Health IT Joint Committee Collaboration

A Joint Policy and Standards Public Advisory Body on Health Information Technology
to the National Coordinator for Health IT

API Task Force

Update for Joint HIT Committee

Josh Mandel, Co-Chair
Meg Marshall, Co-Chair

March 10, 2016

API Task Force Membership

The objective of this membership mix is to have a small, diverse and nimble group of stakeholders to bring forth legitimate concerns re: APIs from multiple perspectives.

Member	Organization	Role
Josh Mandel	Harvard Medical School	**Co-Chair**
Meg Marshall	Cerner	**Co-Chair**
Leslie Kelly Hall	Healthwise	Member
Robert Jarrin	Qualcomm Incorporated	Member
Rajiv Kumar	Stanford University School of Medicine	Member
Richard Loomis	Practice Fusion	Member
Aaron Miri	Walnut Hill Medical Center	Member
Drew Schiller	Validic	Member
Aaron Seib	National Association for Trusted Exchange	Member
David Yakimischak	Surescripts	Member
Ivor Horn	Seattle Children's	Member
Federal Ex Officio		
Linda Sanches, Office for Civil Rights- Health and Human Services		
ONC Staff		
Jeremy Maxwell		
Rose-Marie Nsahlai, Staff Lead		
Maya Uppaluru		

Application Programming Interface (API)

Application Programming Interface (API) – a technology that allows one software program to access the services provided by another software program

- In its 2015 Edition CEHRT rule, ONC has included certification criteria for fully functioning APIs to support patient access to health data via view, download, and transmit (VDT).
- However, in discussing this concept in the proposed rule with our FACAs, *many members expressed concerns about privacy compliance and security of APIs*.

Therefore, the API Task Force was created to…

Task Force Charge and Questions

- **Identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in healthcare.**
  - For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example*, *identity proofing and authentication are not unique to APIs*);
- **Identify perceived privacy concerns and real privacy risks that are barriers to the widespread adoption of open APIs in healthcare.**
  - For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example*, *harmonizing state law and misunderstanding of HIPAA*);
- **Identify priority recommendations for ONC that will help enable consumers to leverage API technology to access patient data, while ensuring the appropriate level of privacy and security protection.**

2015 Health IT Certification Criteria – API Access

- ONC established new 2015 Edition criterion at § 170.315(g)(7) that requires health IT to demonstrate it can provide **a Consumer-facing** application access to the Common Clinical Data Set via an application programming interface (API)
- **At this time the Certification Criteria only requires Read-only APIs**
- Certification criterion is split into three separate certification criteria with each individual criterion focused on specific functionality to enable modularity and flexibility in certification
- The three certification criteria will be adopted at §170.315(g)(7), (g)(8), and (g)(9):
  - (g)(7) Application access—patient selection
  - (g)(8) Application access—data category request
  - (g)(9) Application access—all data request

https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-75

2015 Health IT Certification Criteria – API Access

- To be certified for the "API" criteria, three privacy and security criterion must also be met:
  - Section 170.315(d)(1) "authentication, access control, and authorization;"
  - Section 170.315(d)(9) "trusted connection;" and
  - Section 170.315(d)(10) "auditing actions on health information" or § 170.315(d)(2) "auditable events and tamper resistance."

https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-75

2015 Health IT Certification Criteria – 3rd Party Application Registration

- The intention is to encourage dynamic registration and strongly believe that registration should not be used as a means to block information sharing via APIs.[1]
  - Dynamic registration is that applications should **NOT** be required to pre-register (**or be approved in advance**) with the provider or their Health IT Module developer before being allowed to access the API.
- This is supported by the CMS Meaningful Use Stage 3 Final Rule
  - “Providers may not prohibit patients from using any application, including third-party applications, which meet the technical specifications of the API, including the security requirements of the API.” [2]

1. https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-102
2. https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications

CMS Meaningful Use Stage 3 Final Rule

- CMS included 2 objective in the Meaningful Use Stage 3 Final Rule [1], that references the use of APIs:
  - Objective 5: Patient Electronic Access to Health Information[2]
  - Objective 6: Coordination of Care Through Patient Engagement[3]
- CMS reiterates in these objectives that there are four basic actions that a patient (or patient-authorized representative) should be able to take:
  - View their health information;
  - Download their health information;
  - Transmit their health information to a third party; and
  - Access their health information through an API
- CMS believes that these actions may be supported by a wide range of system solutions, which may overlap in terms of the software function used to do an action or multiple actions, including facilitating provider-to-provider exchange as well as patient access
- CMS proposed for the Patient Electronic Access objective to allow providers to enable API functionality in accordance with the proposed ONC requirements in the 2015 Edition proposed rule

Out of Scope Issues

- Terms of Use
- Licensing Requirements
- Policy Formulation
- Fee Structures
- Certifying Authorities
- Formulation of Standards
- Electronic documentation of consents required by law or policy
- Issues unique to write-APIs

API TF Status

- 7 Meetings Held
  - Workplan extended
- Virtual Hearings
- OCR Presentation
- Use Case Definition/Team Assignments

Virtual Hearings

- Virtual hearings for the Joint API Privacy and Security Task Force were held on January 26th and 28th, 2016
- Panelists were represented from across both non-healthcare and healthcare industries
- Written testimonies have been gathered
- Public comments have been gathered
- Analysis has been conducted to summarize common themes captured across the two days of testimony and discussion

Virtual Hearing Panelists

January 26th		January 28th		
Panel 1- Consumer Tech 1	**Panel 2- Consumer Tech 2**	**Panel 3- Healthcare Delivery**	**Panel 4- Health IT Vendors**	**Panel 5- Consumer Advocates**
David Wollman, PhD- NIST	Alisoun Moore-LexisNexis	Stanley Huff, MD-Intermountain	John Moehrke-GE Healthcare	Adrian Gropper, MD- Patient Privacy Rights (PPR)
Stephan Somogyi-Google	Evan Cooke, PhD-US Digital Service	Paul Matthews-Oregon Community Health Information Network (OCHIN)	Ted LeSueur-McKesson	Mark Savage-National Partnership for Women & Families (NPWF)
David Ting-Imprivata	David Berlind-Programmable Web	Sean Kelly, MD-Imprivata	Chris Bradley-Mana Health	Steven Keating-Patient Advocate/Consumer
Greg Brail- Apigee	Marc Chanliau-Oracle	Tim McKay, PhD-Kaiser Permanente	James Lloyd-Redox Engine	
Eve Maler-ForgeRock	Shue-Jane Thompson, PhD-IBM	Brian Lucas-Aetna		
	Gray Brooks- GSA			

API TF testimony - Important Facts Shared on APIs

- API Resources can regulate how, when, and who uses the API
- APIs provide a well-documented, popular way for organizations to share access to data and services with third parties, while maintaining strict security controls.
  - Clear and concise documentation is important for open standard APIs
- API is extremely precise and allows the opportunity for all the right levels of access and security, e.g. data granularity
- Technical solutions exist for technical problems
- Need consensus best practices to help secure the API
- Business & legal considerations may remain.
  - Does it matter if the discloser "owns" the PHI or not?
  - Provider liability and accountability for data usage and breach, even though OCR/ONC Fact sheets say a discloser is not liable for what a receiver does with data so long as the discloser discloses the data properly.

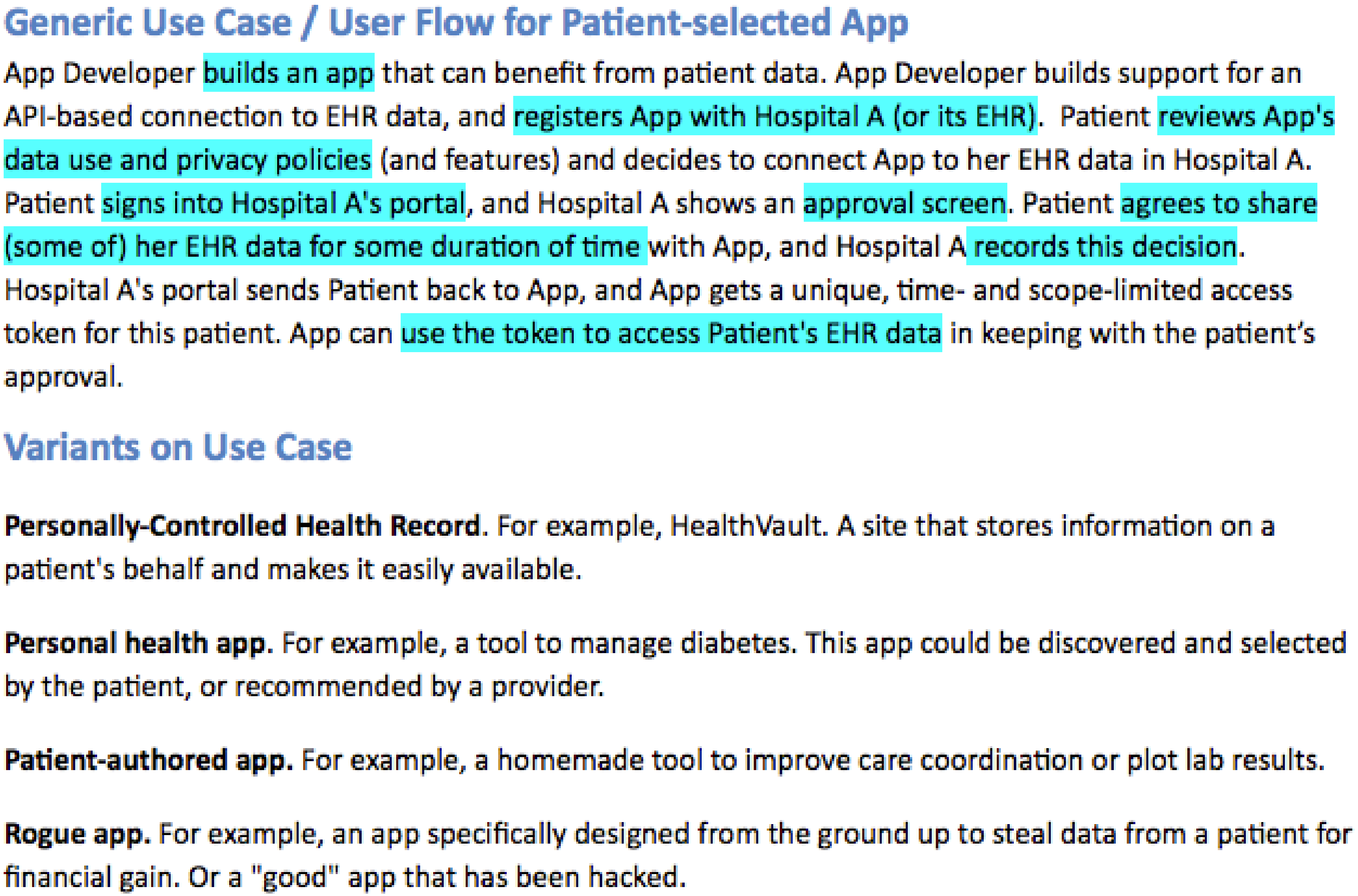
API TF testimony – Consumer Perspective

- More Access, More Patient Control, More Engagement
  - ✓ A panelist indicated access to his data helped save his own life, and asked "why can't patients have access to more of their own data?"
- Choices should be given to patient, and patients are smart enough to make privacy & security choices that are right for them.
- Systems should account for diverse consumers:
  - some want personally to control every decision;
  - some want health information to move where it needs to go without them having to manage that process.
- Transparent data practices are important for consumers
- Role of HIPAA in protecting consumer vs. protections outside HIPAA

API TF testimony – Healthcare Organizations

- Support for Open Standards-based APIs.
- Who do you trust? How do you know that person is accessing your system?
  - Need to verify identity of person accessing system, even through an app.
  - Need to verify that the app is operating on behalf of a verified person
  - Who is accessing and which apps are in use varies by role
    - Patient/individual/caregiver
    - Provider
    - Information systems administrator
- Long term, protections will be in place to allow for varying levels of access.
- Business and legal issues.

Generic Use Case/User Flow



Generic Use Case / User Flow for Patient-selected App

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

Variants on Use Case

Personally-Controlled Health Record. For example, HealthVault. A site that stores information on a patient's behalf and makes it easily available.

Personal health app. For example, a tool to manage diabetes. This app could be discovered and selected by the patient, or recommended by a provider.

Patient-authored app. For example, a homemade tool to improve care coordination or plot lab results.

Rogue app. For example, an app specifically designed from the ground up to steal data from a patient for financial gain. Or a "good" app that has been hacked.

Workplan

Meetings	Task
March 10 Joint Committee Meeting	• **Present themes at Joint HITSC and HITPC**
Tuesday, March 22 10:30am-12:00pm ET	• API Task Force Call
Monday, March 28, 10:30am-12:00pm ET	• API Task Force Call
Tuesday, April 12 10:30am-12:00pm ET	• API Task Force Call
April 19 Joint Committee Meeting	• **Present draft recommendations**
Tuesday, April 26, 10:30am-12:00pm ET	• API Task Force Call
May 4/5 Committee Meetings	• **Present final recommendations to HITSC and HITPC**