HIT Privacy & Security Tiger Team Meeting
April 9th, 2012

Overview
The April 9th meeting of the HIT Policy Committee consisted of a discussion on the Stage 2 Meaningful Use NPRM and the Tiger Team's recommendations that were not included in the proposed rule.

Background
The HITECH Act, part of the American Recovery and Reinvestment Act of 2009, was passed to help promote the adoption of health information technology (HIT) and create a better health care system. The Privacy & Security Tiger Team was created to promote collaboration among the various HITECH created entities. The Tiger Team consists of members from both the HIT Policy and HIT Standards Committees as well as representation from the National Committee on Vital and Health Statistics and outside experts.

Summary of Meeting:

Discussion of Meaningful Use Stage 2 NPRM
Deven McGraw & Paul Egerman, Co-Chairs

Objective: Continue efforts to reach agreement on comments to be provided on the proposed rules to the HIT Policy Committee on the May 2nd meeting.

Focus on previous HITPC recommendation that were not adopted in the proposed rules:
- Patient Portals: secure download, authentication, mechanism to block programmatic or unauthorized attacks; also concerns from HITSC about transparency, security
- EHR modules
- E-Prescribing of Controlled Substances (EHR capability)
- *Digital certificates: testing of use
- *Patient Matching and Demographics: address normalization, testing of demographic formats

*Topic will be addressed in a future meeting later in April.

Patient Portals
Recommendations not included in the NPRM
1. Require testing of certified EHR technology for authentication of patients (using at least single factor) and secure download
    - Proposed rule states that such technical implementations are commonplace & ubiquitous and therefore do not need to be required for certification
2. Require certified EHR technology to include capability to detect and block programmatic and unauthorized user attacks (note: Standards Committee put forth different recommendation)
3. Require certified EHR technology to include requirements for data provenance that is accessible to patient/user
4. ONC should provide guidance to providers and hospitals to enable them to be transparent with patients about benefits and risks of portals

Actions:
- With regards to the first recommendations of this section the Tiger Team decided against making any additional comment because creating a simple authentication requirement may be a hindrance to the development of more secure authentication methods.
- The second recommendation was ignored in favor of adopting the language in the NPRM, which originated in the HITSC. The Tiger Team also recommends that technical advice be created by the ONC or NIST to help adopters.
- The NPRM language for recommendation three is fine, but the Tiger Team reiterates that the provenance information has to be seeable and readable from the consumer perspective.
- Recommendation four should be reiterated in the recommendation, even though it does not require any changes to the NPRM.

EHR Modules

Background

- Stage 1 final certification requirements required EHR modules to be tested for all privacy and security certification requirements (except in certain circumstances)
- Stage 2 proposed rule eliminates this requirement and instead requires the Base EHR to be certified for all privacy and security requirements.
- The HIT Standards Committee adopted a different recommendation – implement or demonstrate capability to achieve through integration

Action: The Tiger Team decided to abstain from making a recommendation on the NPRM in this area, but would like to add that if a module is being certified for most of the Base EHR requirements it should also be certified for Privacy & Security standards.

E-Prescribing of Controlled Substances

Recommendations not included in the NPRM

1. Policy Committee recommended that certified EHR Technology have capability to support such 2 factor authentication as required by DEA interim final rules
2. ONC declined to propose for Stage 2, noting potential policy conflicts with state law and challenges with widespread ability of products that include functionalities to support DEA requirements
3. ONC requests comment on availability point.

Action: No comment for Stage 2 on this issue and address in Stage 3 if necessary.