Collaboration of the Health IT Policy and Standards Committees

Draft Summary of the May 17, 2016, Joint 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 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

HITPC Co-chairperson Kathleen Blake asked for a motion to accept the summary of the April 2016 meeting as circulated with the meeting materials. A motion was made and seconded. The motion was approved unanimously by voice vote.

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

HITPC Co-chairperson Paul Tang thanked two members whose terms recently ended: David Lansky and Alicia Staley. Blake introduced new members Carolyn Petersen, Mayo Clinic; Karen van Caulil, Florida Health Care Coalition; and Jamie Ferguson, Kaiser Permanente (a former member of the HITSC). ONC Principal Deputy Coordinator Vindell Washington mentioned the importance of the agenda items, in particular the alignment with CMS. Jon White, ONC, echoed Washington.

Medicare Program: Merit-Based Incentive Payment System (MIPS) and Alternative Payment Model (APM) Proposed Rule

Tang said that the NPRM includes many of the recommendations of the HITPC. Kate Goodrich, CMS, showed many slides to explain the proposed program, which would repeal the Sustainable Growth Rate Formula, streamline multiple quality reporting programs into the new MIPS, and provide incentive payments for participation in APMs. She said that APMs are new approaches to paying for care in ways that incentivize quality and value, making providers accountable for both the cost and the quality of care of patients. According to the MACRA statute, APMs include: CMS Innovation Center models, the Medicare Shared Savings Program, the Health Care Quality Demonstration Program, and other demos required by federal law. Advanced APMs must meet criteria that include basing payment on quality measures comparable to those in MIPS, requiring use of EHRs, and either bearing more than nominal financial risk or being a medical home model expanded under CMMI authority. The proposed rule spells out the APM scoring standard, which streamlines MIPS reporting and scoring for eligible clinicians in certain APMs and aggregates eligible clinician MIPS scores to the APM Entity level. All eligible clinicians in an APM Entity receive the same MIPS composite performance score. The scoring standard applies to APMs that meet these criteria:

- Participate in the APM under an agreement with CMS

- Include one or more MIPS eligible clinicians on a Participation List
- Base payment incentives on performance (at the APM Entity or eligible clinician level) on cost, utilization, and quality measures

To be considered part of the APM Entity for the APM scoring standard, an eligible clinician must be on an APM Participation List on December 31 of the MIPS performance year. Otherwise an eligible clinician must report to MIPS under the standard MIPS methods. The scoring standard applies to the following:

- Shared Savings Program (all tracks)
- Next Generation ACO Model
- Comprehensive ESRD Care (CEC) (large dialysis organization arrangement)
- Comprehensive Primary Care Plus (CPC+)
- Oncology Care Model
- All other APMs that meet criteria for the APM scoring standard

MACRA does not change how any particular APM functions or rewards value. Instead, it creates extra incentives for APM participation. Like those in regular APMs, these individuals will receive APM-specific rewards, and some individuals (called qualifying APM participants or QPs) will be eligible for a 5% lump sum bonus. To quality for QP status, a provider must be in an advanced APM and have a certain percentage of patients or payments through that advanced APM. This percentage will be 25% when the provision first kicks in but will increase to 75% in later years according to the statute. QPs will not participate in MIPS, and they will instead receive a 5% lump sum bonus. Starting in 2026, the bonus will cease, and they will receive a higher fee schedule update (essentially being paid more per service) than non-QPs, instead of the 5% bonus. Although the financial incentives for participating in an advanced APM are considerable, it is important to note that most people will likely not be QPs and therefore not receive the bonus; instead, they will be subject to MIPS. However, the Quality Payment Program provides multiple ways for practitioners to be rewarded for responsible practice and multiple incentives to participate in APMs.

In order to avoid duplicative reporting across APMs and MIPS while still holding APM participants accountable for MIPS goals to the extent feasible, CMS proposes unique reporting and scoring standards for APM participants who do not become QPs.

Goodrich moved to a description of MIPS. Affected clinicians are known officially as eligible professionals (EPs). In years 1 and 2, EPs will include physicians, physician assistants, nurse practitioners, clinical nurse specialists, and nurse anesthetists. But the types of Medicare Part B clinicians who will participate in MIPS will likely expand during the first 3 years of implementation. For example, in year 3 and beyond, EPs will be expanded to include a much larger group, ranging from physical therapists to dieticians. The exact groups included will be defined in rulemaking, expected to be released later in 2016. There are three groups of clinicians who will not be subject to MIPS:

- Those in their first year of Medicare Part B participation
- Those with a very low volume of patients (the exact threshold for low volume has yet to be defined but will likely be defined in rulemaking to be released later in 2016)
- Certain participants in eligible APMs

MIPS does not apply to hospitals or facilities, only to individual clinicians. Goodrich described how MIPS will change the EHR Incentive Program to Advancing Care Information. Under MIPS, clinicians can choose which categories of objectives to apply to scoring, thereby allowing for reporting that matches practice and experience. Measurement will emphasize patient engagement and align with other Medicare reporting in order to eliminate redundant quality measures. The slides showed the calculation

of the MIPS composite performance score, which is based on quality, resource use, clinical practices improvement activities, advancing care information, and data submission options.

Finally, Goodrich said that the NPRM includes proposed changes not reviewed in her presentation. The 60-day comment period closes June 27, 2016. Commenters must refer to file code CMS-5517-P. For additional information, go to http://go.cms.gov/QualityPaymentProgram.

Discussion

Tang asked about assistance. Goodrich responded that CMS will contract with organizations to assist small practitioners and rural providers. The Transforming Clinical Practice Initiative is making awards to organizations to assess and help select practices. Quality Improvement Organizations can help. Goodrich said that clinicians look to their EHR vendors for assistance on reporting.

Elise Anthony, ONC, said that the 2015 Edition is a foundation for the new programs. The NPRM includes two assertions, one on information blocking and the other on surveillance. ONC is working closely with CMS.

Richard Elmore observed that the program is extremely complex: What about small providers? Although it may be logical for small groups to start with MIPS, the incentive structure may push them to APMs. How will they respond? Goodrich agreed that both the law and the rule are complex. She said that some provisions have been made to simplify reporting for small practices. Communications will be targeted for small practices. CPC+ will recruit small (fewer than 50 clinicians) practices. A CMS staff person explained that CPC+ is a demonstration program intended to help move practices to APMs. Goodrich said the law was intended to move providers into APMs. MIPS will help them to prepare for APMs. For some high-performing clinicians, MIPS may be the best choice. Elmore suggested that CMS collaborate with experienced organizations to help with public education.

Tang asked the members to shorten their questions. Floyd Eisenberg asked about quality measures: What is CMS doing to encourage outcome measures? What about registries? Goodrich said that more outcome measures will be used than in previous years. Specialty societies are more involved with outcome measures. CMS receives $15 million annually to develop measures. A measurement plan was released May 1 to prepare the next generation of measure development. CMS staff will work individually with registries to use electronic data so data can flow smoothly.

Eric Rose referred to quality reporting under MIPS and asked whether payment depends on quality. Goodrich responded that payment is based on performance.

Leslie Kelly Hall said that an ideal clinic pilot would be helpful. Telehealth should be defined consistently across programs. Patient participation in decisionmaking has not been adequately implemented or measured. Kelly Hall then asked about harmonization of standards. Goodrich said that CMS will work with ONC on standards transitioning into MIPS. Anthony said that the 2017 Edition will be a flex year, allowing use of the 2014 Edition, the 2015 Edition, or both. Staff will work with CMS on future editions. Anthony encouraged public comment on this topic.

In response to a question from Troy Seagondollar, Goodrich said that the EHR Incentive Program penalty ends in 2018. Medicaid and EHR incentives do not change.

Blake inquired about QCDRs, saying that the timing of the announcement of approved registries can result in participants not having sufficient measures for reporting. Goodrich said that CMS recognizes that the timeline is an issue. The announcement must precede the start of the reporting period. Staff are working on a solution.

HITSC Co-chairperson Arien Malec asked what is required in 2017 that is new for meaningful users and participants in PQRS. What about qualifying for CCPI? Goodrich said that resource use scoring is done administratively. A minimum caseload will be set for reliability. Providers are to select six measures, including an outcome if available. Bonus points will be assigned for high-value measures. Measures are similar to the current PQRS measures. QCDR measures can be used as well. The performance period is calendar 2017. There is a portfolio of measures. The approach is flexible but complex. Clinical practice improvement will be determined by attestation. Mostly, meaningful users can report what they are already doing without concern with thresholds. No new technology is required. Anthony interjected that measures are the same as the stage 3 measures.

Devin Mann asked what would be done to monitor unintended consequences and the extent of burden. Goodrich indicated that CMS had a process in place. Communication and technical assistance around MACRA will be based on a much more constant engagement with providers than was previously the case. CMS is building its operational capacity. Mann asked that information on the results of monitoring be distributed periodically. Goodrich told him to submit that comment.

Andy Wiesenthal asked about the timeline for administrative claims. Goodrich replied that there is no timeline, because fee-for-service is not being eliminated. She confirmed that for participants in APMs, the resource category is delegated to the APM.

Lorraine Doo, CMC, told Goodrich that she wanted to coordinate her work on claims and prior authorizations with MACRA-related training for providers. Goodrich agreed to meet with her.

Donna Cryer said that she believes that Advancing Care Information places appropriate emphasis on clinician engagement. She wants to be sure that the difference between interoperability and data flow is understood.

HITSC Precision Medicine Task Force Recommendations

Malec announced that HITSC members would vote on the recommendations. Precision Medicine Task Force Co-chairperson Wiesenthal reminded the members that this was the third time that the task force had reported on its deliberations. He and Precision Medicine Task Force Co-chairperson Kelly Hall referred to slides and presented recommendations in three categories.

Interoperability and data reciprocity:

- Provide the ONC Interoperability Roadmap addendum for PMI
- Engage stakeholders to accelerate a definition of minimum data set and standards for PMI, patient generated health data and phenotypic data and include vocabulary where gaps exist using existing standards and efforts
- Provide ongoing guidance and use Technical Expert Panel(s) (TEP) to enhance participant understanding of utilizing various data sources (e.g., validity overlap, provenance) and Roadmap of current efforts that support PMI (e.g., ONC Tech Lab) and inform the research community on interoperability with EHRs and standards in general (non-regulatory is the bias of the task force)
- PMI should consider high value, non-EHR data sources to promote completeness of longitudinal patient information
- PMI should use standard APIs (e.g., FHIR) to source data for meds, labs and claims
- PMI should consider means of patient mediated data donation to reduce probabilistic matching
- Individual participants' access to their aggregated data will promote retention and engagement
- Patients should have access to computable, raw genetic testing and sequencing data

- PMI should define near-term means of access and accelerate individual access; employ patient-facing portals that enable individuals to access all data types (e.g., labs, meds, genomics); and draw from stakeholders with relevant strengths and experiences (e.g., Open Humans, PatientsLikeMe)

Policy considerations:

- NIH should educate patients and providers on data access rights and uses
- Access rights should be consistent with protected health information (PHI) access standards
- Consider *The Framework for Responsible Sharing of Genomic and Health-Related Data* in developing data exchange principles
- Enrollment should include notification of the use of the patient NIH ID
- To accommodate results return and future use cases based on Sync 4 Science recommendations, notification should be sent back to the EHR with patient consent
- NIH direct enrollment should include strong assurance and identify proofing equivalent to the current patient portals model, use direct language, and employ Web Content Accessibility Guidelines (WCAG)
- Gathering patient data from a variety of sources will have implications for identity matching. The task force recognizes that significant efforts are underway to support this necessary capability.
- Inform patients of implications of identifiers used and consent regarding their use and clarify in consent if it applies to copies of the data
- Employ a consent framework that enables new and/or expansive consent as new data needs emerge
- HHS Office of Civil Rights (OCR) should confirm if consent is required for a provider to receive access to NIH data when a covered entity (CE) enrolls a patient into the cohort
- Data access rights should apply to genomic and phenotypic information and use notification to patients and providers when data is harvested
- The task force recognizes that efforts are underway to address access, liability and consent.

Standards and APIs:

- Participants should be constrained to using a specified EHR export format(s)
- Data recipients may need to anticipate a certain level of effort to translate data
- Consensus-based models can facilitate exchange; considerations may include: Data Access Framework and Argonaut; PCORnet, Sentinel, NCI Cloud Pilots and Cancer Genomic Data Commons, Observational Health Data Sciences and Informatics (OHDSI); and Veterans Administration mapping to OHDSI
- For data donation, use consistent FHIR-based APIs (e.g., Sync 4 Science, Argonaut)
- New FHIR resources may not be needed immediately; an extension of existing resources may help (e.g., existing MU CDEs)
- FHIR will become more necessary as it continues to evolve
- HPO enrollment on patients' behalf should include patient generated health data when possible
- Patients will act as an exchange mechanism among their providers and as a data source for data not captured in EHRs
- Promote standardization for use of patient generated health data (e.g., Genetic Alliance) especially in enrollment
- Recognize that standards are evolving

- EHRs are source for: episodic and demographic information, labs, meds, histories, etc. and Common Clinical Data Set minimum bar
- App and API implementation is recommended to enable patient connection to EHRs to exchange CDS to NIH and provide ability for reciprocal queries from EHR for patient specific aggregate requests of patient generated health data

Discussion

Malec noted that the slides on recommendations were somewhat confusing regarding to whom they are directed. Slide 12 applies to ONC, slides 13 and 14 apply to the PMI, and slide 15 applies to NIH. What about the remaining slides? Is the recommendation that ONC coordinate with NIH? Kelly Hall said that that was the intent. Malec asked that the transmittal letter clarify the direction of the recommendations.

Elmore wondered about research-to-clinician feedback. Wiesenthal referred him to a graphic, saying that the model includes feedback to both clinician and patient, with both individual and aggregate data. Elmore noted its absence in the actual recommendations. According to Kelly Hall, this is a gray area. The task force recommended identifiers and a record location system to accommodate feedback. However, exactly how the feedback will happen has yet to be resolved.

Anne LeMaistre inquired about making raw data available to patients. Would a repository be involved? Kelly Hall said that the recommendations recognize the right to access but do not specify a process for movement. Access does not necessarily mean download.

In response to a question from Blake, Wiesenthal said that a patient should determine the level of control over the use of her own data and its accessibility to her provider. Blake pointed out that patient-provider relationships have beginnings and ends. Therefore, the timing of permission for use must be considered. Not everyone will remember that genomic data were obtained and where they are located. Duplicate genomic sequencing should be avoided. Kelly Hall said that that is the purpose of the record locator.

Tang said that the API world introduces a new version of consent that is once and forever. Did the task force consider the implications for APIs? Kelly Hall explained that a complex consent framework is expected. The recommendations pertain to identity assurance for enrollment. Tang wondered whether robust consent management is a precursor to this. Wiesenthal talked about financial services data. He agreed that combining all of these data sources may be intrusive. These are policy issues that no one appears to know how to handle. Policy questions are out of scope for the task force. Tang asked about prerequisite policy. Mandel reminded him that the task force reports to the HITSC; perhaps the policy recommendations should be considered separately by the HITPC. Washington agreed that many policy issues are involved. He asked about standards and the use of aggregate data for CDS. Kelly Hall said that it is a great parking lot item. White elaborated, saying that a coordinating center via a cooperative agreement will hold the aggregated data. OCR is an important partner in the PMI along with other organizations that deal with privacy and security concerns. A grant award for technology to complement these issues is pending.

Petersen requested clarification on slide 16 and the reference to new or expansive consent. Wiesenthal explained that a new framework may be required to allow participants to consent to something not previously contemplated.

Gayle Harrell expressed concern about the long-term implications of storing data. She wants a privacy and security subgroup to investigate these implications. Current law prohibits the assignment of unique identifiers. HITPC should be more involved. Wiesenthal reminded her that the deliberations of the task

force were public. Kelly Hall said that the reference to an identifier pertains to a record locator. Malec reminded them that PMI is under the purview of NIH, not ONC. The charge to the task force is limited.

Someone underscored that research labs are not covered under CLIA. The PMI model represents a change for the research industry.

Malec asked whether committee members had any objections to approval of the recommendations submitted by the task force. Hearing none, he declared them approved for submission to ONC.

> **Action item #2: The recommendations of the Precision Medicine Task Force on standards for the PMI were approved**.

Kelly Hall thanked Mazen Yacoub for excellent staff work.

Office of Standards and Technology Updates

Malec announced that the agenda had been modified to hear this staff presentation before the lunch break. Steve Posnack, ONC, reported on activities related to recommendations made by the HITSC March 2015. Regarding a recommendation to support a convening function, ONC's organizational approach for standards and technology is aligned with the ONC Tech Lab focus areas. ONC has awarded cooperative agreements to HL7 and NCPDP, and staff is participating in multi-SDO coordination projects. Two new cooperative agreement programs, the High Impact Pilot and the Standards Exploration Award, were recently announced. Applicants are expected to use the ISA in selecting among the impact dimensions and priorities categories shown on his slide. The pilots are to be completed within 1 year. Posnack assured the members that staff pays attention to the committees' recommendations.

Q&A

Kim Nolen observed a lack of specifics. Regarding the subcategory of drug cost at care, she wondered whether it referred to cost to patient or total cost, which would include rebates. Saying that he was subject to restrictions on commenting on an open announcement, Posnack said that FOA information sessions for applicants will soon be announced. The purpose of the programs is higher transparency about price paid by patients.

Kelly Hall asked about another sub-category, opioid: Does the primary category of medication management apply to any drug? Posnack indicated that the FOAs do not list specific drugs. He said that an application could include and explain provenance and duplicate management.

Public Comment*:* None

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

On May 12, the 52-page report of the task force was sent by email to committee members so that they would be prepared to act on the recommendations. The task force had presented its preliminary recommendations to the committees at two previous meeting.

The recommendations were organized as follows:

General support for APIs:

> We recommend that ONC address other API use cases in the future when the work can be informed by the lessons learned from experience with the initial use case. For example, future use cases include:

- Patient-directed APIs with Write and Update access to EHRs, including the incorporation of patient generated health data from a non-clinical setting. Such APIs might underpin future certification requirements.
- Patient-directed APIs that access multiple patients (for example, aggregation of populations of patients).

ONC should continue its pursuit of an API strategy as one important mechanism for enabling patient choice and promoting a more efficient health care marketplace. The task force did not identify any "show-stopping" barriers that would prevent the deployment of APIs within the timelines for ONC 2015 CHIT and stage 3. Nevertheless, we urge ONC to respond to our recommendations in a timely fashion, especially where we have requested clarification and guidance.

Oversight and enforcement:

ONC should coordinate with the relevant agencies and congressional committees of jurisdiction where legislation and rulemaking are needed to give agencies the ability to effectively implement rules and regulations that ensure privacy and security of all health data.

ONC should analyze the feasibility of a single, simple, comprehensive oversight framework mechanism that would address the needs of the patient-directed API ecosystem (for all health data shared with all organization types using any technology).

We recognize implementation of such a framework may require congressional action; however, using its role as advisor for all things health IT, ONC should seek to harmonize conflicting, redundant and confusing laws that govern access to health information.
ONC should coordinate with the relevant agencies a single location for all API actors (EHR API developers, app developers, providers and patients) to access in order to become educated and to ask questions about the oversight and enforcement mechanisms specific to patient directed health apps, as well as their specific rights, obligations and duties.
Patients should have one place to access in order to log complaints regarding an app's behavior. For example, the patient should not have to navigate the complex oversight environment to know whether his/her complaint is a HIPAA complaint or an FTC complaint.

App developers should have one place to access in order to log complaints that could launch investigations regarding a provider or an EHR API developer's behavior regarding information blocking. Penalties for bad actors should be clearly communicated, as well as the source of law and enforcing agencies.
We recommend that ONC coordinate with the relevant agencies to publish guidance as quickly as possible for EHR API developers, app developers, providers and patients, as to whether, from a HIPAA perspective, sharing data with a patient directed application should be considered as: an individual's access; access by a third party; or a tool for engaging in treatment (or a combination thereof), so the respective actors could anticipate how to meet HIPAA-specific requirements.

We note there may be a need for further distinction based on the nature of the app and its function, in a manner that affords the patient both the greatest flexibility and the highest protections.

ONC should work with the relevant agencies to provide guidance to providers as to the patient-specific warnings and notices that can and should be made available via the provider's portal prior to the app approval and authorization process.

Types of apps and organizations that provide them:

ONC should coordinate with the relevant agencies and explicitly state in formal guidance that the type of app, and the kind of organization that developed it, are not considerations with respect to

patient access. The only relevant concerns should be technical compatibility (i.e. app works with the API technical specifications) and patient choice.

App registration:

ONC should clarify that its goal is to ensure that when app registration is required, it does not impose an unreasonable barrier to patient choice.

ONC should ensure that in scenarios where registration is a technical requirement, the registration process is frictionless and does not impose unreasonable delays. For example, 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.

ONC should further clarify that self-service registration portals and dynamic registration protocols are two complementary ways to ensure frictionless app registration. In subsequent rules, ONC should require both of these modes of app registration, since they address different developer needs, and it is easy to build a self-service registration portal on top of a dynamic registration protocol.

ONC should clarify its claim that existing certification criteria are "sufficient to allow access without requiring further application pre-registration", since this statement is out of line with real world authorization protocols (e.g., OAuth 2) where registration is sometimes a technical requirement.

ONC should coordinate with the appropriate oversight agencies to ensure that API providers do not charge a fee for the app registration process, when registration is required. We note that HIPAA in general allows CEs to apply reasonable charges for a patient's access to data, but such charges should not be applied to the registration process before any data are flowing. ONC and OCR should clarify that reasonable charges in this context are vanishingly low, even to the point where levying the fee might cost more than the fee itself.

ONC should coordinate with the appropriate oversight agencies to specify how app developers should report any data blocking issues that occur within a provider's app registration process.

Endorsement and certification:

ONC should not require centralized certification or testing of apps. Instead, ONC should encourage a secondary market in app endorsements.

ONC should ensure 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.

Provider organizations, however, should have the ability to present some of an app's endorsements to the patient at the time of app approval. For example, a provider could display endorsements from trusted sources (or conversely, if the app has none, the provider may display a warning and request extra patient confirmation).

ONC should coordinate with the relevant federal agencies that are also holders of patient data (Department of Defense (DoD), Veterans Affairs, CMS) to encourage the publication of federal app endorsement criteria, by which their patient populations would benefit. For example, the DoD may create a list of criteria by which apps that access the EHR data of active military would meet to indicate the app's trustworthiness.

ONC should encourage a secondary market by which patients are able to share their experiences about an app.

Communication of the app's privacy policies:

We recommend that ONC coordinate with the relevant agencies to pursue a concept of privacy literacy, similar to what is known as health literacy. This would include defining the basics of privacy literacy, and outlining strategies and techniques for the government either to act on directly or through providers and app developers to improve privacy literacy at the community and organizational level.

Privacy literacy is the degree to which individuals have the capacity to obtain, process, and understand basic privacy information needed to make appropriate decisions regarding the sharing of personal information, including health data.

We recommend that ONC supports a Model Privacy Notice (MPN) for app developers.

The MPN should clearly define who is responsible for what (individual, app developer, provider, API developer), including example indemnification clauses where applicable.

The MPN should provide standard definitions and terms.

To facilitate easy review and a user-friendly experience, a short-form privacy notice may be valuable, with a link to access the full notice or more detailed information. ONC should provide guidance in its MPN for the minimum data set required for short form notices.

The MPN should allow for the download or other electronic save of the privacy notice (or otherwise saved electronically).

The MPN should ensure a just in time communication when the patient accesses the app.

Users must be informed when the app's practices change.

Privacy policies must be easily accessible in the app for later review.

Where the patient has choice and control, the app should provide meaningful controls such as opt-outs.

Contact information regarding how a patient can contact the app developer if there are problems are concerns must be stated.

We recommend that 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.

We recommend that ONC collaborate with FTC to provide ongoing support to app developers to ensure the app's privacy practices align with the app's marketing practices according to Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information.

We recommend that ONC evaluate methods by which a consumer is able to compare the privacy policies of two or more apps.

We encourage ONC to pursue enforceability of click through agreements specific to health information.

We encourage the private market to develop standards specific to the usability of consumer apps, and until such time, app developers should be encouraged to consult WCAG for a wide range of recommendations to make apps more usable to more types of users.

We encourage the development of private market endorsements to indicate those apps that strive to make content accessible to a wider range of people with disabilities, including blindness and low

vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these.

Patient authorization framework:

We recommend that until clear guidance is available, providers should proceed in defining practices for API disclosures in a manner that focuses on ensuring the patient is in possession of all essential information in order to give his/her valid, informed go-ahead for the provider to enable the patient-directed app access to the patient's data.

While we expect this is no different than what a patient is already asked to agree to for use of the portal for View, Download and Transmit functions, this ensures the authorization represents the patient's control to direct the disclosure (or use the app to make the request).

We recommend that ONC coordinate with the relevant agencies a model authorization form with reusable and reference-able language that contains: name of the patient whose records will be shared, relationship of the authorizer to the patient, name of the app requesting information, and description of the information that identifies the information in a specific and meaningful manner, such as listing the data categories the app is requesting access to (scope of permissions). While we recognize the need to provide more granularity in access permissions as capabilities evolve, we note ONC should be clear in its guidance that there is no expectation to support granular permissions beyond data categories for the 2015 CHIT Edition API requirements, for example, grant "Access to My Meds," not "Access to My Diabetes Meds." The authorization form should also contain a statement as to whether the app can or cannot change information currently in the EHR, the duration, whether the app is authorized to access the EHR asynchronously (when the consumer is not present), and a representation of the individual's intent to complete the authorization (such as "Sign" "OK" "Complete" button). Note that the task force is not commenting on best practices for e-signature. However, this information should be readily obtainable from a web interface (clicking on buttons or typing) and should not require offline processes (such as a faxed signature) or special software.

The patient must be provided a mechanism to email or otherwise electronically save the authorization for his/her own records. Access to the policies regarding the API developer and the provider's obligations to disable access to an app (such as through the provider's obligations to respond to threats under the HIPAA Security Rule), as well as the patient's ability to be made aware of the reasons for which an app is disabled (and any related appeal process) must be provided.

We recommend additional guidance to determine whether there are grounds and specific requirements to support the provider to deny the patient's request to authorize a patient-directed app, such as those specified in 164.524.

As we expect patients will be managing access to their data across multiple EHR APIs from multiple provider portals, use of a model authorization form will help patients be aware of and navigate inconsistencies. We recommend that ONC encourage a standardized mechanism by which a patient can compare authorization requirements for two or more providers.

We recommend that ONC continue advancing work in support of standardized machine computable consent. At the same time, we emphasize that a lack of granular, computable consent standards should not be viewed as a barrier to exchanging data through APIs. Generally, standardized machine computable consent may be helpful for the "to what" aspects of the disclosure. Supporting the request of the API through a standardized, computable process could facilitate the response

matching the request as accurately and completely as possible, and consistently across multiple systems.

In the Interoperability Roadmap, ONC referred to computable privacy as "the technical representation and communication of permission to share and use identifiable health information, including when law and applicable organizational policies enable information to be shared without need to first seek an individual's permission. Once implemented effectively, using technology for privacy compliance saves time and resources, and can build trust and confidence in the system overall. Standards for computable privacy will go a long way to address automating the complex legal, regulatory and policy landscape for patient directed exchange of health information via apps.

We recommend that ONC coordinate with the relevant agencies to publish guidance to providers on best practices for patient directed API authorizations. We recommend the provider include the following statements, which are typical of HIPAA authorizations, to notify the individual:

- The individual has the right to revoke the app authorization, and provide a description of the process to do so.
- The CE may not condition treatment, payment, enrollment or eligibility for benefits on the authorization.
- There is potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by HIPAA.

We recommend that, where feasible, the provider should be required to disclose its relationship to the app and indicate whether the app is covered by HIPAA.

A statement directed at the patient to the effect of, "Please ensure you refer to the app's terms of service and notice of privacy practices for further details" should be made.

Limitations and safeguards on sharing:

ONC should clarify that while API providers may impose security-related restrictions on app access (e.g., rate-limiting, encryption, and expiration of access tokens), it is inappropriate for API providers to set limitations on what a patient-authorized app can do with data downstream.

Given the nature of patient access rights, the provider is not in a legal position to prevent the registration of apps that would aggregate or share data, for example (though the provider might certainly decide to warn the patient, or endeavor to educate and explain these issue to the patient, as part of the provider-hosted app-approval workflow).

ONC should clarify that API providers are not obligated to protect patients by identifying suspicious apps. API providers may suspend API access to an app that has breached the API provider's terms of service, or appears to have been compromised, or if the app poses a threat to the provider's own system. The task force recognizes that there are thresholds of risk, and patients should be able to override some app suspensions if owed to a lower risk (except in the case where an app poses threat to the provider's own system or violates allowable terms of service). ONC and the relevant agencies should provide clear guidance as to the obligations of API providers when mitigating risk of a suspicious app.

ONC should coordinate with the relevant agencies the threshold of proof by which an app may be disabled in order to avoid considerations of information blocking.

ONC should update the certification requirements to ensure that API providers enable patients to share data with certain (coarse-grained, for now) limits, rather than all or nothing. Under the

updated requirements, patients should be able to view a provider-generated list of apps that currently have access to their records; revoke access at any time; and make sharing decisions that restrict the scope of access.

ONC should require that CHIT enable patients to share data with apps at the category level.

While we believe in the value of fine-grained permissions, we also recognize that implementing many narrowly-scoped access control policies would require a costly and difficult redesign of existing systems. Therefore, in the near-term we propose a pragmatic approach that ties back to the capabilities described in the 2015 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), ONC should ensure that patients can approve access at this same level.

ONC should update its data category request requirements to clarify that the first six elements of the Common Clinical Data Set (patient name, sex, date of birth, race, ethnicity, and preferred language) can be grouped into a single demographics category and exposed all together, rather than requiring six separate API calls for these data elements.

Auditing and accounting for disclosures:

We recommend that ONC expand certification criteria to require CHIT to make API access audit logs available to patients through an accounting of disclosures via the portal and show patients a list of all active app authorizations in the portal, include the ability for the patient to revoke any app authorization, and show patients a list of which apps have accessed their data via the API (including relevant details).

Working with the appropriate authorities, ONC should provide guidance to the EHR API developer regarding the information that should be logged to detail the disclosure by the API to the app, in terms of the "of what" information relevant to both the accounting of disclosures and the audit that may be used to meet requirements of the HIPAA Security Rule.

We recommend that ONC review the recommendations for patient authorization requirements to ensure CHIT audit capabilities sufficiently support an artifact that represents such patient authorization. The patient should be informed of the process which he/she needs to follow in order to flag any of the displayed disclosures as potentially inappropriate, which then could trigger an investigation by the provider. The patient flagging process should be supported electronically through the portal and not require any manual processes (such as faxing a signed complaint).

We recommend ONC coordinate with the relevant HHS agencies to publish patient-facing guidance that explains to patients what their rights are when the app developer is not covered under HIPAA as a Business Associate (and therefore not required to provide an accounting of disclosures).

While apps are not covered under ONC's certification program for health IT, and we are not suggesting that they should be, we do recommend ONC should provide guidance regarding voluntary best practices of audit capture and accountings for disclosures to developers offering apps that are intended to interact with CHIT.

We recommend ONC coordinate with the appropriate authorities, including states, to provide an easy-to-use educational resource that details for all API ecosystem actors (patients, providers, app developers and EHR API developers) the rules and responsibilities specific to breach notifications across all enforcement mechanisms (e.g., HIPAA, FTC).

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 stage 2-era patient portal sign-in and View, Download, Transmit (VDT). Specifically, a provider organization must have an appropriate level of assurance of a patient's identity, and must authenticate the patient through an appropriate mechanism. The same sign-up and login process that is used for portal access can and should be used to bootstrap API access. At the same time, ONC should continue working with other federal stakeholders including the National Strategy for Trusted Identities in Cyberspace to better define a national approach for identity management.

ONC should recommend that APIs should be secured via standardized mechanisms (such as OAuth) that allow patients and/or their authorized representatives to use existing provider portal account credentials during the app approval process.

ONC should indicate that API providers must not impose patient identify proofing or authentication barriers for API access that go beyond what is required for VDT access. APIs give the opportunity to provide simple and seamless access to patient information.

ONC should collaborate with the appropriate agencies to provide clear and distinct API developer and API appropriate usage privacy and security standards in order to encourage API development and adoption.

ONC should clarify that for registering patient authored apps (or any app authored by an individual to benefit only that individual or the individual's close relationships, such as family members), existing patient identity proofing and authentication is sufficient. In other words, 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 other apps, ONC should clarify that identity proofing of developers must be non-onerous and automatable (e.g., e-mail address or domain verification would be reasonable; a review of tax records or inspection of facilities would not).

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, and that providers must ensure that app approval and data access can occur without active involvement from the API provider or app developer. In other words, the only person who should have to take action to approve an app's access to patient data is the patient (or representative).

ONC should establish that an API provider's portal-based identity proofing and patient authentication procedures (i.e. the capabilities they use to enable access to patient portals) are deemed sufficient for granting an app access to the API.

Any process that presents a substantially greater burden to the patient for API access approval should be considered information blocking.

Discussion

Malec reminded the group that, this being a joint task force, members of both committees will vote. Tang referred to page 18, APIs, and the donation of genomic data, which may eventually be captured via APIs. He expressed concern about the complexities and implications of these aggregated data and the consumer's informed consent in the absence of any federal endorsement. API Task Force Co-chairperson Mandel responded by reminding Tang that the charge was to focus on the meaningful use

clinical data set, which does not include genomic data. Regarding sharing data permanently, permission should come with time parameters. Many players should be involved in endorsements. He referred Tang to page 22, recommendations 4.a and 4.b, as well as to the overview, saying that these recommendations were added to respond to Tang's comments at the previous meeting. API Task Force Co-chairperson Meg Marshall said that there are recommendations for an MPN and also for the authorization process. The recommendations focus on ONC's role, although other agencies have oversight and enforcement responsibilities. ONC should coordinate with those agencies.

Tang went on to talk about overreliance on the private sector. The FTC can only enforce what entities say they do, and bad actors will not say anything. The federal government could use the DoD criteria referenced in the report. Marshall asked for his opinion on the MPN, pages 22 and 23. Mandel declared that the recommendation is that ONC recommend criteria for an MPN.

Malec said that the task force seemed to be seeking a balance by stating that although patients should have the right to use any app to access their information, providers have a responsibility to protect their organizations and patients.

Paul Egerman thanked Marshall and Mandel for going directly to the recommendations without showing slides. He opined that the concepts of transparency and privacy notices help the vendor more than they help the consumer. Patients may not understand what it means for data to be sold. Unexpected disclosures can be very serious. Damage cannot be reserved. Providers should be able to prohibit apps. He informed them that he intended to vote again acceptance of the recommendations. Mandel agreed that there are risks, but opportunities are also present. He pointed to the recommendations (6.c and 5.b) that providers can turn off access to apps in certain situations. The task force wanted to balance this protection against any intent for data blocking. Marshall observed that it would be burdensome, if not impossible, to vet every possible app. The recommendations balance providers' rights and responsibilities to protect their systems with patients' rights. Egerman pointed out that physicians are responsible to do no harm. They should block an app if they believe that it may cause damage to the patient. Consumers could easily download the data and then run apps.

Blake read from the report that consumers testified that they wanted their data. The issue is whether the information goes directly to the app developer or first to the patient and then to the developer. In the latter case, the patient has the opportunity to view and review the data before sending it. Did the testimony raise this concern? Mandel reiterated that the charge was to look at APIs, which implies a certain workflow; otherwise, how would data reach the app? Blake replied that the patient would send the data. Mandel said that that flow is not an API interface, which is the charge. That workflow does not work well. The issue is the opportunity for the patient to have an easy workflow. Blake observed that the level of comfort with sharing data has increased now that insurers are prohibited from discrimination based on preexisting health conditions.

Kelly Hall reported that these issues were discussed in the task force. We already have VDT, so patients can review their data before doing anything with them. Patients say that choice is important. They already make important decisions. Patients can be taught. The opportunity for error is diminished with apps. Physicians have opportunity to inform their patients. Malec said that there are two legitimate policy preferences involved, and both are reasonable.

LeMaistre commented that there should be a mechanism for the physician to say that she disagrees with the app, similar to stating that something is against medical advice. Mandel said that page 18 describes the opportunity for the provider to disagree with a particular app or suggest that the patient reconsider its use.

Anjum Khurshid asked about downstream restrictions, saying that providers and patients can be considered a team. What if the provider believes that the patient would be harmed by an app? Mandel said that the task force members believe that both the patient's right to access and the provider's right to limit access must be protected. The provider can educate, inform and warn. The patient may want a second opinion. There are many use cases. The provider should not have to know what the app will recommend. Balance is required. Malec reminded everyone that under HIPAA, the provider cannot limit the patient's use of data.

Elmore asked that the recommendations be strengthened by eliminating the offer of optionality and recommending OAuth 2.0 specifically. Regarding authentication, greater clarity about identity proofing is needed. Mandel said that the task force agreed not to make technical recommendations, such as OAuth. The certification process focuses on functions rather than specific technology. Malec asked members not to repeat comments made by others.

Rose requested that a vote be delayed, given the complexity of the recommendations. He reported that he often gets requests for the release of records from patients who, he believes, do not have the knowledge base to use them appropriately. Although he nevertheless releases those records, he believes that it is a bad idea to allow apps to interface with the providers' records.

Petersen cautioned against making judgements about patients' ability to understand scientific evidence. Her experience with oncology patients indicates that patients are often able to master complex material to manage their health care. She offered to provide references supporting that concept. Patients often interact with complimentary care services without the involvement of their doctors. She would like to see consumers involved in enforcement of apps. Mandel responded that in recommending that federal agencies work together, it was assumed that consumers would be invited and involved. Marshall referred to page 11 on the role of the patient in lodging complaints. Marshall indicated that this section could be expanded to include Petersen's point.

In response to a request for clarification from Mann, Marshall said that the recommendation is to ask for clarification and clear guidance on the provider's right to refuse. There is a difference between provider's obligation and provider's right. Risk level should be considered. If a safety issue is involved, the provider should be able to block. The task force wants a balance but does not necessary have the answer. Mann noted that with an API, unlike with VDT, there is an ongoing relationship.

Someone asked about the extent to which the CE can encourage the use of its own app. CEs should be able to strike the balance. Do the recommendations address the limits of what parents can do? Mandel responded that recommendation 5.b says that API access is no different from access to the medical record in terms of minors and patient representatives.

Brent Snyder asked about security, endorsements, and limitation of risks. Mandel said that the patient approves sharing her data with an app. The patient can view any endorsements from organizations that she trusts. If an app is compromised or hacked, the provider can turn it off. But the patient still has the right to come back and turn it on. Marshall added (page 17) that the provider can notify the patient that the app has not received any certification or endorsement. Snyder said that he is more concerned about the risk to the provider organization. Marshall said that the task force followed HIPAA policy on access and protection of the provider's liability. The recommendation is to ask OCR for guidance.

Malec interjected that based on his understanding, bad app quality from a provider's point of view is a valid reason to shut down the app. He observed that although the task force's report is a long one, the discussion had been confined to a single policy issue. Members' comments and questions indicate a conflict between which should have greater weight—the provider's desire to protect the patient or the

patient's desire and right to use an app of choice. Tang disagreed, saying that the concern is that providers are patient advocates and need proper tools. His concern is the proscription on federal protection mechanisms and on provider intervention to protect patients. Malec declared that it could be possible to revise the document to better align with Tang's and Egerman's position. However, many members would be opposed to a motion to that effect; many will likely vote against the recommendations as currently stated. One path forward is additional deliberation to redesign the recommendations to accommodate the difference of opinions. Alternatively, the committees can just acknowledge the debate and differences and leave any resolution to ONC. Malec went on to say that the task force recommendations already follow ONC and OCR policies. Any action today will result in a significant minority vote, and it is FACA policy to strive for consensus. Malec requested a sense of the group by a show of hands. Mandel declared that the report reflects consensus of the task force after extensive debate. Further deliberation will not change the recommendations. Malec talked about finding a model that better reflects the desire for health care organizations to serve as advocates for patients and avoid harm. Egerman pointed out that it would not be fair to send the report back, because the task force had done good work. He preferred to take a vote and recognize the difference of opinions.

Malec said that he was looking for a solution that documents the difference of opinions. Blake referred to recommendation 6.b, which delineates the cases in which a provider may suspend the app. The next sentence states that the suspension may be overridden. Blake proposed a change in the paragraph to mirror the language in that section. If there are other concerns on the part of provider, the recommendation could say that the patient is notified of the concern. If DoD criteria have been adopted by some organization, failure to meet those criteria could become a legitimate reason to block the app. Malec said that the recommendations already include provider warnings. Comments about trustworthiness ensued. Mandel said that page 16 lists items pertaining to trustworthiness. It would be very difficult to delineate all criteria for which blocking is justified. That is why the task force left the decision to patients. Providers would not be required to vet in any way, which would add liability, according to Marshall.

Malec suggested adding that the provider organization can block if an app does not adhere to known good privacy and security guidelines. Kelly Hall was adamant that the decision rest with the patient. Malec announced an amendment to the effect that providers have every right to inform or warn patients of the risks associated with an app and require a signature that the patient has noted the warning. Someone observed that the amendment is not necessary, since warnings are included in the recommendations. Mandel said that he accepted the amendment as a clarification. Malec asked for a motion to approve the recommendations as amended. Cryer so moved, and the motion was seconded. Malec asked for a vote by the raising of hands and called on the members who were participating by telephone to state their vote. The count was 13 in favor and 10 opposed. The motion and the recommendations with one amendment were approved.

> **Action item #3: The recommendations of the API Task Force as presented, with one clarifying amendment to the effect that providers have every right to inform or warn patients of the risks associated with an app and require a signature that the patient has noted the warning, were approved by a vote of 13 to 10.**

Dale Nordenberg acknowledged his confusion, saying that a better consensus is needed. Providers always impose their practice patterns on patients; patients stay or leave. How is this situation different? If a provider denies use of an app, the patient is free to find another provider. Malec responded that although that may be a reasonable policy, it is not the pattern with which OCR and ONC have provided

guidance. Avoiding recommendations is not appropriate. The committees either put forward a minority report or modify the current report.

Wiesenthal remarked that it is a non-issue about what is convenient for patients. The physician can give advice, and the patient is free to reject it.

Tang offered another amendment to the motion already passed. If a list of required criteria for apps were put forth, the consumer would have better information and the FTC could back it up. The provider would be out of the loop. These would be criteria that apps must adopt. Malec asked whether that would imply that apps must use the privacy notice. Tang said that he was recommending that ONC delineate the required criteria. Marshall commented that endorsements are generally specific to a particular app. Tang replied that he is not using the term "endorsement"; the requirement would be a checklist for developers and would also inform consumers. It would be more of a requirement for doing business. Mandel asked how that would change the MPN. Tang seemed to indicate that the notice would be required.

Washington told the members to think about the activities without the technology. The recommendations do cover security. Patients can obtain their paper records regardless of the provider's perception of risk. Consensus may not be possible. There is a distinction between access for apps and what the app and the patient do with the information.

Malec observed that although many hands were up, it was time to adjourn the meeting. The recommendations were narrowly approved. The co-chairpersons will confer with staff regarding the best way to proceed. Consolazio asked members to email any remaining concerns to her.

Next Meetings: Virtual meeting June 8 and in-person meeting June 23

Public Comment

Adrian Gropper thanked everyone.

Two members of the public submitted comments via the Web meeting chat function.

Gary Dickinson, CentriHealth, wrote, "What effort is going to ensure that MACRA/MIPS does not create a greater burden on physician time spent on counting, measuring and reporting vs. time spent in actual clinical practice? Is this demonstrated in real practice settings?"

Steven Quentzel, GMA Consulting, wrote, "What 'provisions' would there be for integrating data from participants in clinicals and specifically those receiving blinded interventional therapy?"

Gary Dickinson wrote again, "Paul Egerman is right on.... It's not limited risk; rather it's unlimited risk."

SUMMARY OF ACTION ITEMS

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

Action item #2: The recommendations of the Precision Medicine Task Force on standards for the PMI were declared approved insofar as there were no objections.

Action item #3: The recommendations of the API Task Force as presented, with one clarifying amendment to the effect that providers have every right to inform or warn patients of the risks associated with an app and require a signature that the patient has noted the warning, were approved by a vote of 13 to 10.

Meeting Materials

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