July 8, 2016

Karen DeSalvo, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. DeSalvo,

The Application Programming Interface (API) Task Force convened on November 30, 2015, as part of a joint collaboration between the Health IT Policy Committee (HITPC) and Health IT Standards Committee (HITSC), to address the privacy and security issues concerning the use of open APIs in healthcare. The recommendations, approved on May 17, 2016, were developed with consideration of the testimony from public and private industry stakeholders and experts during virtual hearings in January 2016.[1] [2]

Charge for the Joint API Task Force

In response to the 2015 Edition Certified Electronic Health Record Technology (CEHRT) Rule, which included certification criteria for fully functioning APIs to support patient access to health data via "View, Download, and Transmit (VDT)" and addressed concerns about privacy and security implications, a Joint HITSC and HITPC Task Force, the API Task Force, was formed.

The API Task Force was charged with exploring real and perceived privacy and security concerns and risks with APIs in healthcare, in light of the open/published read-only API requirements in ONC's 2015 Edition Rule (and related CMS rules). The goal of the proposed task force recommendations is to enable consumers to leverage API technology to safely access data with the appropriate level of privacy and security protections. ONC's API rule leverages consumers' right to access their own data and send it to a third party, including an app, under the HIPAA Privacy Rule.

Developing its Recommendations

The API Task Force held nine hours of virtual hearings in January 2016, where experts from non-healthcare specific consumer technology industries, healthcare providers, health IT vendors, payers, and consumer advocates provided written and verbal testimony on the privacy and security issues related to the use of APIs and web-based and mobile applications in a broader sense.[3]

Following the virtual hearings, the Task Force met approximately twice monthly through April 2016 to consider the information presented. Their deliberations also included a deep dive with staff from the

[1] January 26, 2016 Virtual Hearing: https://www.healthit.gov/FACAS/calendar/2016/01/26/api-task-force-virtual-hearing

[2] January 28, 2016 Virtual Hearing: https://www.healthit.gov/FACAS/calendar/2016/01/28/api-task-force-virtual-hearing

[3] For a complete list of panelists and each panel's specific prompt questions see the agendas for the January 26, 2016 Hearing here: https://www.healthit.gov/FACAS/sites/faca/files/APITF_HearingAgenda_2016-01-26.pdf ; and the January 28, 2016 Hearing here: https://www.healthit.gov/FACAS/sites/faca/files/APITF_HearingAgenda_2016-01-28_FINAL2.pdf

HHS Office for Civil Rights to understand the privacy and security legal landscape in which the Task Force's work was occurring. The Task Force Co-Chairs also supplied interim updates to the Joint HITPC/SC in February, March, and April. Finally, the Task Force Co-Chairs, Josh Mandel, MD and Meg Marshall, JD, presented the Task Force recommendation at the Joint Collaboration meeting on May 17, 2016 where a majority approved the recommendations. The final report is attached.

We note that the scope of the Task Force was quite limited, partly as reflected in the charge, and partly as a result of policies already enacted into laws and regulations, as are detailed in the report itself. Nevertheless, the complex and emerging landscape of consumer-mediated exchange and apps the individual chooses to use raise a number of areas of concern to the Joint Federal Advisory Committee. Committee discussion about these complexities and unknowns leads us to send, along with this transmittal, a further recommendation that ONC and its Federal Advisory Committees not only continue to monitor the App/API ecosystem, but also to ensure that the Advisory Committees have deeper knowledge of the experience of users of apps and of the mechanisms available to protect individuals from adverse privacy, security or health consequences of using apps.

Summary of Recommendations

The report provides extensive and detailed recommendations ranging over topics ranging from how apps should identify themselves to the APIs ("app registration") to privacy controls, to facilitating the growth of voluntary, private-sector led app certification programs. The high level summaries of the recommendations are included below. Where a recommendation stands alone, it is included in its entirety. Where a recommendation has several parts, they are summarized.

Recommendation 1: What Types of Apps Can a Patient Use:
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. Except for privacy considerations (addressed under Topic 4), the only relevant concerns should be technical compatibility (i.e. app works with the API technical specifications) and patient choice.

Recommendation 2: Registration as a Technical Requirement so APIs Recognize Apps:
Developers should be able to register the apps they develop in a self-service environment on the web. This process can be entirely automated, and should be frictionless, with no manual form-filling and no waiting period. A completed registration advances the app to the next state, a post-registration step called "app approval", where the API provider verifies the patient's identity and records the patient's decision to share. Registration and app approval should not be a barrier to patient choice.

Recommendation 3: App Endorsement:
ONC should encourage a market in app endorsements. To preserve patient choice, ONC should not require centralized certification, or the testing of apps. ONC should not use endorsement or the lack thereof as a reason to block registration or block patients from sharing information with an app. However, provider organizations may discuss, inform, and counsel their patients on the known benefits, risks, as well as any concerns about risks of using certain apps, as well as apps they endorse.

Recommendation 4: Privacy Practices of Apps
Recognizing that our laws do not regulate the privacy choices an individual makes for him or herself, nevertheless, ONC in conjunction with other federal agencies should pursue a concept of "privacy

literacy," similar to what is known as "health literacy." This includes defining the basics of privacy literacy, and outlining strategies and techniques for the government either to act directly - or through providers and app developers - to improve privacy literacy at the community and organizational level. An important component of this recommendation is supporting the adoption by developers of the Model Privacy Notice ONC has under development.

Recommendation 5: Authorization, or Ensuring the App is Authorized by the Patient to Receive Data: Providers need to be confident that Apps are legitimately acting on behalf of the identified patient, and that the patient wants the app to act for them. Therefore, until clear guidance is available, providers should define 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 or her valid, informed consent for the provider to enable the patient-directed app access to the patient's data. These processes, like registration (above) should be automated and on-line, and not result in unnecessary barriers to patient access. ONC could facilitate this by developing a model authorization form that can be built into provider portals and signed electronically without offline processing.

Recommendation 6: Limitations and Safeguards on Sharing:
ONC should clarify that while API providers may impose security-related restrictions on an app's access (e.g., rate-limiting, encryption, and expiration of access tokens) to the API provider's system, 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 or a conversation with the patient).

Recommendation 7: Auditing and Accounting for Disclosures
Knowing what apps have accessed a patient's data is an important transparency feature that will build trust with patients. 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 that function 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), among other features.

Recommendation 8: Connecting the Patient's Identity to the App.
ONC should provide guidance that the patient identity proofing and authentication requirements in an API ecosystem are not different from the requirements for MU2-era patient portal sign-in and View, Download, Transmit. The same sign-up and login process that is used for portal access can and should be used to bootstrap API access. While identity proofing is important, for a patient's chosen app, ONC should indicate that API Providers must not impose patient identify-proofing or authentication barriers for API access that go beyond what's required for "View, Download, Transmit" access. APIs give the opportunity to provide simple and seamless access to patient information.

We appreciate the opportunity to provide these recommendations and look forward to discussing next steps.
Sincerely yours,

Paul S. Tang, MD
Co-Chair, Health IT Policy Committee

Kathleen Blake, MD, MPH
Co-Chair, Health IT Policy Committee

Lisa Gallagher
Co-Chair, Health IT Standards Committee

Arien Malec
Co-Chair, Health IT Standards Committee