# Joint HITPC and HITSC
# API Task Force
# FINAL
# Report of the January 28, 2016, Virtual Public Hearing

**Name of ONC Staff Liaison Present:** Rose-Marie Nsahlai

**Purpose of Hearing:** None stated

**Review of Agenda and Opening Remarks**

Task Force Co-chairpersons Meg Marshall and Josh Mandel thanked the staff for organizing the hearing and the panelists for their participation. Each panelist was given 5 minutes.

**Panel 3: Health Care Delivery**

Questions

- Does your organization use APIs for apps which are available internally or to third parties? If so…
- Do you publish your documentation online or make it available to third-party developers?
- How do you determine who can get access to your API?
- Do they need to be "certified" for privacy or security standards by your organization to use?
- Are there terms of use that include specific language for privacy and security?
- Are there production deployments of these APIs/third-party applications using APIs?
- Are there any well-known threats or vulnerabilities associated with APIs themselves that should be addressed (e.g., security engineering considerations/best practices)?
- As APIs are gaining adoption, are there steps organizations need to take to mitigate any additional threat vectors to data? Are these just specific to APIs in general? What might be unique/specific to health care?
- How does the issuer of the API ensure that the API won't become a tool used for malicious activity which could compromise the data source?
- How are APIs distributed in a way that the recipient/end user of the API can trust the API is authentic?
- How to improve consumer experience with the third-party apps using the APIs
- User stories/use cases
- Is there a catalogue or store of tools that are built for the APIs for third parties to access?

Stanley Huff, Intermountain, submitted written testimony. He described Intermountain's commitment to FHIR and SMART. Intermountain negotiated with Cerner Corporation to support standards-based services to all its customers. In conjunction with Cerner, Intermountain developed FHIR-based services. They borrowed services designed by Mandel's organization, including a growth chart application that is now used live in pediatrics. The concept is to support and use standard APIs, not proprietary ones. Many services and applications are still under development. Internally, Intermountain uses the same APIs for access to legacy systems.

Paul Matthews, CHCCN-OCHIN, did not have written testimony. His network works with a regional extension center in Oregon, school-based health centers, Federally Qualified Health Centers, behavioral health services, and health departments, to name a few. Health care organizations are learning that

correctly constructed APIs can be used in mobile applications, research, and data warehouses and to improve care by small providers. Matthews referred to an article on APIs as untapped resources in health care, published in the *Harvard Business Review*, that described four key points for exploiting those resources: offer financial incentives to encourage data exchange for outcomes, use OAuth and OpenID in response to concerns about privacy and security, implement standardized and open APIs, and show value to overcome resistance. According to Matthews, propriety APIs are in use, and their modification for each organization results in a large gap in the value of the data. Specification of vocabularies can create data gaps that increase the need for mapping and the frustration of users. APIs should not allow variation in the basics so that these tools are agnostic to EHRs.

Sean Kelly, Imprivata, submitted written testimony. He said that as an emergency physician, he strongly advocates for open frameworks that improve interoperability and access to patient data. Medically, ethically, and legally, access to data has a significant impact on care delivery. Kelly gave examples of the questions that should be answered upon arrival at the ED:

- What is the patient's medical history?
- Do they have a seizure disorder?
- Are they diabetic?
- Do they or their family have a history of heart disease?
- Is there any recent trauma?
- Is the patient on anticoagulants?
- What other medications do they take that could contribute to the differential or affect treatment?
- What is their code status? Do they have advanced directives and a health care proxy?

Kelly said that the fragmented databases storing patient information have become detrimental to delivering efficient and high-quality care. In the current system, if a patient is followed at another hospital that uses a different EHR, the information cannot be accessed in a timely manner, even when the hospitals are affiliated. Kelly advocated for enforcing standards of integration that promote an open framework with architecture that allows for secure access to patient information. This type of system may require supervised enrollment, credentialing, and access controls using strong authentication methods. Despite these steps, a system of this complexity is preferable to not being able to access patient data when they are needed. Good technology can actually reduce the complexity of such security and privacy standards, allowing for convenience and efficiency if implemented properly. This type of architecture already exists in many other industries in which privacy and security are of utmost importance. For example, in the financial sector, APIs and other mechanisms are used to ensure interoperability between institutions and customers in a secure and transparent fashion. The mortgage application process allows for participants to easily check credit scores and financial metrics. APIs in this sector also allow a consumer to give permission to financial institutions to perform the same functions on their behalf, including checking financial records and verifying eligibility for a loan. There are already proven methods in the health care industry and beyond that facilitate the secure exchange of potentially life-saving data while mitigating the risks of sharing that data. The risks of such interoperability are far outweighed by the risks inherent in not sharing essential data between caregivers. Lack of data interoperability is adversely affecting patients on a daily basis. Most health care professionals would support a standardized architecture allowing for exchange of data, even if it required enrollment ahead of time and strong authentication methods, such as biometrics.

Tim McKay, Kaiser Permanente, did not submit written testimony. He began with a description of his organization's system for interchange of data with patients and went on to talk about the API program documentation via the interchange portal. It includes (1) a sandbox for testing apps against data and technical guidelines and (2) FAQs. Developers must register to interact with the system. Interchange is not yet enabled for accessing patient-specific information. A critical first step will be to develop a comprehensive ecosystem infrastructure to ensure that access to patients' clinical information is secure.

McKay outlined management's concerns. One is the management of the potentially large volume of requests for device authentication and verification. However, he acknowledged that health care organizations do not have to develop independent programs for app security, privacy, and compliance certification. A second concern is that app and device authorization mechanisms that purport to act on behalf of the patient have not been fully proven, and the appropriate level of access to specific patient health information has not been well-defined in a policy or technical capability context. From the security perspective, it might not be sufficient that the app or device knows the patient username and password. A token-based approach to authorization would require a national ecosystem. The third concern is establishing and maintaining the common industry standard for audit logs. McKay indicated that until these innovations reach maturity, regulation is premature.

Brian Lucas, Aetna, Inc., submitted written testimony and showed slides. APIs should be easy to use and safe. Lucas described the health care business as having aligned economic incentives between payers and providers and set a goal of a simpler, more transparent consumer experience and technology that seamlessly connect to the health system. The system is transforming rapidly. More players are involved, and the data sharing needs are expanding. After 5 years of API development, Aetna has mobile, Web, voice, partner, and internal applications in production that consume APIs, touching most key constituent types. The manual process for access consists of internal and vetted external organizations that request access and manually controlled documentation. Participants must pass security and compliance assessments and agree to terms and conditions. Industry standard authentication and authorization methods are used to manage APIs. Moving into the future, Aetna sees open yet secure and compliant systems in a healthier world, with a digital ecosystem for information sharing. These systems will meet all constituents' privacy expectations and conform to regulatory compliance. This evolution will use the Roadmap to advance API usage. The old will be preserved, and the new will be advanced.

***Q&A***

In response to a question from Leslie Kelly Hall about a seal of approval, McKay said that his organization is working on a framework for certifying apps on a first level. The question is about the openness of the system—a system that is completely open to apps of choice or one that accepts well-known, more standardized apps. There may be need for some regulation. An HL7 standard is in development that would define and be embedded in workflow. One needs to look at an app from an engineering point of view in order to get to the correct granular level to certify. Huff asked that they use terminology correctly. Open APIs means that different companies create and openly publish them, but they are different for each company. In contrast, open standard APIs can communicate with any system in a standard way. Thus, they are much more beneficial than open APIs. Open standard APIs have exactly the same architecture and vocabulary. Mandel said that the focus of the hearing is the security and privacy aspects of APIs, rather than their data payload, which is out of scope for the task force.

Mandel went on to ask questions. What is the ideal way to determine which app to run? Who makes these decisions—the provider, the patient, or the third party? Huff acknowledged that his organization is not yet doing it. He hopes that in the future, there will be bodies that certify compliance with standards along with the opportunity to certify apps against a certain platform. A provider would ask a third party to test and certify a consumer's app in the provider's environment. Providers want to maintain the prerogative to decide. Matthews said that the willingness of small providers to pay for the certification must be taken into account. Both engineering and compliance needs must be considered. Matthews wondered whether a survey of patients' needs and desires has been conducted. The scale and cost of testing and certification are not known at this time. McKay added that any new software introduced in a system has a cost, such as regression testing, to consider all the things that can go wrong, which, in his experience, is 80% of testing costs. The system is hampered with problems of known patient identity, which are more complex with APIs. Lucas talked about problems with privacy and security, such as verifiable app identity codes, user identity, and linkage of the individual credential to the individual's data. Aaron Miri asked about precedence. The business case concerns whether API facilitation is the right method for exchange of information. Lucas said that APIs are the best method

currently known. Kelly Hall talked about granting patient access. Identity proofing is the key first step. Regarding patient health data, is there a difference between requesting data from an API and submitting data via API? McKay said that his organization is working on submission of data. There is an intermediate place for the aggregation of data, which are then pulled into the EHR. McKay is looking at a way to get metadata to know how the data were used or whether the data came from an FDA-approved device. Another issue is how to attach the app to the data set and then normalize and aggregate the data for use. Miri asked Kelly to explain how to trust the source of the data and their quality. Kelly talked about role and identity proof credentials, especially when putting data into the system. Should use and input be treated differently? Different levels of permission and authentication are required. Biometrics should be considered for provider proof to change or enter something into the medical record.

Marshall asked about scope negotiation to restrict access to less than the full dataset—for instance, the use case of 42 CFR Part 2 or a consumer's wish to restrict access. Kelly said that on the provider level, there are different levels of access based on hospital credentialing and monitoring; it is more complicated with patient-facing apps. It is difficult to restrict access to certain parts of the chart because of the associations between, for example, the problem list and the med list. Lucas described a distinction between the consumer and the application. If an app has no direct users, then it is granting access to data at a granular level. This is best controlled by controlling the app. Also, what can the user of the app get to, or what is the scope? On the provider side, access is based on role. For the consumer, the question is what user control can be put in place. One example of need to block is divorce in which one party may want to block a provider. A delegation model is needed, and the industry should help with a solution. Marshall asked Huff for his thoughts on barriers. Huff responded that much more work is required to get to systemic interoperability. To create a community, everyone should use the same configuration. Conformance testing could get in the way by certifying for every app for every platform. Certification should be an automated process. Someone interjected a question about patient-generated health data being held to the same standards as clinicians' data. Kelly responded that it is helpful to know where information comes from, such as the patient's reports on medication. Someone inquired about tracking provenance of data. Lucas said that provenance is tied with semantic ontology. Data provenance is important metadata, but health data are duplicated, replicated, recombined, and therefore difficult to track for provenance. Data pass through many systems and may be remapped or transformed. Huff commented that enough provenance should be available that the user can trust the accuracy of the data. There should be one trusted process for security with sufficient provenance for interpretation. Also, CDA documents are echoes of data. The principle should be that the original collector of data assigns a global identifier ID that accompanies the data throughout the system. Huff advocated stating this principle. McKay responded to another question, saying that it is difficult to design systems based on ideas; use cases are necessary. Consumer devices are made for patients to monitor their health, not to provide data for clinicians. When are data void? To be useful, the data should carry a date stamp and information about the manufacturer. Sometimes a patient narrative is needed to understand device data.

Mandel asked whether patients should be allowed to bring whatever apps they want, with the provider able to shut them down if they are malicious, or providers should give consumers information on which apps are appropriate. A panelist reported that he allows his patients to bring in images in any modality. The image goes to a broker, such as a radiologist, who decides whether it meets standards for usefulness. Mandel pointed out that he was interested in letting a patient use an app to connect to her data. McKay indicated that it is too soon to allow that access. The workflow must be considered. Some minimal vetting is essential, because many apps are bad or have no terms of use. An open system is unrealistic without a better understanding of the pitfalls. Huff agreed that it is too early for an open system. Eventually, there will be protections in place to open the system. Providers have a responsibility to open the system. Huff speculated that the design of protections will be market and provider driven. However, he acknowledged that a national discussion is needed. Miri opined that both regulation and incentives will be required, because organizations are hoarding their data. McKay cautioned that although open is a goal, the paths to the goal may differ.

Drew Shiller referred to the use cases mentioned and wondered to what extent APIs will solve all challenges or only consumer-driven challenges. Matthew answered that providers and consumers have different needs. Providers are subject to and primarily concerned with the compliance requirements. Compliance, not technical hurdles, is the block. Aaron Seib believes that there is a need for a better way for patients to express their desires in end-of-life care. Huff expressed concern regarding unintended results of rushing legislation. No good solution for workflow interoperability is available. Use cases must be delineated, followed by model designs.

Kelly Hall referred to a natural tension between privacy and security. With access to blue button, consumers will download to apps that are not connected to the health system. They will need education, but the day of approved use is gone. The regulations say that patients can select any apps; the burden for use and privacy is on the patient. Kelly Hall wondered how to accelerate access. Huff agreed that patients and providers can choose any app that they want, but the provider needs an infrastructure that prevents them from bringing the system down. The purpose of testing is to protect the health care organization from attack. McKay said that the entry and extraction of data are the primary concerns.

**Panel 4: Health IT Vendors**

Questions

- Does your organization use APIs for apps that are available internally or to third parties? If so…
- Are they clinician facing, or consumer facing (or both)?
- Do you publish your documentation online or make it available to third-party developers?
- How do you determine who can get access to it?
- Do they need to be "certified" by your organization to use?
- Are there terms of use that include specific language for privacy and security?
- Are there production deployments of these APIs/third-party applications using APIs?
- What are the perceived and actual privacy concerns or barriers to the adoption of APIs?
- What are the perceived and actual security risks or barriers to the adoption of APIs?
- Are there third-party certifying authorities in non-health care industry that we can leverage?

John Moehrke, GE Healthcare, submitted written testimony and one slide. He assured the task force that GE Healthcare is and has been a strong supporter of standards-based interoperability and is an active participant in standards development. He emphasized that RESTful APIs do not change security. Policy, rather than technology standards, is the primary challenge. Such policy issues focus on the roles and responsibilities for the various requirements regarding privacy and security operation: identity management, authentication, consent, accountability, and incident management. Patient identities are an especially problematic area of identity management. With no controlled patient identity, privacy cannot be managed or assured. This challenge applies to data management, consent management, and patient access management. User identities need to be managed by the health care provider organization. The health care organization must take responsibility for the functionalities of user provisioning, user de-provisioning, authentication, account recovery and suspension, account deletion, and monitoring. Vendors and applications can leverage the use of standards like OpenID Connect by using OAuth. Moehrke emphasized that the security and privacy challenges associated with APIs reflect and are a consequence of the wide variety of maturity among health care provider organizations in both policy and technology.

Chris Bradley, Mana Health, had no written testimony. He explained that his organization extracts the clinical and non-clinical patient-generated data sources and allows access to a unified view of the patient through a standards-based API. Mana Health also has a business line of patient portals. Bradley seemed to agree with other panelists that the main challenges are not technical ones. Although there are technological challenges, many are solved in other areas with high sensitivity to data privacy and security. One challenge is how to enable rapid securing of the APIs and security infrastructure. Several

questions must be answered: “Once I have access to this data through an API, how do I assign that ownership to the correct individual and grant access to the correct individuals?” “Where is the hierarchy of concept management?” “Who has access to what data at what time within that hierarchy?” When a care team is involved, the situation is much different from the involvement of the single patient.

Ted LeSueur, McKesson, did not submit written testimony. He read responses to each question. Regarding publication, he said that McKesson has not published its financial and consumer-facing APIs, although it plans to in the near future. Documentation is provided to third parties after a request and a technical review. After determining that a relationship is technically feasible and valued, McKesson requires the third party to obtain a software developer user license. Once that license is acquired, API documentation is available. Although a formal certification is not required, adherence to specific user terms and policies is required and attested to by the third party using the API. McKesson managers are considering broadening the reach of the APIs to consumer-facing applications that are not currently bound by the same regulatory obligations as the current APIs. A more formal certification process may be established. McKesson has deployments of APIs in production today across multiple business units. For example, it has a picture archives communication system, or PACS, and a document management system, to name two. Consumer-facing applications are not currently bound by HIPAA. There is not a generally adopted certification process or regulatory obligation. Patient consent is a critical part of the function, and McKesson has not adopted a trust framework for consent management. Security risks are the same as any interaction between applications—that is, ensuring the appropriate access controls. Right now, there is not a commonly agreed-upon framework to ensure that the applications accessing the API are not bad actors, so there is concern that if the data were incorporated into an insecure application, an unsuspecting consumer would be placed at risk. In the absence of a trust framework, each vendor will likely define its own framework with varying levels of tolerance. This variance could result in less risk-tolerant members being perceived as information blockers.

James Lloyd, Redox Engine, did not provide written testimony. He explained that his company has both provider- and patient-facing applications. Redox creates a standardized API for developers that can span multiple EHR vendors and variances among health care organizations. API assistance is provided publicly, and a user can start to build an application without needing to engage directly with the help of an application developer. Once the user goes to the top of the platform, Redox staff and the user go into the health system and assess the security and legal requirements of the system and go through any necessary steps for testing. Redox reviews all of the workflows and securities to guide the user through the process. Redox is live in production with a number of applications in a number of different industries and specialties. One of the biggest concerns is identity verification of the patient. Patients do not always know how to identify their health system, and lack of access to a directory can be a barrier. Government regulations can be the biggest bottleneck, and checklists would help.

***Q&A***

Mandel asked about shared responsibility of vendors and health care systems: What structures are in place for sharing? Bradley said that technology, policy, and documents are in place to track and audit access. The goal is to bring as much information as possible to authorized persons. The establishment of trust between the patient, the care team, and vendors involves a lot of people, so a standard should be created for these situations. To scale APIs, automated ways to give authority are required. Moehrke noted the great variability in organizations. Although a common set of rules and responsibilities is preferable, a one-on-one discussion is often required. However, that solution is not reproducible.

Shiller wondered whether a common API framework is possible. Lloyd believes that it would be challenging, given the current state of the ecosystem. In health care, there must be a balance of optionality and consistency. Some vendors are only partially implementing FHIR, which results in gaps. Lloyd wishes that FHIR standards were less optional. Bradley opined that ubiquity of standards will not be by legislation but by recognition of its universal value. Then technologies and policies around the APIs are necessary, for example, for patient identity. Vendors currently have to figure out the policies first. A

common framework is possible. Moehrke agreed, saying that everyone should focus on the basics. Customized APIs are not a solution. Privacy and security can be separated, and security models can mature at their own level. Good security models are available. Moehrke encouraged separation. HEART is not just for health care; various experts are involved. There are a number of policy problems to solve. Someone asked about low hanging fruit. Moehrke reported on an HL7 initiative to focus on document sharing and access to the documents by player-based interactions in SCX architecture. The new VDT function could include harmonization of identities, policies, and consent. Someone said that the ubiquity of one standard creates value. Once the API potential is understood, the technologies and policies around the API will be the challenge. Whether it is identical from system to system is not that important, as long as it follows basic specifications.

Kelly Hall said that the use case is to expose the common core data set to the ecosystem. She wondered whether it is doable. What about a seal of approval and regulation? What should be the lines between standards organizations and regulation? Bradley responded that regulation could clarify issues regarding access to the data. The common core is a good place to start. However, the use case in the inpatient setting is more difficult.

Mandel asked about designing standard APIs for data and normalizing the semantics versus designing security protocols. He wondered about focusing on a common set of authorization protocols ahead of time, even if they are authorizing different data APIs and the semantics of the data are not worked out. Would working on the authorization first have a better cost-to-benefit ratio? Bradley opined that both are essential. Data use cases require semantic and data modeling to access subsets of data. Standards and management of access are both needed and can be separated for very narrow use cases. More complex, cross-system use cases require not only that the API itself be secure but that a semantic and data-modeling language allow secure components of the dataset. Moehrke said that they should be separated. He mentioned that a security workgroup has worked on an interaction model that is independent of the security model. Many good security models are available, and they can mature at their own pace. Moehrke stated that he encouraged separation of the security and privacy layers from the data modeling and interaction modeling layers.

Mandel asked about working with providers to deploy apps and the timeline required for integration: Is time saved in the second deployment? Lloyd replied that 6–8 weeks are typically required for the coordination of reviews of approximately 10 checkboxes, each requiring different people. The time required for the health care system is shortened the second time, depending on the testing paradigm. Bradley observed that the time required for deployment is proportional to the organization's size and maturity. Every organization has to come up with policy and procedures first. A set of standards for security review for agreement would accelerate the process. LeSueur talked about a standard app versus a hosted one, saying that the hosted one may be less costly.

Shiller inquired about establishment of identity without a system of unique identifiers. Bradley responded that the challenge is to authenticate the identity and then link it to the correct records. Although the error rates for mismatches are low, the numbers are concerning when applied to the population. Lloyd reported that Saudi Arabia has a unique ID system, but problems with incorrect matches are common. Therefore, an organization must have policies on handling mismatches. There is always risk, and organizations must learn to manage it. Perhaps there are ways to engage consumers in management. Someone referred to the straightforward ways to establish and verify identity in the financial sector and wondered why it is more difficult in health care. Bradley repeated that identity is not the difficult part; the difficulty is linking the identity to the correct medical data. Panelists and members called out other differences: a set of questions to establish identity in financial services, revocable accounts, and use of evaluated levels of identify proofing. Kelly Hall pointed to several workflow differences. In addition, in banking, the record belongs to the bank; the customer does not change or contribute to the record. The patient must be protected while allowing the use of patient data.

Marshall asked the panelists about the supports of their business model. Bradley said that standards-based access would reduce barriers for small providers, even though there is variation across practices. Moehrke observed that standards would eliminate overhead. Regarding perceived privacy concerns, Bradley pointed out that institutions have to be concerned with regulation. Patients are much less concerned with privacy. Lloyd declared that different types of consumers have different concerns. The everyday patient has different concerns than the institution does. There are no data on the importance of privacy to patients. However, a trust framework is needed.

Kelly Hall referred to her experience of working with a medical ethicist. If interoperability is achieved by using APIs to move data around, who should be responsible for the privacy of the moving data? How can design incorporate patient responsibility? Moehrke acknowledged that, logically, it is the patient who has the most at stake for the use of these data. However, the momentum is with the decentralized system. The majority of patients want to trust the system. A smaller group of patients is concerned about control of their data. Kelly Hall disagreed, saying that data indicate that patients are using their data. She called for more transparency and openness and less need for trust. The current situation is one of trying to manage a void.

**Panel 5: Consumer Advocates**

Questions

- What are your concerns around privacy and security using APIs?
- How would you suggest the industry address these concerns?
- Are the topics that need to be clarified in the existing guidance or regulations?
- Are there production deployments of these APIs/third-party applications using APIs?
- What are the privacy and security concerns from the provider community as to the use of APIs?

Adrian Gropper, Patient Privacy Rights (PPR), submitted written testimony and one slide. He talked about the current gaps that affect patients' health. Gropper expanded on five key API points. A distinction between a patient-facing API and the FHIR API is unnecessary and undesirable. HIPAA explicitly allows patients to delegate direct third-party access to their records and lab results. Per HIPAA, the designated record set accessible via other means will also be available through a patient-controlled API. The HIPAA Security Rule, as applied to FHIR or to a patient-controlled API, could be misused for data blocking by institutions. Potential security gaps can be fixed by appropriate protection design of UMA, HEART, and FHIR so that the unified public API does not force a compromise between privacy and security. Gropper said that the JASON report and task force laid the foundation for the public API. Stakeholders must leverage the market forces behind FHIR and Argonaut to improve access by patient-directed third parties. The recent OCR guidance makes clear that HIPAA gives patients the right to have their health records and lab test results sent directly to a third party, even one that may be considered insecure or unwise by the covered entity or data holder. Paternalism is not legal. Unfortunately, according to Gropper, the current guidance can force the patient into accepting an insecure transfer method, such as unencrypted email, or the use of a slower and less reliable method, such as a direct email attachment. Data blocking will continue as long as covered entities and health data holders control which API apps or clients are safe under the HIPAA Security Rule. FHIR, HEART, and this task force must end the paternalistic, illegal blocking of patient access to EHR data and lab test results. FHIR and HEART should be harmonized to enable a public API by applying privacy engineering now, while the standards are still immature.

Mark Savage, National Partnership for Women and Families, submitted written testimony and showed slides. He said that APIs should ensure that all patient-facing functionalities are equally available through the API. There are significant privacy and security implications for patients who download their data through APIs or portals and upload them to applications of their choice. HIPAA's privacy and security protections do not apply to many commercial apps and personal health records unless provided by HIPAA-covered entities such as providers, payers, or their business associates. Applications and devices may have poor privacy policies, weak security controls, or policies that explicitly share data liberally with

third parties or allow broad uses. Many patients have limited understanding of how privacy and security protections change or end when they move health data from a HIPAA-covered entity to a third-party application or device. Savage recommended that ONC, OCR, and CMS collaborate on ways to educate consumers about their rights and steps that they should take to protect their data; examine policy options that improve privacy and security for patients who use apps and APIs to download and use their data; and educate providers (especially those in small practices), who are likely to receive questions from patients and family members about APIs, such as what they mean, how they work, and whether they are safe. API and application developers must communicate their privacy policies clearly, in plain language, to patients and consumers as well as providers. Access and use through APIs should be available at no cost to the patient. Savage described his organization's Get My Health Data campaign to help patients request their electronic health data and illuminate problems in the system along the way. His slides showed the results of a national survey of consumers about the use of technology and their health information.

Steven Keating, a self-defined patient advocate and an MIT PhD candidate, showed 25 slides describing his personal experiences with health care. Beginning with a description of the use of social media technology, he wondered why health care is so far behind other sectors. Health care organizations are still using fax machines, mailed CDs, and constrained patient portals. There are legal gray zones, a lack of tools and standards, and no translucency. Keating's slides described how access to his own data from a research study helped save his life. APIs should be standardized, open to third parties, and patient controlled and should provide full access to raw data. APIs should enable research data and patient-submitted data and should provide better measurement tools for API compliance.

***Q&A***

Seib asked about the importance and preservation of the right to have data sent by any method, including one that is insecure. Keating said that choice and responsibility should rest with the patient. Genome community contributors have to pass a test to ensure that they understand the risks before their participation is allowed. Regulations seemed to be designed for worst case scenario. Data and analysis can be separated, and patients should always be able to obtain their raw data. Savage talked about the importance of transparency and variability in choices. A member wondered how to educate and ensure that the patient has made an informed choice. Kelly Hall interjected that when the patient so indicates.

Mandel wondered how to foster systems to meet the needs of and protect consumers from diverse backgrounds with different needs. According to Keating, it can be done similarly to the way Apple runs its app store. There may be approved and experimental apps. People in critical situations should not be restricted to approved apps. Organizations should help to open up health information. 23andMe is one example. Anyone can download and use raw data. Patients complain that there is no way to send their data to these communities. The burden is always on the patient. An API could do that, along with scraper tools to use with portals. Gropper said that patients need to have the ability to direct their information to third parties. FHIR and the federal health architecture are available. Decisions should be made about what to pilot. Savage referred to his recommendations to allow for different choices by users.

Kelly Hall restated an issue. An app is registered to a patient. The vendor that provides the app is a business associate. Therefore, this is a new direct relationship between the patient and the vendor that is no longer governed by HIPAA. The app was selected by the patient without regard to any relationship between the patient and the covered entity. ONC and OCR need to develop guidance on the issue. Linda Sanches, OCR, interjected that OCR has updated the HIPAA access requirements. She declined to opine on Kelly Hall's example. She offered to work with ONC on clarification. Someone described another example. Initially, the relationship is between the subject and the covered entity. At first the third party may be unknown. When the third party shows up to ask how the data were used, UMA provides

separation from the patient-controlled element and the transaction of the data flow from the covered entity to the third party. The separation allows scalability, including for 42 CFR Part 2.

Seib asked for clarification on how UMA works. Someone said that consumer preference is held to a higher standard. With UMA and HEART layered on FHIR and using the same technology, the patient matching problem is lessened. The speaker added that the finance and credit model is not always applicable to health care. Credit is a choice. Health care is a right. There is not a right to be coercive in tracking patients.

Seib asked Gropper about separate APIs for provider organizations and consumers. According to Gropper, there should be a common set at the technical level. The constraints could be layered. There are ways to layer protections. The standards are the same standards, although the use cases are different.

Mandel inquired about anything on behalf of consumers that had not been mentioned during the Q&A. Keating urged the task force members to talk to the major companies about implementation. Mandel wondered what tradeoffs could be made regarding risks to patients. Deborah Peel, PPR, declared that the questions ignore a strong individual-rights culture. People feel strongly about making their own risk decisions. Paternalism is evident in the questions. Consumers want to compare care across organizations. Due to HHS, there is still no accountability and transparency about disclosures.

Gropper said that all the testimony presumes that patients do not have their own electronic records. This will change. Standards-based access to a record under patient control is the future. It cannot be assumed that patients cannot have their own technology. Keating talked about risks and compassionate care. Due to CLIA regulations, he does not have complete data on his tumor.

**Closing Remarks**

Marshall summarized, mentioning themes of a balance of a seal of approval and an open standards body, providers' obligation to protect, small providers' capacity, reduction of burden through standards technology, identity proofing and matching, and the importance of data provenance.

Mandel pointed out themes of the importance of standards-based APIs, whether authorization and standards can be separated, providers and vendors working together, government as a barrier, policy on mismatches, diversity of consumers, and the distinction between raw data and their analysis. An overarching theme is that although credit is a privilege, health care is a right.

**Public Comment**

The following written comments were received via chat during the meeting.

John Moehrke wrote, "The best approach I have seen to changing development/deployment culture is the 'Privacy By Design' initiative. GE Healthcare has adopted this a few years back."

Joseph Arnold, Aetna, wrote, "I would like to have the panel address what role to they see API Gateways in providing security and standardization?"

Ann Racuya-Robbins wrote, "Can we be reminded of the scope and meaning of privacy? Are you talking about a narrowly construed PII?"

Nick Saunders, Greenway Health, wrote, "Didn't clinics ask you to pay for those records though?"

Ann Racuya-Robbins wrote, "In the UMA context?"

Additional comments can be submitted via the chat or email.

**Next Steps**

The task force is scheduled to meet February 9.

**Flag to ONC Staff for Coordination:** None

**Meeting Materials**

- Agenda
- Panelist bios
- Questions
- Written testimonies
- Presentation slides

**Attendance**

| Name | 01/28/16 | 01/26/16 | 01/12/16 | 12/04/15 | 11/30/15 |
|---|---|---|---|---|---|
| Aaron Miri | X | X | X | X | X |
| Aaron Seib | X | X | | X | X |
| David Yakimischak | X | X | X | X | X |
| Drew Schiller | X | X | X | X | X |
| Ivor Horn | | X | X | X | X |
| Josh C. Mandel | X | X | X | X | X |
| Leslie Kelly Hall | X | X | X | X | X |
| Linda Sanches | X | X | X | | X |
| Meg Marshall | X | X | X | X | X |
| Rajiv B. Kumar | X | X | X | | |
| Richard Loomis | X | X | X | X | X |
| Robert Jarrin | | | X | X | X |
| Rose-Marie Nsahlai | X | X | X | X | X |