HIT Policy and Standards Committees
FINAL
Summary of the March 10, 2016, Joint Virtual Meeting

KEY TOPICS

Call to Order

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

Remarks and Announcements

Deputy National Coordinator P. Jon White introduced Kathleen Blake, who was recently elevated to co-chair of the HITPC, and ONC Principal Deputy Coordinator Vindell Washington. Washington's appointment was announced at the January meeting.

Review of Agenda

Co-chair Paul Tang mentioned each item on the previously distributed agenda. Blake thanked ONC. HITSC Co-chair Arien Malec introduced and welcomed new members Dale Nordenberg, Novasano Health and Science; and Kevin Johnson, Vanderbilt University Medical Center. Tang asked for a motion to accept the summary of the January 2016 meeting as circulated. A motion was made and seconded. The motion was approved unanimously by voice vote.

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

Precision Medicine Initiative (PMI) Update

White described recent PMI events and activities. The National Institutes of Health (NIH) announced an award to Vanderbilt University in collaboration with Verily (formerly Google Life Sciences) to launch the first phase of the PMI Cohort, which will lay the foundation for a national community of 1 million or more U.S. volunteers who will partner with researchers, share data, and engage in research to transform understanding of health and disease through precision medicine. In collaboration with ONC, NIH will coordinate Sync for Science pilots through an open standards development process with several electronic health record (EHR) developers. The lessons learned will inform efforts to scale individual data access and donation for precision medicine research and could be used to support implementation of consumer-mediated data access across the health care industry. For information, visit the PMI Data Security Policy Principles and Framework: https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/PMI_Security_Principles_and_Framework_FINAL_022516.pdf. To make a public comment, go to https://www.whitehouse.gov/webform/precision-medicineinitiative-draft-data-security-policy-principles-and-framework.

ONC's role in PMI includes the following:

- Accelerate innovative collaboration around pilots and testing of standards that support health IT interoperability for research
- Adopt policies and standards to support privacy and security of cohort participant data
- Advance standards that support a participant-driven approach to patient data contribution

Sync for Science pilots will test promising approaches for individual participants to contribute their EHR data to the PMI cohort and provide data and experience to decide how to extend application program interface (API)-based contribution of data to all or a subset of individually enrolling participants.

Precision Medicine Task Force Co-chair Leslie Kelly Hall expressed her enthusiasm with the recent summit at which President Obama demonstrated his understanding of the importance of PMI. Malec, who also participated in the summit, agreed. Kelly Hall explained that the task force was charged to provide a forum on how ONC can support interoperability challenges for federal partners and the broader precision medicine community and to be a coordinated, aligned approach to PMI health IT standards. PMI's partners are NIH, the Food and Drug Administration (FDA), the National Cancer Institute (NCI), the U.S. Department of Defense (DoD), the U.S. Department of Veterans Affairs (VA), Allscripts Healthcare Solutions, Inc., athenahealth, Inc., Cerner Corporation, drchrono, Epic Systems Corporation, and McKesson Corporation. The PMI is a collaboration with industry to pilot the use of standards to enable data donation, allow patient access through APIs with standards (e.g., Fast Healthcare Interoperability Resources [FHIR], OAuth 2.0), and identify standards for use cases to support interoperability. The task force will focus on data types critical to PMI and prioritize piloting the exchange of those data. This year the task force members listened to invited presentations from NCI, FDA, ONC, and NIH. Efforts in the coming months will include the following:

- Computable consent
- Sync for Science
- The PMI for oncology
- precisionFDA
- VA's Million Veteran Program
- Lab data interoperability and patient access
- Patient rights and ownership of genomic pattern data
- Demographic data and how to improve structured data capture and transfer

Recommendations will be submitted to the HITSC for action in June.

Discussion

John Scott requested that the name of the DoD representative be added to slide 3. Regarding data flows, he wondered whether anyone is prototyping a personal health record (PHR) that allows a patient to download all of his or her EHR data and then share them. Kelly Hall agreed to add the name of the DoD representative. She indicated that the task force is not concentrating on any specific mechanism for sharing and contributing data. The focus is more on the means than on the type. Malec interjected that Sync for Science will test a capability for capturing and forwarding data, building upon work with FHIR and OAuth. He said that it would be helpful if the VA and DoD portals supported such a capability.

Tang asked members to use the hand-raising tool to reduce confusion and avoid having multiple speakers at the same time. Consolazio helped members who were unable to use the tool. In response to a question from David Kotz, White explained that the research cohort is primarily an NIH responsibility. Karen DeSalvo and he are ex officio members of an NIH PMI advisory group. A coordinating center will be formed by a contractor yet to be selected.

Rich Elmore commented that PMI is a unique opportunity to align patient identity proofing in a distributed environment. He wondered whether the task force will address standards for queries to a distributed research data base. Kelly Hall responded that the task force is in the early stages of understanding the architecture.

Blake expressed appreciation for the federal agency cooperation. She said that PMI should build on several ongoing cross-agency efforts to create large cohort databases, such as the FDA Sentinel Initiative, the FDA Medical Device Epidemiology Network Initiative, and PatientsLikeMe.

Scott asked about patient consent and what information and findings will be shared with patients and their providers: Are there best practices or recommendations for dealing with the entirety of the data generated by a genetic study? Kelly Hall assured him that work on standards for doing that is underway. White said that such issues will most likely be addressed by the awardees. Johnson said that his organization's grant, which was awarded very quickly, will address the standards for other awardees to use. The NIH Big Data to Knowledge initiative is relevant to this topic.

Saying that his research focus is on privacy and security, Kotz suggested that the committees consider going beyond clinical data to think about exposomics data. Andrew Wiesenthal pointed out that plenty of data can be assembled from publicly available records and datasets that do not require individual consent. Consideration should be given to the policy issues involved. Floyd Eisenberg observed that the PMI work could also be applied to quality measurement of outcomes.

Wes Richel acknowledged that exposomics was for him a new concept. He said that the committees should be concerned about the rigor of data collected from nonclinical sources. There is risk of over-specifying the outside world. Specific pieces of external data may correlate well with medical data, but those data may not be structured to health care needs.

ONC Updates

Steve Posnack described ONC's reshaping of its standards and technology approach, saying that there are four focus areas: standards coordination, testing utilities, pilots, and innovation, all combined in a tech lab. The reshaping is based in part on recommendations from the HITSC. Staff will be working with Health Level Seven International on the Consolidated Clinical Document Architecture, feedback loops, and a provider directory, among other projects. The comment period for the 2016 standards advisory is still open. A task force will be convened for input on the 2017 advisory. ONC has published two new challenges to app developers. For information, visit https://www.challenge.gov/challenge/consumer-health-data-aggregator-challenge/ and https://www.challenge.gov/challenge/provider-user-experience-challenge/. A funding opportunity announcement for a cooperative agreement was released March 1 for an app discovery marketing opportunity. See http://www.grants.gov/web/grants/view-opportunity.html?oppId=281872. The Interoperability Proving Ground is a mechanism for showcasing ongoing work and filtering information by state. For a snapshot view, see https://www.healthit.gov/techlab/ipg/.

Elise Sweeney Anthony showed slides and gave an overview of the notice of proposed rulemaking "ONC Health IT Certification Program: Enhanced Oversight and Accountability." She emphasized what the rule would not do. It would not establish new certification requirements for health IT developers or providers participating in U.S. Department of Health and Human Services programs. It would not establish a means for ONC to directly test and certify health IT or establish regular or routine auditing of certified health IT by ONC. The ONC-Authorized Certification Bodies (ACB) will continue to test and certify. The rule would enable ONC to directly review certified health IT products and increase ONC oversight of health IT testing bodies, transparency, and accountability by making identifiable

surveillance results of certified health IT publicly available. The proposal would expand ONC's role to encompass the ability to directly review health IT certified under the program and, when necessary, take corrective action, including the suspension and termination of certified health IT. Direct review would be independent of and may be in addition to reviews conducted by ONC-ACBs and would extend beyond the continued conformance of the certified health IT's capabilities to the specific certification criteria and test procedures. Direct review would extend to the interaction of all capabilities within the certified health IT with certified capabilities and the interaction of all capabilities with other products and focus on situations that pose a risk to public health or safety.

According to Sweeney Anthony, the goals are as follows:

- Support greater accountability for health IT developers under the program
- Provide greater confidence that health IT conforms to program requirements
- Permit ONC to work with health IT developers to remedy any identified nonconformities of certified health IT in a timely manner

Sweeney Anthony gave examples of nonconformities that could warrant ONC direct review. If a developer has products certified by two different ONC-ACBs, and if a potential nonconformity with certified capability may extend across all developers' certified health IT, then ONC could step in. Other examples follow:

- Systemic, widespread, or complex issues (e.g., certain fraudulent activities) that could be difficult for ONC-ACB to investigate or address in timely, effective manner
- Risk to public health or safety, such as capabilities (certified or uncertified) of health IT directly contributing to or causing medical errors
- Other exigencies, such as a nonconformity that could compromise the security or protection of patients' health information in accordance with applicable law or lead to inaccurate or incomplete documentation and resulting inappropriate or duplicative care under federal health care programs
- Issues with confidential information or information that cannot be shared with ONC-ACB

Another proposal pertains to the ONC-Accredited Testing Laboratories (ATLs) and would be a means for ONC to have direct oversight of the National Voluntary Laboratory Accreditation Program and ATLs by having them apply to become ONC-ATLs. The proposal is a means for authorizing, retaining, suspending, and revoking ONC-ATL status under the program, similar to current ONC-ACB processes. The goal is to enable ONC to oversee and address testing and certification performance issues throughout the entire continuum of the program in an immediate, direct, precise manner.

Sweeney Anthony went on to talk about an RFI on the public availability of identifiable surveillance results, which would require ONC-ACBs to make identifiable surveillance results publicly available on their websites on a quarterly basis. It is expected that this would enhance transparency and provide valuable, balanced information about the continued performance of certified health IT and surveillance efforts. Staff expects that the prospect of publicly identifiable surveillance results would motivate some health IT developers to improve their maintenance efforts. Additionally, this information could reassure customers and users of certified health IT.

The public comment period for the "ONC Health IT Certification Program: Enhanced Oversight and Accountability" proposed rule is open until 5 p.m., May 2. For review and comment, go to https://federalregister.gov/a/2016-04531. A Microsoft Word version of the proposed rule and a comment template are available at https://www.healthit.gov/policy-researchers-implementers/standards-and-certification-regulations.

ONC is updating the Model Privacy Notice (MPN). The MPN provides a standardized, easy-to-use framework to help developers clearly convey information about privacy and security practices to their users. It is a voluntary, openly available resource for developers and consumers. The 2011 version focused on PHRs, which were the emerging technology at the time. The update will make it applicable to a broad range of consumer health technologies beyond PHRs. For information, visit https://federalregister.gov/a/2016-04239 or https://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice.

Questions and Answers

Tang wondered whether the plans regarding transparency and surveillance could be extended to how well certification was passed. Sweeney Anthony told Tang that he was welcome to submit a comment to that effect. Posnack noted that the certification process results in certification or no certification, not a grade. He mentioned potential challenges of exposing intellectual property. ONC is transitioning the certified product lists to the open Certified Health IT Product List (CHPL), and information on each certification criterion will be available. Tang said that Apple Watch is open to review and, consequently, competition and innovation are enhanced. Health care could benefit from a similar open market process. Posnack said that CHPL must list the task used in user-centered design testing, which will make safety information more readily available.

Observing that the discussion was running longer than scheduled, Consolazio asked members to be brief. Sweeney Anthony announced that an upcoming webinar will provide an opportunity for answering questions. She urged members to made public comments.

Eric Rose said that he expects that the volume of requests will strain ONC resources. Reviews by competing developers must be fair and consistent. He agrees that certification should be more transparent; perhaps reports on the certification process could be released with the agreement of vendors. This could be easily implemented and would help providers select products.

Paul Egerman wondered about the application of the review process to open source and self-developed software. Sweeney Anthony repeated that review applies to any certified technology. The proposed rule would allow ONC to step in on any certified technology.

Rishel referred to slide 8 that depicted two paths for corrective action: What is the difference? Sweeney Anthony responded that one is suspension and one is termination. Rishel asked whether the testing criteria for ACBs and ATLs are the same. Sweeney Anthony replied that the accreditation of ACBs will not change under the proposal, but oversight would be expanded to ATLs. Regarding nonconformity or potential nonconformity, if ONC received a report, then staff would investigate to determine whether the information is reliable. The review of the testing labs is separate and different; staff would look at the system and allow developers to explain their processes. Actual testing would not be conducted. Rishel said that in his years of experience of applying methods to compare vendors, he learned that it is very difficult. Vendors will quibble over ratings and exert considerable backlash. He advised Sweeney Anthony to go slowly.

Kelly Hall recommended that the proposed privacy practices consider the future use of APIs and apps. Sweeney Anthony said that she looked forward to receiving that comment. Chris Lehmann asked what would happen to a small provider if her product were suspended. Sweeney Anthony explained that ONC and the Centers for Medicare & Medicaid Services (CMS) have worked together to develop frequently asked questions for a situation in which a product is decertified. ONC's goal is to work with the parties involved to correct the problem. Action would depend on the safety and public health issues affected.

Potential nonconformist concerns could come to ONC's attention in various ways, including via patient safety organizations.

Elmore said that most developers respond rapidly to patient safety issues. The new regulatory process should not slow down developers' responses. He wondered about possible overlapping investigations with other regulatory agencies. Sweeney Anthony said that it is possible for reviews to occur simultaneously. ONC could defer to another agency. ONC's focus is on the product that was certified. She suggested that Elmore submit a written comment.

Gayle Harrell urged that the MPN require plain language as well as languages in addition to English. Sweeney Anthony said that any linguistic competency requirements will depend on the results of public comment.

Update from the Joint API Task Force

Consolazio requested that the co-chairs condense their report to accommodate the extended discussion of the ONC updates. API Task Force Co-chair Meg Marshall told the members that API is a technology that allows one software program to access the services provided by another software program. In its 2015 edition certified EHR technology rule, ONC has included certification criteria for fully functioning APIs to support patient access to health data via view, download, and transmit. However, in discussing this concept in the proposed rule with the FACAs, many members expressed concerns about the privacy compliance and security of APIs. The API Task Force was created to identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in health care and to make recommendations to ONC that will help enable consumers to leverage API technology to access patient data while ensuring the appropriate level of privacy and security protection.

ONC established a 2015 edition criterion at §170.315(g)(7) that requires health IT to demonstrate that it can provide a consumer-facing application access to the Common Clinical Data Set via an API. At this time, the certification criteria only require read-only APIs. The certification criterion is split into three separate individual criterions focused on specific functionality to enable modularity and flexibility in certification. They are patient selection, data category request, and data request.

According to Marshall, third-party application registration is expected to encourage dynamic registration. Registration should not be used as a means to block information sharing via APIs. Dynamic registration means that applications should not be required to preregister (or be approved in advance) with the provider or the module developer before being allowed to access the API. This is supported by the CMS Meaningful Use Stage 3 Final Rule. Two objectives reference the use of APIs: Objective 5, Patient Electronic Access to Health Information; and Objective 6, Coordination of Care Through Patient Engagement. With these objectives, there are four basic actions that patients (or patient-authorized representatives) should be able to take: view their health information, download their health information, transmit their health information to a third party, and access their health information through an API. CMS expects that these actions may be supported by a wide range of system solutions, which may overlap in terms of the software function used to do an action or multiple actions, including facilitating provider-to-provider exchange as well as patient access. CMS proposed for the patient electronic access objective to allow providers to enable API functionality in accordance with the proposed ONC requirements in the 2015 edition proposed rule.

The task force convened two virtual public hearings in January. API Task Force Co-chair Josh Mandel summarized the following points made during the hearings:

- API resources can regulate how, when, and who uses the API.

- APIs provide a well-documented, popular way for organizations to share access to data and services with third parties while maintaining strict security controls.
- Clear and concise documentation is important for open standard APIs.
- API is extremely precise and allows the opportunity for all the right levels of access and security (e.g., data granularity).
- Technical solutions exist for technical problems.
- ONC needs a consensus on best practices to help secure the API.

In addition, the following business and legal considerations were raised:

- Does it matter whether the discloser "owns" the protected health information (PHI)?
- Providers need liability and accountability for data usage and breach, even though Office for Civil Rights (OCR) and ONC fact sheets say that a discloser is not liable for what a receiver does with data so long as the discloser discloses the data properly.

During testimony, consumer representatives demanded more access, patient control, and engagement, saying that choices should be given to patients and that patients are smart enough to make privacy and security choices that are right for them. Systems should account for diverse consumers. Some want to control every decision personally, and some want health information to move where it needs to go without them having to manage that process. Transparent data practices are important for consumers. Protection outside of the Health Insurance Portability and Accountability Act (HIPAA) authority is also important. Although health care organizations support open-standards–based APIs, they are concerned with the identity of the persons accessing their systems.

Mandel referred to a slide and described a generic use case that the task force will use to formulate recommendations.

Discussion

Tang wondered whether the example use case will consider the limitations of the "I agree" screen. Mandel indicated that he wants to understand the existing processes and practices, such as a summary that allows drilling in. The task force will likely make recommendations on that topic.

Egerman pointed out that most users do not read fine print and will blame others when something goes wrong. An API developer can retain PHI because the developer is not governed by HIPAA. The task force's approach does not include policy recommendations. An API developer should automatically be required to be a BA and therefore subject to HIPAA. Patients trust providers to take care of their PHI regardless of what an agreement says. Mandel responded that, on the other hand, patients have the right to access. Marshall interjected that OCR and ONC are providing information on BAs' and others' responsibilities.

Blake talked about the dangers of small-font approvals. She said that she prefers a series of checkboxes, including ones that hold harmless provisions. If an app developer breaches, everyone involved can be sued. Although the plaintiff may not win, the litigation will use up resources. There should be some indemnity, Blake believes.

Saying that consumers are frustrated by restrictions on access and sharing, Scott wondered about the possibility of an ONC seal of approval for PHRs and apps, although he agreed that approval should not be required. Mandel acknowledged that the task force is considering a seal of approval, but from various entities other than ONC. Scott reported that both the VA and DoD have a library of endorsed apps. Mandel responded that endorsements should be available but not required.

Elmore commented on the challenge of identity proofing, saying that requirements vary widely across states and should be as simple as possible. Regarding the use case described on slide 15, he wondered what will happen when the use case breaks down. Mandel replied that identity proofing for patients is not unique to apps. The approval process should begin at the portals and is the same with apps. Elmore said that the level of assurance deserves attention. Malec noted that there is a provider side and a patient side to boundaries. The patient side is not within the purview of ONC. However, some level of protection may be needed. The task force should consider the legitimate reasons for a provider to shut down access, the necessary level of security proofing, fair notice, and liability.

Public Comment

These comments were submitted via the Web meeting chat.

Kotz wrote, "The exposome encompasses the totality of human environmental (i.e., nongenetic) exposures from conception onwards, complementing the genome. It was first proposed by Dr. Christopher Wild, a cancer epidemiologist, in a 2005 article entitled 'Complementing the Genome with an "Exposome": The Outstanding Challenge of Environmental Exposure Measurement in Molecular Epidemiology.' [Wikipedia]"

Dr. Jude Haney, William Carey University, wrote, "Great presentation. This is the point that I was interested in. A lot of rural areas simply cannot afford the highly certified EMR systems and are working with systems that may or may not be up to date on certs. More oversight will directly impact their bottom line. If the larger EMR firms don't work, something out there may be an issue in quality of care." She added, "Also, yes, patient portals in other languages is crucial."

Thompson Boyd 2 wrote, "Expanding on Paul Egerman's comment: What is the provider liability if patient has a bad outcome using a new app? For instance, the patient later finds that the API developer sells the patient's information to a third party? In addition, what if the patient finds that their information is in a 'surprise' location?" He added: "There should also be guidance (education) for the patient, regarding their handling of their personal information (e.g., best practices)."

SUMMARY OF ACTION ITEMS

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

Meeting Materials

- Agenda
- Summary of January 2016 joint meeting
- Presentations and reports slides