# HITPC-HITSC Joint API Task ForceReport of the April 12, 2016, Virtual Meeting

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

## Purpose of Meeting: Not stated

## Meeting Outcome

Subgroup homework assignment had been collected by staff, summarized on 26 presentation slides, and distributed to members by e-mail on April 11. A few minutes prior to the meeting, members were given access to late submission homework via Google docs. Task Force Co-Chairperson Meg Marshall began the meeting by directing attention to the Google document on consent and authorization. She asked whether members were comfortable with the definition of authorization. Talk ensued. Aaron Miri mentioned the importance of including consumer education. David Yakimischak preferred the word consent rather than authorization. Miri described the potential for confusion with the concept of consent in human subjects research, saying that authorization is a broader concept. Marshall declared that they will work off-line to clarify. She invited members to submit suggested language. Task Force Co-Chairperson Josh Mandel said that “HIPAA authorization” and “OAuth Authorization” could be used to clarify. Marshall moved to the next paragraph and read through the consent and authorization recommendations and their detailed qualifications. She said that the co-chairpersons will present preliminary recommendations slides to the HIT Joint Committee meeting; the background material to support the draft recommendations will be distributed with the meeting materials. Marshall reported that she and Mandel had discussed the recommendations with Leslie Kelly Hall, who was absent from the meeting. Kelly Hall was reportedly satisfied with the recommendations. Marshall apologized for not distributing the Google docs in advance of the meeting so that members could be better prepared for discussion.

Regarding consent and authorization, it was recommended that (summarized):

* ONC coordinate with the relevant agencies to publish guidance *as quickly as possible* for EHR API developers, app developers, providers, and patients, as to whether sharing data with a consumer-directed application counts as an individual's access, or access by a third party, or as a tool for engaging in treatment.
* ONC continue advancing work in support of standardized machine computable consent.  While this should not be considered a barrier to effectively exchanging data through APIs, standardized machine computable consent may be helpful for the “to what” aspects of the disclosure. Supporting the request of the API through a standardized, computable process could facilitate the response matching the request as accurately and completely as possible, and consistently across multiple systems.
* Until clear guidance is available, providers should proceed in defining practices for their EHR portals in a manner that focuses on ensuring the patient is in possession of all essential information in order to give his/her valid, informed “assent” for the provider to enable the consumer-directed app access to the patient’s data.  While we expect this is no different than what a patient is already asked to agree to for use of the portal given its ability to view, download and transmit, this ensures the “assent” represents the patient’s control to direct the disclosure (or use the app to make the request).
* The provider include statements, which are typical of HIPAA authorizations, to notify the individual of the right to revoke the app authorization, and provide a description of the process to do so; that the CE may not condition treatment, payment, enrollment or eligibility for benefits on the authorization; and the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by HIPAA.
* Where feasible, the provider be required to disclose its relationship to the app and indicate whether the app is covered by HIPAA.

Marshall agreed to make several clarifications suggested by members.

Marshall directed members’ attention to the draft document on auditing and disclosures. It was recommended that (summarized):

* ONC expand certification criteria to require CHIT to make API access audit logs available to patients through an Accounting of Disclosures via the portal.
* ONC coordinate with the relevant HHS agencies to publish patient-facing guidance that explains to patients what their rights are when the app developer is not covered under HIPAA as a BA (and therefore not required to provide an accounting of disclosures).
* ONC review the task force’s recommendations for patient authorization requirements in to ensure CHIT audit capabilities sufficiently support an artifact that represents such patient authorization.
* While apps are not covered under ONC’s certification program for health IT and we are not suggesting that they should be, ONC provide guidance regarding voluntary best practices of audit capture and accountings for disclosures to developers offering apps that are intended to interact with CHIT.

Miri requested that the recommendations include a point pertaining to a patient-facing guidance that clarifies the complaint process. In response to a question from Yakimischak about legal protections for patients in the absence of coverage under a BAA, Lucia Savage, ONC, reported that FTC is responsible for consumer protection against misleading, unfair and deceptive practices, as described on the FTC Website ([https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool](https://webmail4.altarum.org/owa/redir.aspx?SURL=TKXcu7nLUE6R8AoVEmFs4xlQThyFEDgfW2kJhO7ke2DJwBW0NmPTCGgAdAB0AHAAcwA6AC8ALwB3AHcAdwAuAGYAdABjAC4AZwBvAHYALwB0AGkAcABzAC0AYQBkAHYAaQBjAGUALwBiAHUAcwBpAG4AZQBzAHMALQBjAGUAbgB0AGUAcgAvAGcAdQBpAGQAYQBuAGMAZQAvAG0AbwBiAGkAbABlAC0AaABlAGEAbAB0AGgALQBhAHAAcABzAC0AaQBuAHQAZQByAGEAYwB0AGkAdgBlAC0AdABvAG8AbAA.&URL=https%3a%2f%2fwww.ftc.gov%2ftips-advice%2fbusiness-center%2fguidance%2fmobile-health-apps-interactive-tool)). Yakimischak wondered about clarification of the distinction between HIPAA and other forms of protection. Marshall indicated that the topic was covered in another section of the recommendations. She said that she will distribute that language for members’ feedback. A member opined against implying that better security is provided with CEs and BAAs. Miri talked about adding something about non-CEs being required to provide some notification of any breach. Someone said that FTC regulations include something on notification. Savage indicated that state laws often refer to breach notification. Some cloud services are provided by BAs, but some are not. She suggested that similar to the federal agencies’ agreement pertaining to apps, the task force could consider a recommendation about helping stakeholders to understand the rules regarding breaches and notifications. Since states and tribes are independent entities, federal agencies cannot dictate to them. It would be overly burdensome for ONC staff to collect and make available that state information to users. Marshall said that she will collect any additional comments and incorporate them into the final document.

Mandel walked through the recommendations slides on types of apps and organizations that provide them, registration process, and endorsement and certification. Regarding registration process, the members agreed to clarify the definition of registration to indicate that registration is between deployment and an organization and may be handled in different ways by vendors. Members also seemed to agree to add a recommendation that ONC clarify what registration is in order not to restrict access to apps and to add something about providing a way for patients to report problems. Regarding information blocking, there is a reporting path via OCR. Although there was not time to complete the discussion of endorsement and certification, members expressed their opinions on the pros and cons, including possible unintended consequences, of endorsements, as well as alternative processes for endorsements. Mandel reminded them that he wanted a discussion of the slides, which cannot contain too many details.

Preliminary recommendations of the following topics were not discussed: HIPAA-when does an app developer need a BAA; how do apps communicate their policies to users prior to sharing; limitations and safeguards on sharing; audit trail and recording requirements; identity proofing, user authentication, and app authentication; and general support for APIs. Members were told to review the meeting materials and send any corrections or suggestions to the co-chairs and staff.

## **Next Steps**: Preliminary draft recommendations will be presented to the HIT Joint Committee for discussion April 19. The task force will meet April 21.

## Public Comment:

Two members of the public commented via the Web meeting chat.

Kel Callahan, wrote, “MITRE has used Consent Management”.

He wrote again, “HHS Papers, studies and content has always referred to this process and Consent Management”.

Connie Patterson, Updox, wrote, “Where in the process should the testing/approval occur? Does ‘registration process’ refer to the 3rd party registration with a Health IT vendor (which should include testing and some type of vetting to ensure the app developer is who they say they are) or does this refer to registration by the patient to access their info via the app?”

Later, Callahan, HIPAAT, added an oral comment, saying that although he was late to the call and therefore missed some content, he has been engaged in software solutions for consent management for many years. He was concerned with the consent and authorization language, saying that there are many ONC resources on patient preferences regarding consent and consent directives. He urged the task force to be consistent with the historical use of these concepts. He pointed to a subtle difference between security construct as related to authorization and the privacy construct related to disclosure. He went on to recommend that they address purpose of use. He acknowledged that he had not reviewed the meeting materials.

## Flag to ONC Staff for Coordination: None.

## Attendance

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | 04/12/16 | 03/28/16 | 03/22/16 | 03/08/16 | 02/22/16 | 02/09/16 | 01/28/16 |
| Aaron Miri | X | X | X | X | X | X | X |
| Aaron Seib | X |   | X | X | X | X | X |
| David Yakimischak | X | X | X | X | X | X | X |
| Drew Schiller | X | X | X | X |   |   | X |
| Ivor Horn |   | X |   | X |   | X |   |
| Josh C. Mandel | X | X | X | X | X | X | X |
| Leslie Kelly Hall |   | X | X | X | X | X | X |
| Linda Sanches | X |   |   | X | X | X | X |
| Meg Marshall | X |   | X | X | X | X | X |
| Rajiv B. Kumar |   |   |   |   |   | X | X |
| Richard Loomis | X |   | X | X |   | X | X |
| Robert Jarrin | X | X |   |   |   |   |   |
| Rose-Marie Nsahlai | X | X | X | X | X | X | X |