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

AGENDA

Joint Health IT Policy and Standards Committee Meeting
API Task Force
Virtual Hearing
January 26, 2016, 12:00pm – 4:10 pm ET

12:00 p.m.   **Call to Order/Roll Call**
– *Michelle Consolazio, Office of the National Coordinator*

12:05 p.m.   **Review of Agenda and Opening Remarks**
– *Josh Mandel, co-chair*
– *Meg Marshall, co-chair*

12:10 p.m.   **Panel 1: Consumer Technologies**
– *David Wollman, NIST*
– *Stephan Somogyi, Google*
– *David Ting, Imprivata*
– *Greg Brail, Apigee*
– *Eve Maler, ForgeRock*

2:00 p.m.   **Panel 2: Consumer Technologies**
– *Alisoun Moore, LexisNexis*
– *Evan Cooke, US Digital Service*
– *David Berlind, Programmable Web*
– *Marc Chanliau, Oracle*
– *Gray Brooks, General Services Administration (GSA)*
– *Shue-Jane Thompson, IBM*

3:55 p.m.   **Closing Remarks**
– *Josh Mandel, co-chair*
– *Meg Marshall, co-chair*

4:05 p.m.   **Public Comment**

4:10 p.m.   **Adjourn**

Panelist Questions

Questions for Panel 1: Consumer Technologies

1. Are there any well-known threats or vulnerabilities associated with APIs themselves that should be addressed (e.g. security engineering considerations/best practices)?
    a. As APIs are gaining adoption, are there steps organizations need to take to mitigate any additional threat vectors to data?
    b. Are these just specific to APIs in general? What might be unique/specific to healthcare?
    c. 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?
2. How are APIs distributed in a way that the recipient/end-user of the API can trust the API is authentic?
3. Are there existing metrics or is there a need to develop metrics to measure the maturity of security and privacy controls in the use of APIs?
4. Is there a catalogue or store of tools that are built for the APIs for third parties to access?
5. Are there known compliance implications with the use of APIs?
6. What are the perceived and actual security concerns or barriers to the adoption of APIs?
7. How can these risks be mitigated/how are you addressing this?

Questions for Panel 2: Consumer Technologies

1. Does your organization use APIs for apps which are available internally or to third parties? If so:
    a. Do you publish your documentation online or make it available to third party developers?
        i. How do you determine who can get access to your API?
        ii. Do they need to be "certified" for privacy or security standards by your organization to use?
        iii. Are there terms of use that include specific language for privacy and security?
2. Are there production deployments of these APIs/third party applications using APIs?
3. What are the perceived and actual privacy and security concerns or barriers to the adoption of APIs?
    a. How can these risks be mitigated/how are you addressing this?
4. How to improve consumer experience with the third party apps using the APIs?
5. Are there third party certifying authorities in non-healthcare industry that we can leverage?