Collaboration of the Health IT Policy and Standards Committees

Final Summary of the April 19, 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 Policy Committee (HITPC) and the 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. Members introduced themselves. Consolazio told members to identify themselves for the transcript before speaking.

Remarks and Review of Agenda

ONC National Coordinator Karen DeSalvo reported that the committees' FACA charters have been restructured and approved to accommodate committee co-chairpersons. Previously, the National Coordinator served as HITPC chairperson. The revised structure is intended to contribute to sustainability and ease of transition of leadership. DeSalvo introduced Principal Deputy Coordinator Vindell Washington, who said that he is excited about the agenda of the next few months.

HITPC Co-chairperson Paul Tang thanked DeSalvo. During roll call Tang disclosed that he is now employed by IBM Watson Health. He mentioned the importance of each item on the previously distributed agenda. Tang asked for a motion to accept the summary of the March 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 March 2016 joint meeting was approved unanimously by voice vote.**

Joint HITPC-HITSC Application Programming Interface (API) Task Force Recommendations

HITPC Co-chairperson Kathleen Blake thanked ONC for circulating the meeting materials well in advance of the meeting to ensure that members had the opportunity to be well prepared for discussion. She emphasized that these are draft recommendations. API Task Force Co-chairperson Meg Marshall said that in addition to the 50 presentation slides, the task force will present its final recommendations in June in a document format. After Marshall repeated information from the report at the March meeting about the purpose and scope of the task force and definitions, API Task Force Co-chairperson Josh Mandel showed a slide that described the use case (and four variants) on which the members have agreed to focus:

> App Developer builds an app that can benefit from patient data. App Developer builds support for an API-based connection to EHR data, and registers App with Hospital A (or its EHR). Patient reviews App's data use and privacy policies (and features) and decides to connect App to her EHR data in Hospital A. Patient signs into Hospital A's portal, and Hospital A shows an approval screen. Patient agrees to share (some of) her EHR data for some duration of time with App, and Hospital A records this decision. Hospital A's portal sends Patient back to App, and App gets a unique, time- and scope-

limited access token for this patient. App can use the token to access Patient's EHR data for some duration of time in keeping with the patient's approval.

Marshall and Mandel explained that the task force is working on the following recommendations in 10 general areas:

General support for APIs:

- ONC should continue its pursuit of an API strategy as an important mechanism for enabling patient choice and promoting a more efficient health care marketplace
- ONC should consider advice from this task force to mitigate privacy and security fears, and to provide an explicit framework that balances the risks and opportunities of a health API ecosystem
- The task force encourages ONC to collaborate with other agencies to offer guidance to app developers regarding best practices
- We recommend that ONC encourage OCR to develop guidance for covered entities and business associates

Types of apps and organizations that provide them:

- ONC and CMS should explicitly state that the type of app, and the kind of organization that developed it, are not considerations with respect to a patient's right to access

Oversight (HIPAA—When does an app developer need a BAA?):

- OCR should provide additional guidance to clarify whether a BAA is required in certain scenarios

Registration process (including dynamic registration API and self-service registration):

- Ensures that app registration does not impose an unreasonable barrier to patient choice
- The registration process shall not impose delays. The registration process is not intended to be a point where apps undergo rigorous testing, clearinghouse approval, on-site inspection, or other high bars of control
- Self-service registration portals and dynamic registration protocols are two complementary ways to ensure frictionless app registration

Process of endorsement and certification:

- ONC should avoid requiring any centralized certification or testing of apps. Instead, ONC should pursue regulations that enable a secondary market in app endorsements
- In such a market, various kinds of organizations (EHR vendors; security experts; consumer advocacy groups; clinical professional societies; provider organizations, etc.) can "endorse" a given app through a distributed, publicly visible process, without centralized regulatory oversight
- This approach to endorsements avoids the pitfalls of defining a centralized certification process and the difficulty of standardizing privacy policies, but still allows consumer-facing discoverability benefits
- ONC should clarify that provider organizations must not use endorsements (or the lack of endorsements) as a reason to block the registration of an app, or to block a patient's ability to share data with an app

How do apps communicate their policies to users prior to sharing? (combined with who's in charge if the policies are violated?):

- ONC should encourage an app developer voluntary Code of Conduct that outlines best practices regarding how and what an app should communicate to consumers regarding its privacy and security policies
- ONC should support a Model Privacy Notice (MPN) for app developers (who is responsible for what, indemnification clauses, standard definitions and terms, privacy policies, notices of when they change, meaningful controls such as opt-outs, and contact information)
- ONC should provide guidance in its MPN for the minimum data set required for short form notices

Limitations and safeguards on sharing:

- ONC should clarify that while API providers may impose security-related restrictions on app access, it is inappropriate for API providers to set limitations on what a patient-authorized app can do with data downstream
- ONC should clarify that API providers are not obligated to protect patients by identifying "suspicious" apps
- An API provider may suspend API access to an app that has breached the API provider's terms of service, or appears to have been compromised, or poses a threat to the provider's own system
- Patients must be able to override this suspension (unless a threat)
- Need clarification about where terms of service end (between app and provider) and HIPAA begins; also where complaints should go
- ONC should update the HIT certification requirements to ensure that API providers enable patients to share data with certain (coarse-grained for now) categories, rather than "all or nothing"
- Patient should be able to view a provider-generated list of apps that currently have access to their records; to revoke access at any time; and to make sharing decisions that restrict the scope of access
- Implementing many narrowly-scoped access control policies would require a costly and difficult redesign of existing systems
- Short term, we propose a pragmatic approach that ties back to the capabilities described in the 2015 certified electronic health record technology (CEHRT) Certification Criteria: since CEHRT must already enable access through separate API calls at the data category level (e.g. medications, vital signs, or lab results)

Audit trail and recording requirements (when a patient approves an app approval, and for subsequent API access):

- We recommend that ONC should require EHRs to make API access audit logs available to patients through an Accounting of Disclosures via the portal
- We recommend that ONC collaborate with appropriate stakeholders to provide guidance to app developers regarding best practices of audit capture
- ONC should provide guidance around breach notifications rules and responsibilities

Identity proofing, user authentication and app authentication:

- ONC should provide guidance that the patient identity proofing and authentication requirements in an API ecosystem are not different from the requirements for MU2-era patient portal sign-in and VDT
- Any process that presents a substantially greater burden to the patient for API access approval should be considered information blocking
- Standards like OAuth 2.0 should be used to allow patients to leverage existing portal account infrastructure as the means for approving access to an app
- API providers must not impose patient identify-proofing or authentication barriers for API access that go beyond what's required for VDT access
- ONC should collaborate with the OCR and the FTC to provide clear and distinct API developer and API appropriate usage privacy and security standards in order to encourage API development and adoption
- For registering patient-authored apps, existing patient identity proofing and authentication is sufficient. Any patient who is able to sign into the portal of an API provider should be able to register any app that they chose with that API provider
- For non-patient-authored other apps, ONC should clarify that identity proofing of developers must be automatable and not onerous
- ONC should further clarify that in situations where greater assurance is desired, app endorsements can achieve this assurance in a non-blocking, low-friction way without preventing registration of non-endorsed apps
- ONC should recommend that at approval and data access time, authenticating apps via standards-based mechanisms like OAuth 2.0 client authentication should be acceptable
- Providers must ensure that app approval and data access can occur without active involvement from the API provider or the app developer
- The only person who should have to take action to approve an app's access to patient data is the patient (or representative)

Consent and authorization framework:

- ONC should coordinate with relevant agencies to publish guidance for the respective actors (app developer, patient, etc.) on whether sharing data with a consumer-directed application is considered to be part of an individual’s access, access by a third party, or a tool for engaging in treatment
- ONC should continue advancing work in support of standardized, machine-computable consent.
- ONC should coordinate a model authorization form with reusable/referenceable language and a standardized mechanism by which a patient can compare authorization requirements for two or more providers
- Providers should include statements, typical of HIPAA authorizations, to notify patients of their rights to revoke app authorization, the role of the covered entity, disclosure of any provider relationships to apps, and HIPAA coverage
- Until clear guidance is available, providers should proceed to define their practices for EHR portals to ensure patients provide the essential information necessary for valid, informed go-ahead for the provider to enable consumer-directed app access to data

Discussion

Mandel asked members to keep their comments at a high level. Editorial and minor suggestions can be emailed. There is considerable work to be done prior to the presentation of final recommendations for action at the June meeting.

Richard Elmore referred to identity proofing and the lack of current and consistent standards. He wondered how the OCR guidance handles the validation of security. Mandel responded that the task force focused on read-only recommendations that could be implemented now. Since there are no agreed-upon standards, the recommendations will refer to reasonable practices. The security of the app is not an issue for the provider. The provider organization need only be concerned with the security of its own system.

Tang said that the recommendations should acknowledge the need to educate consumers on privacy. Consumers will need to understand the implications of their choices; what is the role of government in helping users make reasonable decisions? Saying that only one of every 20 startups succeeds, he wondered what will happen to users of apps when the developers go out of business. Mandel agreed that literacy on privacy is very important. Consumers vary greatly in their knowledge. Good models are needed on how to convey information to consumers. Mandel asked for suggestions in addition to notices. Marshall reported that although the task force members talked about endorsement and certification, they eventually took a stance in favor of consumer choice. However, some members hope to see the development of third party endorsement.

Gayle Harrell said that she foresees and is concerned about bad actors. Education and safeguarding of consumers is very important. What if a provider suspends use of an app, resulting in data blockage? What about proof and punishment of bad actors? What is ONC's role? Mandel replied that the approach is to safeguard access by focusing on a chain of access with reporting at each point of the chain. No recommendations are expected on enforcement. There are limits on what can be guaranteed, so the fallback is on the consumers. Marshall added that it is assumed that the portals are CEs and, therefore, subject to HIPAA. Blake instructed members to be brief.

Paul Egerman observed that all of the examples in appendix C involve data flowing from the EHR to the patient. The flow from EHR to server to someone, who is not necessarily the patient, is not considered. Since most apps are free, the developer may have an incentive to sell the data, some of which may be PHI. Patients expect providers to protect their data. They will not be happy to find out later that the fine print said that privacy and security are their responsibility. Egerman suggested that the task force recommend that any app developer become a BA. Then HIPAA would apply. Mandel said that the task force did not have an opinion on servers. Comments obtained from select stakeholders indicated that BAAs were undesirable in this case. BAAs would constitute Insurmountable barriers. Egerman said that OCR could create a standard BAA for developers, stating what happens if the developer goes out of business. Marshall declared that the suggestion was worth considering. Mandel reminded everyone that BAAs are agreements with CEs, not OCR or consumers.

Patricia Sengstack questioned the assumption that patients can access and activate their portals sufficiently to use apps. Perhaps the recommendation could focus on educational efforts for providers as well as patients.

Aaron Malec said that since ONC is charged with coordination, it can work with the four federal agencies that may allow access to apps and other agencies that will likely develop apps themselves. ONC coordination could be a mechanism for acting on the recommendations. With regard to enforcement, the task force could recommend a centralized site for complaints. ONC and OCR cannot fix the tangled

interagency regulations. Mandel indicated that the task force intends to specify which recommendations apply to which agencies.

Leslie Kelly Hall, herself a member of the API Task Force, called for an explicit recommendation on access. Patient education must honor choice. Plain language must be used. Patients make important and complex decisions about health daily and are capable of decisions about apps.

Donna Cryer said that since patients are driving the use of apps, probably a crowd sourcing situation will be devised to centralize complaints. Someone should design talking points for providers to use in talking to patients about apps.

Nancy Orvis said that patients will want to store and combine data, which must be computable. Mandel clarified that when he referred to read-only, he was talking about the EHR data. The apps will be able to compute.

Floyd Eisenberg asked about patient-authored apps, saying that someone could design an app to change providers' data. How will providers decide what is harmful? Will the app maintain provenance of the data? Mandel said that apps will not be able to write back to providers' data.

Expressing concern about apps directly accessing providers' data, John Scott said that a personal health record hosted by the provider as an intermediary would place less burden on the provider's system. Mandel said that providers can segregate data for patient access. It would be an internal decision. Blake told members to email any additional comments on this thread. Blake noted that the agenda item had been completed on schedule.

HITSC Precision Medicine Task Force Recommendations

Precision Medicine Task Force Co-chairperson Leslie Kelly Hall referred to slides on ONC's role in the Precision Medicine Initiative (PMI), the charge to the task force and process, repeating information provided at previous meetings. Kelly Hall acknowledged that the task force is at a very early stage in making recommendations. The task force has been working on interoperability pathways critical to PMI and attempting to answer these questions:

- What data sources are available?
- What are the gaps?
- What are the known gaps regarding high value data needed for PMI?
- What efforts could be accelerated to help the work of PMI?
- Are there areas for which standards could be recommended to promote scalable and repeatable development for PMI?

The near-term recommendation (2016) will focus on EHR data first. Participants should be constrained to using a specified EHR export format(s), and data recipients may need to anticipate level of effort, depending on their internal data models, to translate data once they receive them. Consensus-based models to consider may include:

- Data Access Framework and Argonaut
- PCORnet, Sentinel
- NCI
- Observational Health Data Sciences and Informatics
- Veterans Administration mapping to Observational Medical Outcomes Partnership

Mid-term recommendations (2017) will enable data gathering from other independent non-provider sources. PMI should consider data sources, in addition to the EHR, that promote completeness of longitudinal patient information. Examples include: medication history and dispensing data, commercial and hospital labs, and claims. Gathering patient data from a variety of sources will have implications for identity matching, consent and authorization, and means of patient-mediated data donation to reduce needs for probabilistic matching.

Long-term (2017-2018) recommendations are to return an individual participant's aggregated data from multiple sources, and eventually research results. Patients should have the option to access computable raw genetic testing and sequencing data because these raw data are among the most potentially useful to patients in the long term. NIH could consider a participant-facing API that would allow an individual to pull her aggregated data from the cohort to the app of choice and should leverage existing and emerging standards (e.g., FHIR). Important issues to address are:

- Privacy and security implications of returning an individual's aggregated data
- Clarification of related policy considerations would facilitate patient data access and return of research results (e.g., CLIA, HIPAA)
- Liability issues of working with genomic data with respect to what a researcher is obligated to disclose back to the patient
- Granularity of permissions
- Options related to types of data patients would like to access or receive

Kelly Hall invited comments on the adequacy of the three stages, as well as the identification of other groups doing similar work.

Discussion

In responding to a question from Scott, Kelly Hall said that the task force has not yet considered whether consent would include any copy of data or records maintained by a provider.

Washington underscored the importance of a single set of standards in the three phases as they contribute to a learning health care system. A single set is required for data from other sources. This is the specific use case standing on the bedrock of a learning system.

Blake said that patient registries should be added to slide 9. Regarding the completion of activities in 2016, she wondered whether the time line is realistic and asked about the extent of outreach on constraint of standards. Kelly Hall referred to several ongoing efforts across standards organizations. The task force will possibly recommend constraints, for example, in registration. Common data elements across organizations may be identified. Although the time line is challenging, people are inspired and eager to participate. Blake went on to ask that the task force align with other requirements for quality measurement.

Troy Seagondollar suggested that when gathering data from multiple locations, notification could be given to patients that their data have been harvested. The notification would be similar to what is done with credit reports. Kelly Hall said that patients will participate in identity matching. She will forward the suggestion to the task force members.

Cryer expressed concern about the scope of the effort, although the use of registries may make it more manageable. Many of the priority data domains are not relevant. Identification of biomarkers and environmental triggers, which are essential, requires identification of additional data sources. It is important to learn about the scope of existing registries.

David Lansky highlighted the importance of capturing information on the context of the patient's care. He called for acceleration of obtaining information on claims, benefit design, provider cost constraint measures, and patients' self-reports on their ability to pay and their own expenditure reduction efforts.

Elmore talked about distributed queries and holding genomic data in cohorts. Kelly Hall said that because of the huge volume of genomic data, which are not computable, data storage is a concern.

Kevin Johnson pointed to slides 8 and 12 and wondered about another sequencing. According to Kelly Hall, the hottest discussion is how quickly to give feedback to participants and what can reasonably be done in 2 years. Johnson referred to slide 10 and said that data aggregators may be helpful

Malec pointed out that with Sync for Science Mandel is working on a solution, which is a pragmatic place to start to open up APIs.

Public Comment*:* None

State Medicaid Director Letter 16-003 February 29, 2016

Thomas Novak, ONC, explained that the CMS Medicaid Data and Systems Group and ONC Office of Policy have updated the guidance on how states may support HIE and interoperable systems to support Medicaid providers in attesting to stages 2 and 3. The guidance allows the use of Medicaid HITECH funds to support all Medicaid providers with which EPs want to coordinate. Medicaid HITECH funds can now support HIE onboarding and systems for behavioral health providers, long-term care providers, substance abuse treatment providers, home health providers, correctional health providers, social workers, and others. It may also support the HIE onboarding of laboratory, pharmacy and public health providers. This funding goes directly to the state Medicaid agency in the same way existing Medicaid HITECH administrative funds are distributed.

This funding is in place until 2021 and is a 90/10 federal-state match. The state is still responsible for 10%. The funding is for HIE and interoperability only, not to provide EHRs, and only for implementation, not for operational costs. The funding still must be cost allocated if other entities than the state Medicaid agency benefit. All providers or systems supported by this funding must connect to Medicaid EPs. Several HIE modules and use cases are specifically called out for support:

- Provider directories
- Secure messaging
- Encounter alerting
- Care plan exchange
- Health information services provider
- Query exchange
- Public health systems

Medicaid systems must adhere to Medicaid Information Technology Architecture (MITA), which requires adherence to seven conditions and standards:

- Modularity standards
- MITA condition
- Industry standards condition
- Leverage conditions
- Business results condition
- Reporting condition
- Interoperability condition

45 CFR Part 170 delineates:

- Transport standards (e.g. Direct)
- Functional standards (e.g. clinical decision support)
- Content exchange standards (e.g. CCDA)
- Implementation specifications for exchanging electronic health information
- Vocabulary standards for representing electronic health information

Existing guidance on the following other activities that can be supported remains in place:

- Personal health records
- System and resource costs associated with the collection and verification of meaningful use data from providers' EHRs
- System and resource costs to develop, capture, and audit provider attestations
- Evaluation of the EHR Incentive Program (Independent Verification and Validation and the program's impact on costs and quality outcomes)
- Data analysis, oversight, auditing, and reporting on EHR adoption and meaningful use
- Environmental scans and gap analyses
- SMHP updates and reporting, IAPD updates
- Developing data sharing and BA agreements
- Ongoing costs for quality assurance activities, Multi-State Collaborative for Health IT annual dues, staff and contractual costs related to the development of state-specific meaningful use and patient volume criteria, Medicaid staff training and professional development
- System and resource costs associated with the National Level Repository interface
- System and resource costs associated with state interfaces of a HIE (e.g., laboratories, immunization registries, public health databases, other HIEs, etc.)
- Creation or enhancement of a data warehouse or repository (should be cost allocated)
- Development of a master patient index (should be cost allocated)
- Communications and materials development about the EHR Incentive Program and/or EHR adoption and meaningful use
- Provider outreach (workshops, webinars, meetings, presentations, etc.)
- Provider helpline, dedicated email address, call center (hardware, software, staffing)
- Web site for provider enrollment and FAQs
- Hosting conferences and convening stakeholder meetings
- Business process modeling

Novak said that ONC and CMS staffs hope that this new eligibility will stimulate states to expand in these other activities. Staff is in the process of meeting with representatives of states that have indicated interest in applying for funds. Staff works closely with states preliminary to the submission of their applications.

Q&A

Malec said that although some states have been successful in building statewide architecture, other models are also being used. He asked about the flexibility to onboard to existing activities. Novak indicated that there is flexibility. Instead of onboarding, some states work on governance on top of ongoing network efforts. A state government can be more aggressive than a private entity. They can use various methods. Malec urged greater flexibility. Regarding standards guidance, ONC has established sub-regulatory mechanisms for the ISA: Why was this effort tied to regulation rather than sub-

regulation? Novak said that a state Medicaid agency could do a notice of alternative considerations. ISA is referenced as a resource. CMS is working on moving Medicaid to a modular system. Some modules are HIE-like. Letters are forthcoming.

Harrell voiced her excitement about moving HIE into behavioral health and long term care. She inquired about any requirement for a specific threshold of Medicaid patients. Novak indicated that any Medicaid provider can be considered regardless of number of patients. ONC and CMS are also working on data segmentation to deal with the restrictions on exchange of behavioral health data.

Blake asked about the possibility of collaboratives of adjacent states. Novak told her that the letter notes and encourages multi-state collaboratives. CMS is actively encouraging notifications across states.

A member asked about the inclusion of private HIEs. Novak said that there is no relationship between previously ONC-funded HIEs and the expansion defined in the letter. As long as a state can justify its relationship with an HIE, it may qualify. This letter introduces more flexible in the kind of HIE that is eligible.

Office of the Chief Privacy Officer (OCPO) Updates

HITSC Co-chairperson Lisa Gallagher introduced Lucia Savage, ONC, who began by reporting that one-third of patients seen by a health care provider in the past year reported a gap in information exchange. Stakeholders are asked to take the interoperability pledge:

- Consumer Access: To help consumers easily and securely access their electronic health information, direct it to any desired location, learn how their information can be shared and used, and be assured that this information will be effectively and safely used to benefit their health and that of their community.
-
- No Blocking/Transparency: To help providers share individuals' health information for care with other providers and their patients whenever permitted by law, and not block electronic health information (defined as knowingly and unreasonably interfering with information sharing).
-
- Standards: Implement federally recognized, national interoperability standards, policies, guidance, and practices for electronic health information, and adopt best practices including those related to privacy and security.

Savage briefed the members on HIPAA. A new HIPAA access guidance is available: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. OCR issued the new guidance in early 2016. Key concepts for apps and APIs in ONC's 2015 Edition are timing of providing requested records, automation, and electronic formats, if readily available. However, a provider can reject media (such as a thumb drive) that reasonably threaten the security of the provider systems, and psychiatric notes and prison medical records can be withheld. There are other limits that the individual can appeal. OCPO launched a four-part blog series entitled "The Real HIPAA Supports Interoperability" on February 4. OCPO and OCR published educational fact sheets to supplement the blog series. HIPAA permitted uses and disclosures (PU&D) are situations in which a CE is permitted, but not required, to use and disclose PHI without first having to obtain a written authorization from the patient. Such situations are: quality assessment and improvement activities, case management and care coordination, population-based activities to improve health or reduce health care cost, development of protocols, and evaluation of health care providers and/or health plans. The 2015 CEHRT automates PU&Ds. Under HIPAA, health information can be shared for permitted uses. Patients have the right to an electronic copy of their medical records, if the records are stored electronically, and the right to send a copy

(transmit) elsewhere. Stage 3 requires that patients must be given electronic access to a portal within 24 hours in order to view online, download, and transmit their health information, and access to an API that can be used by third party apps. 2015 Edition CEHRT requires API functionality, including lookup and retrieve whole or partial patient record, API security measures, and a transmit option that includes unencrypted email.

Savage reminded the members that the Interoperability Roadmap calls for greater consistency across state privacy laws. ONC awarded a grant to the National Governors Association to identify barriers to the exchange of information across states. Funds for the second phase (September 2016 – May 2017) were recently awarded. See ONC Funding Opportunity Announcement (FOA)/Award: http://www.grants.gov/web/grants/view-opportunity.html?oppId%3D277387.

Savage continued. Regarding security, ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cybersecurity for critical public health infrastructure. This includes enhancing information sharing capabilities within the health care and public health sector for bidirectional information sharing about cyber threats and vulnerabilities. ONC will work with the National Institute of Standards and Technology (NIST) and OCR to finalize and publish the NIST Critical Infrastructure Cybersecurity Framework and HIPAA Security Rule Crosswalk. ONC will work with stakeholders and ASPR to develop best practices for actions that small and medium size health care organizations can take when they become aware of cyber threats. ONC will consult with OCR to make sure the practices are compliant with the HIPAA rule.

The Cybersecurity Information Sharing Act of 2015 section 405(c) orders HHS to form a Healthcare Industry Cybersecurity Task Force, in collaboration with NIST and the Department of Homeland Security (DHS). Complete information is available at http://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx. The first in-person meeting is scheduled for April 21, 2016 and is open to the public. This is the first of four in-person meetings that the task force will hold during the next year before reporting findings to Congress and the public.

Another cyber threat information sharing effort focuses on information sharing and analysis organizations (ISAOs), which are created to gather, analyze, and disseminate critical infrastructure information. ISAOs offer a flexible approach to self-organized information sharing activities and may offer increased and timely awareness of cyber risks so that members can mitigate and reduce the frequency and impact of attacks. ASPR awarded a grant to Harris County (Texas) Health to gauge an understanding of the needs for cybersecurity information for the health sector. The grant is HHS' first step in selecting a strategy that will enable organizations to collaborate within the private sector and between the private sector and government. This grant complements HHS' effort in facilitating the President's Executive Order (EO) 13691—Promoting Private Sector Cybersecurity Information Sharing. The competition among information sharing organizations in the health sector is not present in other sectors. This competition has led to inefficiency and delays in sharing information. HHS has not been able to ensure that information is shared beyond each organization's membership. There is less economic incentive for companies within the sector to focus on cybersecurity compared to other sectors. Since HHS is encouraging the expanded use of electronic systems for managing health information, it has a responsibility to ensure that these systems are secure.

Other ONC efforts in security and cybersecurity are numerous, such as, to name a few:

- Work with the Critical Infrastructure Partnership Advisory Council (CIPAC), Healthcare and Public Health Government Coordinating Council (HPH GCC) on cyber related activities.
- Coordinate with DHS

- Serve on the Joint Government Coordinating Council/Sector Coordinating Council (GCC/SCC) Cybersecurity Working Group
- Ensure alignment and coordination with Interoperability Roadmap commitments
- Advise on the ASPR planning grant on ISAO
- Participate on the Privacy Incident Response Team (PIRT)

Under PIRT, ONC will get advanced notice of any privacy incidents and provide guidance to the affected agency to aid in response. The purpose is to establish a coordinated approach between the various HHS organizations and offices that need to collaborate in responding to cyber incidents and events.

Q&A

Malec commented that although ransomware attacks get more attention, identity theft leading to financial and insurance fraud may be the greater danger. The health care sector is inconsistently prepared and needs more substantive guidance. He told Savage that she did not address the federal government's roles as purchaser and payer of services. A common set of approaches could be established. Contracts could be let contingent on cybersecurity standards. Savage said that each federal agency would have to examine its authority and resources. She suggested that task force members could direct their requests to other agencies.

Responding to other questions, Savage said that the restrictions on behavioral health data do not derive from HIPAA. The Healthcare Industry Cybersecurity Task Force is required to submit a final report in a year. It may or may not continue beyond that time. ONC will award a cybersecurity grant by the end of the fiscal year. She had no information on a possible ASPA grant.

Seagondollar inquired about the testing of products; does OCR look at app developers and vendors? Savage declined to speak for OCR, although she reported that ONC had recently announced a desk audit endeavor. The Healthcare Industry Cybersecurity Task Force will focus on information sharing; it does not change OCR's role.

Metrics Request for Information (RFI)

Talisha Searcy, ONC, described the RFI to solicit input on the measurement of interoperability, which is mandated by MACRA 106(b). The law requires that not later than July 1, 2016, and in consultation with stakeholders, the secretary of HHS shall establish metrics to be used to determine if and to the extent that the objective of interoperability has been achieved. If the secretary determines that the objective has not been achieved by December 31, 2018, then the secretary shall submit to Congress a report, no later than December 31, 2019, that identifies barriers to interoperability and recommends actions that the federal government can take.

Interoperability is defined as the ability of two or more health information systems or components to exchange clinical and other information, and use the information that has been exchanged using common standards to access longitudinal information for health care providers to coordinate care and improve patient outcomes. The scope of measurement is the extent to which meaningful EHR users are electronically sending, receiving, finding, and integrating information that has been received, and subsequently using that information. However, according to Searcy, ONC staff is asking two questions. Shouldn't the scope include populations other than meaningful EHR users? How does this relate to the measurement efforts outlined in the Interoperability Roadmap?

The Roadmap calls near-term (2015-2017) for an increase in the proportion of individual, office-based physicians, hospitals, and behavioral health, long-term care and post-acute care providers that send, receive, find, and use electronic health information; have electronic health information available from

outside sources and make electronic health information available to outside sources; and use electronic health information to inform decision-making. Long-term (2018 and beyond), the Roadmap expects an increase in the proportion of individuals and entities that send, receive, find, and use electronic health information; have electronic health information available from outside sources and make electronic lealth information available to outside sources; and use electronic health information to inform decisions, resulting in positive impacts on outcomes sensitive to interoperability.

Searcy reported on staff efforts to evaluate potential measures of interoperability. She described the strengths and limitations of several well-known surveys and other data that are being considered. The following are select examples of factors being considered:

- Does ONC's operationalization of exchange and use (e.g., send, receive, find, integrate, and subsequent use) adequately address MACRA's definition of interoperability?
- Should the focus of measurement be limited to use of certified EHR technology?
- Should the focus of measurement be limited to meaningful EHR users, and their exchange partners, or be consistent with the Roadmap?
- Do potential measures adequately address the exchange component of interoperability per MACRA?
- Do the reconciliation-related measures serve as adequate proxies to assess the subsequent use of exchanged information?
- Should staff develop measures to evaluate progress related to interoperability across health care providers, even if this data source may only be available for eligible professionals under the Medicare EHR Incentive Program?
- What other data sources and measures should ONC consider for Section 106(b) (1) of MACRA or interoperability measurement more broadly?

RFI comments are due June 3, 2016; see https://s3.amazonaws.com/public-inspection.federalregister.gov/2016-08134.pdf. Staff will compile and report to the committees in August on comments received.

Q&A

Eisenberg commented that the devils are in the details. In terms of operational definitions, percent of reconciliations is challenging. Eisenberg referred to his work on reconciliation of immunization registry data and pointed out that reconciliation is a cognitive process. Providers often just attest that reconciliation was done. Operational definitions are missing; for example, for incorporation. Eisenberg proposed devising something like LeapFrog used in hospitals to test the capability of ambulatory EHRs. The concept is to test capability, but not how often the function is used. He pointed out that Searcy's examples are process measures; health is the outcome. He suggested that one could look at providers' use of registries and subsequent improvement in outcomes.

Mandel opined that the approach is too much yes, no, up, down, right, left—binary distinctions. What about an experience survey that asks respondents what they have done? Searcy assured Mandel that the existing surveys do ask questions about experience and attitudes regarding EHR use and barriers. But MACRA has a more narrow focus. Kelly Hall suggested that they look for unintended consequences and not neglect experience.

Malec summarized that the different data sources can be used to measure different things. Survey data can be used to consider what is working. Transmissions are occurring but doctors hate the processes. He referred to an ONC data brief on acute care and adoption of EHRs that confused basic and certified

EHRs. Systemic biases can be identified in various ways and corrected. Searcy said that data briefs using the most recently available data are forthcoming.

Tang said that use should be measured as a byproduct of use. Attestations became check lists that are counterproductive.

Washington reported that staff has discussed all of the measurement issues. Better health care, not interoperability, is the real goal. Regarding the sufficiency of subjective data, he reported that AMA representatives are opposed to a time consuming process measure, which would constitute an undue burden.

Egerman acknowledged the difficulty of the topic. He suggested using something like reduction of duplicate lab tests as an indicator of interoperability. Another example is multiple opioid prescriptions. Change over time can be tracked. Searcy indicated that these measurements are being taken.

Seagondollar expressed concern about interoperability and integration. Without strong interoperability, integration cannot be expected. Integration should be defined. Searcy said that integration (or lack thereof) affects measurement. One survey defined integration as occurring with no manual input.

A member who identified as an epidemiologist talked about the ability to move quantity with quality. Mapping, data entry, security, and compromised data are all variables that affect safe analytics. A system of systems consists of many complex interfaces. Sampling can be used to answer specific questions of interest. A broad discussion of methods should be undertaken.

Blake pointed out that meds reconciliation is not a simple process and may not be a good marker. Regarding level of satisfaction with the EHR system, she suggested examination of the need to purchase a new system in a short time or sooner than expected. For use of information exchanged, she suggested asking providers whether they received a piece of information that changed their prescribed treatment. She reported that AMA found that the amount of time clinicians spend tracking compared to face time with patients is greater than 100%. The extent to which the ratio declines over time can be measured and tracked. Someone commented that ease of use is basic.

Sengstack declared that the focus should be on why. Perhaps ONC can partner with vendors on measurement. Kelly Hall said that the extent to which fax machine use has been eliminated (or reduced) may be an indicator of computability. Searcy reminded the members to submit comments.

ONC Announcements

Staff announced the upcoming convening of new (or reconstituted) groups. The Consumer Task Force will initially focus on the Blue Button connector site. Another task force will work on NPRMs, including MACRA. Members interested in participating may email Consolazio. Others can go to the FACA web site data base to volunteer.

The comment period for the Proposed Rule to Support the Reliability, Transparency, Accountability, and Safety of Certified Health IT will close May 2. A Webinar on the oversight rule will be held April 21 at 2 pm.

The committees will meet in person May 17.

Public Comment

Three members of the public submitted comments via the web meeting chat function.

Alan Viars, Videntity, wrote, “I agree with the recommendations, but I would imagine some pushback. Perhaps state/regional HIEs can meet the requirement on behalf of health organizations? Data from an HIE is likely to be broader. This could provide a new revenue (sustainability) model for HIEs.”

Julie Maas, EMR Direct, wrote, “It's difficult to balance ease of access with oversight of app trustworthiness. Perhaps a patient should also be able to opt out entirely (or first opt in to?) any automated process to grant Application Access.”

David Tao wrote, “Suggestion for Leslie Kelly-Hall on PMI Task Force. You mentioned the need for data sources such as PBMs and retail pharmacies to provide dispensing data to evaluate patient adherence. Does that go far enough? Prescriptions may be filled but not taken. What about PGHD capture to get as close to the patient and caregiver as possible?”

SUMMARY OF ACTION ITEMS

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

Meeting Materials

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