity and Mortality Weekly Review*. Algorithms have been used to advise IT developers on the incorporation of Zika-related order sets. However, the local variation challenge introduced complexity-mapping variations that may prohibit an automated push of order sets. Nevertheless, the current documentation (i.e., vocabulary standards, etc.) on order sets as related to the clinical guidance documents remains useful. Daniel's slides contained information and links to many algorithms for developers.

In describing next steps, Daniel said that clinical decision support modules on the Zika work flow are still built at the local level. Agencies are working on the capture of pregnancy status and other data related to Zika case management, including linkage to the U.S. Zika Pregnancy Registry. More states are developing capacity for immunoglobulin M and plaque reduction neutralization antibody testing, and additional testing in commercial laboratories is underway.

Regarding the establishment of an all-hazards approach, clinical decision support and structured data capture are key factors. Collecting the right information will require data on:

- A patient profile and patient characteristics
- Exposure
- Symptoms
- Physical findings
- Assessment and plans

In order to establish the right building blocks, one must consider that for a given situation the order of the building blocks may change, and certain blocks may be of less importance. The objective is to determine the right blocks and where they belong. Other considerations may include order and work flow optimization (i.e. move individuals out of the queue, drive reflective questioning). The Zika virus questionnaire uses Centers for Disease Control and Prevention (CDC) links for travel history and testing recommendations. The clinical quality framework uses FHIR clinical reasoning. Data extraction is based on FHIR resources with standard terminology for measures, measure reports, and clinical decision support.

Q&A

Rose inquired about the use of the Electronic Directory of Order Standards (eDOS). Daniel responded that eDOS is being used in data entry for pregnancy status. A representative from the Association of Public Health Labs is working on the project. Guidance will be given back to public health departments.

Eisenberg, who consulted on the project, added that collaboration with CDC is very productive. Kelly Hall asked what is being done to connect consumers who self-test for pregnancy, thereby generating patient health data for input into the pregnancy registry. Acknowledging that he did not have detailed information to answer the question, Daniel assured Kelly Hall that CDC staff is working on that process.

Blake reported that she is encouraged by recent reports on progress in immunization development. Since immunization may soon be available, the use of that data should be anticipated. Daniel agreed, noting that immunization information systems are well developed. Blake said that these data could be used in assessing the early effects of immunization.

Larry Wolf acknowledged the evidence for a learning health system on the technology side and asked about the opportunity for developing the science of Zika. Daniel said that the first step is to establish a framework for a vocabulary.

Rajesh Dash observed that lab efforts had recently been reduced and wondered whether ONC is properly equipped with resources for an all-hazards approach, which could be applied to laboratory orders across many diseases and conditions. Daniel explained that several organizations, particularly, CDC and labs, are working with ONC. Lab interoperability is a consideration.

Andy Wiesenthal reported that the Robert Wood Johnson Foundation (RWJF) is funding a project on governance and infrastructure for routine bi-directional exchange with public health agencies. It builds on other efforts. Visit http://phii.org/digital-bridge. Daniel said that the daily alignment of health care and public health is essential.

Chesley Richards, CDC, interjected that CDC staff is already working on the things commented upon by members. CDC is seeking recommendations on pathways to doing these things.

Public Comment

None

HITPC/HITSC Consumer Task Force Model Privacy Notice (MPN) Update

Task Force Co-chairpersons Donna Cryer and Patty Sengstack, and Margeaux Akazawa, ONC, reported. The MPN is a voluntary, openly available resource to help developers provide transparent notice to consumers about what happens to their data. It is a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users. The 2011 version of the MPN was developed in collaboration with the Federal Trade Commission and focused on personal health records (PHRs), which were the emerging technology at the time. ONC staff wished to modernize the MPN to be a more useful resource for consumers and developers in a market with more varied products that are collecting different digital health information. ONC put out a request for information on March 1, 2016, and sought comment on what information practices health technology developers should disclose to consumers and what language should be used to describe those practices. Thirteen public comments were received from developer organizations representing more than 5,100 members, provider organizations representing more than 200,000 providers, and consumer organizations representing patients and consumers across the country. The comment period closed in April 2016. Staff requested additional comments from the consumer perspective in a second comment period that closed in September. Additional comments from the Consumer Task Force were then sought. Task Force members were given homework, which consisted of responding to questions:

- Is the MPN language clear and are terms understandable to consumers? If not, what suggestions do you have to make the content more consumer-friendly and easier to understand?
- What are consumers' primary concerns with privacy and security of their data when using health apps or devices? Are there any concerns that are missing from this draft notice template?
- How can we simplify the notice?
- Does the draft content provide enough detail on privacy and security terms for consumers to understand? If not, what additional details or definitions should be included?

The Task Force reported that:

- Overall, members felt the MPN was clear, simple, and well done.
- Members identified certain terms and items that could use additional definition, plain-language replacements, or a hyperlink to additional information.
- Members suggested that the tone of the notice could be more conversational.
- Members recommended a drop–down format that would allow for consumers who wish to learn more to get more details while keeping the notice simple.
- Members discussed how clear the two categories of data, identifiable versus de-identifiable/aggregate, and the terms privacy versus security would be to consumers. Members recommend not only indicate the difference between the terms but what happens in certain scenarios, consequences of those scenarios, and how a consumer can get more information.

Q&A

In response to several overlapping questions, Cryer said that this model is voluntary. Some products may continue to use long and complex notices. Links to longer, legal notices can be provided.

Mike Lipinski, ONC, interjected that staff is still gathering feedback from stakeholders, such as developers. It may be possible for covered entities to make use of the model.

Malec recalled that, although active and engaged companies adopted the previous version of the MPN, not everyone did: How will staff ensure that the MPN will get in the hands of all potential users? Cryer referred to the diversity of the task force membership. Targeted outreach to the legal community may be useful. Various suggestions were called out by members.

Tang referred to the *Contract Guide*, saying that questions to ask should be included in the MPN. Akazawa said that the MPN is also an educational tool. Blake said that a balance of depth of content and usability is important. Terrence O'Malley suggested having a list of the data that the app will collect and retain.

Information Sharing and Analysis Organizations (ISAOs) Update

Nickol Todd, Assistant Secretary for Preparedness and Response (ASPR), and Rose-Marie Nsahlai, ONC, reported. In accordance with one of its commitments outlined in the *Interoperability Roadmap,* ONC staff is coordinating with the ASPR on priority issues related to cybersecurity for critical public health infrastructure. Criminal cyber-attacks against health care organizations are up 125% compared to 5 years ago, replacing employee negligence and lost or stolen laptops as the top cause of health care data breaches. The average consolidated total cost of a data breach was $3.8 million, a 23% increase from 2013 to 2015. For the past 3 years, ONC has worked with ASPR, the Office of the Assistant Secretary for Administration, the Office of the Chief Information Officer's Office of Information Security, and the Office of Security and Strategic Information's Cyber Threat Intelligence Program to develop the means to facilitate cyber threat information sharing across the health care and public health sector.

The Cybersecurity Information Sharing Act (CISA) outlines new requirements for cyber threat information sharing. Section 405(c) establishes the Health Care Industry Cybersecurity Task Force. Section 405 (c) (1) (D) and 405 (c) (1) (E) outline the task force's duties regarding recommendations for cybersecurity threat information dissemination. The task force was asked to recommend a plan for the federal government and health care and public health sector stakeholders to share actionable cyber threat indicators and defensive measures.

Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity (February 19, 2013), defined HHS's information sharing role with respect to cybersecurity threats. It calls on HHS to participate with other sector-specific agencies and the Department of Homeland Security (DHS) to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." On February 13, 2015, the President signed EO 13691, Promoting Private Sector Cybersecurity Information Sharing, which encourages the development of ISAOs to serve as focal points for cybersecurity collaboration within the private sector and between the private sector and government. This broadens existing terminology related to "information sharing and analysis centers" (ISACs), by identifying ISACs as one type of organization among other types of ISAOs. Per EO 13691, all ISACs are ISAOs. ISAOs do not need to be organized by sector; they may instead be organized by geography, type of threat, or professional affiliation. ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest. They provide a partnership structure for DHS and the government to connect with the private sector. The National Cybersecurity and Communications Integration Center can enter into information sharing agreements with ISAOs for increased collaboration between ISAOs and the federal government.

ONC and ASPR have each recently awarded a cooperative agreement to expand the capacity of an existing ISAO to share cyber threat information (CTI) bi-directionally between HHS and the sector. The purpose of the ONC agreement is to:

- Build internal resources to serve as a single ISAO
- Expand its current membership base
- Focus more of its business and resources on CTI sharing;
- Create a lower entry cost for smaller health care and public health sector organizations that wish to join an ISAO
- Eventually provide some level of free CTI sharing services to the entire sector

The ASPR awardee will:

- Provide resources to focus the awardee's efforts on cybersecurity information sharing
- Broaden access to cybersecurity information for health care organizations of smaller sizes
- Reduce the costs to organizations receiving cyber threat information

Both cooperative agreements were awarded to the National Health Information Sharing and Analysis Center. A previously awarded planning grant found that:

- Perceived effectiveness of cyber threat information sharing was low
- Organizations vary between potential sensitivity to price (preferring free options) and favoring more "reputable" sources
- There is generally low awareness, appreciation, and/or understanding amongst the respondents of common or popular cyber threat information sharing standards such as STIX, TAXII, and TLP
- Automation is highly preferred amongst all respondents
- 93% of respondents would like an ACTIVE ISAO that provides threat intelligence, analysis, and education ,and not simply a platform to share
- Operationalize sharing as part of incidence response

These types of information were shared:

- Malicious sites
- Threat actors, objectives

- Threat indicators
- TTPs, observables
- Courses of action
- Exploit targets
- Denial of service attacks
- Malicious emails
- Software vulnerabilities
- Malicious software
- Analysis and risk mitigation
- Incident response

For the FAQ and additional information on this Funding Opportunity Announcement, go to https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/opportunity-sharing-information-cyber-attacks

Q&A

Malec referred to a recent Government Accountability Office (GAO) report that criticized the Office for Civil Rights (OCR) for not sharing information with CMS on the meaningful use program. Malec seemed to question the appropriateness of such sharing across agencies with different missions. Given the variety of regulatory levels available to HHS, he wondered about an approach to segregation of information to both promote a learning health system and protect users who are concerned with sharing their information. Nsahlai said that the information shared is not PHI and is autotomized and aggregated. OCR was not invited to participate in the discussion because of concern about potential regulation. Malec asked about the participation of the Department of Defense and other federal agencies that provide health services. Todd said that these federal agencies are involved in sharing. Nsahlai and Todd agreed to gather more information on these topics and inform the members.

Wolf urged staff to reach out to small and medium-size providers. Mostly, large organizations are the ones that are doing something.

Kotz asked about the Cyber Health Task Force, formed by the FBI, which seems to serve a similar purpose. He said that he had recently been invited to join. Nsahlai said that HHS agencies coordinate directly with the FBI.

Dale Nordenberg asked how the FACAs can be involved with these efforts. Cyber is a health care and public health challenge, not simply an IT challenge. Standards for data exchange are being recommended, an area in which the FACAs have expertise. Nsahlai said that the DHS is running the standards for data exchange initiative. Todd indicated that staff wants feedback on gaps and products from the new awards. Regarding the question about the need for a FACA cyber security task force, Malec said that such a group had been formed and made recommendations some time ago. He questioned the need for one at this time.

Miri asked about the possibility of fair harbor being extended to providers. He also wondered which HHS body or position will be ultimately responsible. Nsahlai responded that she was not aware of any action on liability protections although they were discussed. Nsahlai agreed to follow up with an email when she obtains more information. Todd said the authority for the ultimate coordination within the government has been deferred to the next administration.

ONC Office of Standards and Technology Update

Steve Posnack, ONC, quickly reported the announcement of seven recipients of two cooperative agreement programs to design standards-based solutions that facilitate the exchange of health information. The awardees for the High Impact Pilot programs are:

1. The Heartland Pilot is a partnership between The Health Collaborative and the Strategic Health Information Exchange Collaborative to use existing standards to advance a "network of networks" model as part of a patient-centered data model pilot project.
2. The Lantana Consulting Group will create a new standard for electronic pharmacist care plans, which have not been included in the Interoperability Standards Advisory. The project pilot will use health IT standards to integrate pharmacist care plans into coordination efforts for patient care across the health continuum.
3. A collaborative project between RxREVU, a Denver-based prescription intelligence company, and the Banner Health System plans to leverage patient-specific data shared via FHIR to reduce overall prescription drug spending, provide useful information on patient medication adherence, and operationalize organizational best practices.
4. Clinicians at the University of Utah's vascular surgery service who use common EHR platforms will share information through a novel closed-loop surgical referrals dashboard application. This app will be designed to integrate with commercially available EHRs using SMART.

The awardees for the Standards Exploration Awards are:

1. Arkansas Office of Health Information will implement interoperable, bi-directional health information exchange with behavioral health providers.
2. The Cincinnati Children's Hospital Medical Center project will explore the cost efficiencies of integrating health care and clinical research systems with the medical center's EHR.
3. Sysbiochem, in collaboration with Boston Children's Hospital, Intermountain Healthcare, and Massachusetts General Hospital, will develop services to facilitate the integrated flow of data between an EHR, laboratory informatics system, and an analytic application to help clinicians coordinate care for breast cancer patients.

Public Comment

Denise Anderson, NH-ISAC, commented via the chat function of the web meeting site. "We are plugged in with the FBI healthcare group already. Also to clarify we have an embedded presence on the NCCIC floor as well as the NICC. I also serve as Chair of WG2 of the ISAO Standards Organization so we are plugged in there as well and the ISACs are providing a lot of input into the SO. Finally I also serve as Chair of the National Council of ISACs so we are very plugged in to all of the other ISACs."

"As far as the concern with sharing, ISACs provide anonymity for the organizations that share. CISA provides liability protections to those who share via an ISAO or ISAC."

Next Meeting:

A joint virtual meeting will be scheduled for November.

SUMMARY OF ACTION ITEMS

Action item #1: The summary of the September 13, 2016, joint meeting was approved unanimously by voice vote.

Meeting Materials

- Agenda
- Summary of the September 13, 2016, joint meeting
- Presentations and reports slides