Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

November 21, 2013
Jacob Reider, MD
Acting National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Reider:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team:
The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic HIE, and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to ARRA and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

This letter provides results of HITPC/Privacy and Security Tiger Team discussion on data intermediaries to the National Coordinator, Department of Health and Human Services (HHS).

Background
In advance of Stage 3 of the EHR Incentive Program, the HIT Policy Committee (HITPC) and the Quality Measures Work Group (QMWG) convened a subgroup, the Data Intermediary Tiger Team (DITT), to make recommendations on data intermediary roles, including those related to privacy and security. The goal was to have certification criteria that would allow data intermediaries to serve as the module for quality reporting functionality. Related to this effort, the HITPC Privacy and Security Tiger Team was asked to provide guidance on whether there are privacy and security considerations to be addressed as part of the certification process for data intermediaries.

Previous Recommendations
In September 2010, the HITPC made recommendations on data intermediaries, which it referred to as "third party service organizations," as follows:

- **Collection, Use and Disclosure Limitation**: Third party service organizations may not collect, use or disclose personally identifiable health information for any purpose other than to provide the services specified in the business associate or service agreement with the data provider, and necessary administrative functions, or as required by law.
- **Time limitation**: Third party service organizations may retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider, and necessary administrative

functions. Retention policies for personally identifiable health information must be established, clearly disclosed to customers, and overseen. Such data must be securely returned or destroyed at the end of the specified retention period, according to established NIST standards and conditions set forth in the business associate or service agreement.

- **Openness and transparency**: Third party service organizations should be obligated to disclose in their business associate or service agreements with their customers[1] how they use and disclose information, including without limitation their use and disclosure of de-identified data, their retention policies and procedures, and their data security practices.
- **Accountability**: When such third party service organizations have access to personally identifiable health information, they must execute and be bound by business associate agreements under the Health Insurance Portability and Accountability Act regulations (HIPAA). However, it's not clear that those agreements have historically been sufficiently effective in limiting a third party's use or disclosure of identifiable information, or in providing the required transparency.

The HITPC/Tiger Team concluded at the time that while significant strides had been made to clarify how business associates (Bas) might access, use and disclose information received from a covered entity, business associate agreements (BAAs), by themselves, did not address the full complement of governance issues, including oversight, accountability, and enforcement. The Tiger Team recommended that the HITPC oversee further work on these governance issues.

Tiger Team Deliberations

In reviewing these recommendations, the Tiger Team concluded that they were still sound but the discussion again raised concern about the inadequacy of BAAs in limiting BA disclosure and use, and in promoting transparency regarding BA disclosures and uses of health data, both identifiable and de-identified. In light of these continuing concerns, the Tiger Team deliberated on potential vehicles for implementing its previous recommendations on third party service organizations/data intermediaries including (1) Meaningful Use Stage 3 requirements and/or (2) the CMS Proposed Rule on Revisions to Payment Policies under Physician Fee Schedule.[2] Under one or both of these rules, the HITPC/Tiger Team considered whether to require providers to:

- Attest that any BAA with a data intermediary provides for transparency to the provider[3] of data uses and disclosures of health information by the BA and
- Provide a copy of BAA provisions focused on transparency.

Another option considered was to define quality measures that only use data already in the EHR, thus limiting the number of intermediaries involved.

[1] The "customer" of a third party service organization data is the provider or other entity that hires the organization to perform a service on its behalf.

[2] The NPRM proposed to define a ''qualified clinical data registry'' (QCDR) for purposes of the PQRS as a MS-approved entity (such as a registry, certification board, collaborative, etc.) that collects medical and/or clinical data for the purpose of patient and disease tracking to foster improvement in the quality of care furnished to patients. The NPRM proposed QCDRs must enter into and maintain with its eligible professionals appropriate BA agreements that provide for QCDRs' receipt of patient specific data from the EPs as well as public disclosure of quality measure results. (78 FR 43362; 7/19/2013)

[3] Providers have the option of disclosing these data uses to patients in their HIPAA Notice of Privacy Practices or other transparency venues.

Ultimately, the Tiger Team concluded there was not an appropriate policy vehicle available at present to hold BAs accountable for greater transparency to providers around their uses and disclosures of identifiable health information. Regarding a possible attestation requirement, the Tiger Team concluded that attempting to hold providers accountable for the behavior of data intermediaries was problematic and there was a lack of policy vehicles available under the HITECH incentive program to directly regulate these entities. The Tiger Team also noted the potential large number of data intermediary BAs, and the difficulties inherent in identifying them and in defining the precise meaning of "BAA provisions focused on transparency." The HITPC/Tiger Team reserves the option, as always, to revisit this issue as the environment continues to evolve.

Key Points

Although the HITPC is not making additional recommendation at this time, it would like to share key points raised during the Tiger Team deliberations and offer these to ONC for further discussion and consideration. In particular, this discussion highlighted a serious concern that the superior bargaining power of large data intermediary BAs results in providers being "forced" to agree to BAAs/data use agreements (DUAs) granting BAs broad rights to future uses and disclosures of provider data. Specifically, the Tiger Team saw the following as key issues:

- Patient control & autonomy – patients have no say in whether or how data intermediaries use their information; further, these uses are not transparent to patients
- Proliferation of data intermediaries – the larger the number of data intermediaries that hold patient data, the greater the risk that problems will occur

This discussion led the Tiger Team to the belief that from a privacy and security standpoint, it may be desirable to define quality measures in such a way that they can be derived from the data already in EHR systems, thus limiting the number of data intermediaries that need to be involved. The Tiger Team further recognized that other balancing factors (not the least of which is the need for robust measures) may need to be considered. It ultimately concluded that such a recommendation would be beyond its scope, but offers the results of this discussion to ONC for further consideration.

We appreciate the opportunity to provide these recommendations on data intermediaries and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee