# API Task Force Hearing

# Questions for Panelists

#### 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)?
	1. As APIs are gaining adoption, are there steps organizations need to take to mitigate any additional threat vectors to data?
	2. Are these just specific to APIs in general? What might be unique/specific to healthcare?
	3. 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:
	1. Do you publish your documentation online or make it available to third party developers?
		1. How do you determine who can get access to your API?
		2. Do they need to be “certified” for privacy or security standards by your organization to use?
		3. 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?
	1. 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?

#### Questions for Panel 3: Industry Sectors

1. Does your organization use APIs for apps which are available internally or to third parties?  If so:
	1. Do you publish your documentation online or make it available to third party developers?
		1. How do you determine who can get access to your API?
		2. Do they need to be “certified” for privacy or security standards by your organization to use?
	2. 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. Are there any well-known threats or vulnerabilities associated with APIs themselves that should be addressed (e.g. security engineering considerations/best practices)?
	1. 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 healthcare?
	2. 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?
4. How are APIs distributed in a way that the recipient/end-user of the API can trust the API is authentic?
5. How to improve consumer experience with the third party apps using the APIs:
	1. User stories/use cases
6. Is there a catalogue or store of tools that are built for the APIs for third parties to access?

#### Questions for Panel 4: Healthcare Delivery

1. How does your agency use APIs and apps today?
2. What are the security or privacy challenges you faced in standing the APIs up?
3. Are there liability and compliance implications from other federal agencies to consider?
4. What challenges and/or barriers have you seen with the growth of APIs in your departments/agencies/organizations?
5. What remains to be solved for your organization to take full advantage of this technology?

#### Questions for Panel 5: HIT Vendors

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