Health IT Policy Committee

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

August 23, 2013
Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

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 recommendations to the National Coordinator, Department of Health and Human Services (HHS) on provider queries for patient health information and the subsequent response from the data holder, for the purposes of direct treatment.[1]

Background
Query and response actions among different providers are a regular occurrence in health care today. Many of these transactions are conducted via paper, faxes, or verbally via telephone. The Tiger Team considered challenges and questions raised when this process is automated.

There are existing laws that address the issue of query and response in health information exchange among disparate or unaffiliated providers. HIPAA and state laws regulate when most health care providers are permitted to disclose identifiable protected health information (PHI), including in response to a query for records. It is important to note, however, that these rules permit, but do not require, providers to release PHI in a range of circumstances. As a result, if there are uncertainties, such as with respect to potential liability for improper disclosure or breach, providers may choose not to disclose data to minimize their risk. The rules also leave the judgment about the timeliness of a response to a query up to the provider/data holder.

[1] "Direct treatment" is defined as a health care provider delivering health care directly to the individual. Direct treatment does not include "indirect treatment," which is defined as a health care provider delivering health care to the individual based on the orders of another provider and reporting the results to the health care provider, who then provides them to the individual.

The Tiger Team identified three query scenarios, as follows:

1) Targeted Query, where a provider is querying another specific provider (or specific providers) known to have seen the patient, for direct treatment, with HIPAA as the controlling law;
2) Targeted Query for Direct Treatment, with stronger privacy laws controlling; and
3) Non-targeted Query for Direct Treatment, where the patient's providers are not known and which involves looking for a patient's records using information about the patient (versus querying one or more specific providers).

At the April 4, 2013, HIT Policy Committee meeting, the Tiger Team initially presented recommendations on query and response for health information exchange for each of three scenarios above. These recommendations are not intended to alter existing rules that vest providers with the duty to share patient information responsibly and within the bounds of the law. Instead, these recommendations are intended to reduce potential real or perceived barriers to responding to a query consistent with a provider's professional obligations and the law.

Further, these recommendations are based on the existing obligations of the data holder and the requester. Specifically, the data holder:

- Needs some reasonable assurance as to the identity of the entity requesting the data,
- Needs some reasonable assurance that the querying entity has, or is establishing, a direct treatment relationship with the patient,
- Makes a decision about whether to release data, and if so, what data, consistent with law, and
- If responding, needs to send back data for the right patient, and needs to properly address the response and send it securely.

The requester:

- Needs to present identity credentials,
- Must demonstrate (in some way) the treatment relationship, and
- Must send patient identifying information in a secure manner to enable the data holder to locate the record(s).

Scenario 1 Recommendations: Targeted Query for Direct Treatment Under HIPAA

The Tiger Team began its query and response discussion with Scenario 1, which is defined as a provider requesting PHI from another specific provider (or other specific providers) about a particular patient for direct treatment purposes. The query and response in this scenario are controlled by HIPAA; no stronger privacy laws apply.

Responding to the goal of providing clarity to both the requester and the data holder on satisfying their legal and professional obligations, the Tiger Team answered six questions. For questions 1 and 2, the answers provide possible options for addressing requester and data holder obligations and are not intended to be exhaustive.

1) *What supports "reasonable" reliance, by the data holder, that the requester is who they say they are? (Possible solutions)*
    a. The use of a DIRECT certificate may provide reasonable assurance of a requester's identity to the data holder. When issued at the entity level, the expectation is that entities have identity proofed and authenticated individual participants as per HIPAA.

b. The requester may have membership in a network (HIO, vendor network, integrated delivery system (IDS), virtual private network (VPN), etc.) that the data holder trusts.
c. The requester is known to the data holder, such as through a pre-existing relationship.

2) *What supports "reasonable" reliance, by the data holder, that the requester has (or will have) a direct treatment relationship with the patient –and in this direct treatment scenario, therefore has legal authority and is otherwise authorized to obtain the data? (Possible solutions)*
   a. A data holder's own knowledge or history of the requester and patient's relationship is sufficient to determine the requester and patient's direct treatment relationship.
   b. A data holder may have the capability to confirm a requester's direct treatment relationship with a patient within a network or IDS.
   c. A network that the data holder trusts has rules providing accountability for false attestation, such as penalties against the requesting entity.
   d. A requester may provide some official communication of patient consent that does not conflict with expressions of patient wishes known to, or on file with, the data holder.
   e. There may be a known existing treatment relationship with the patient. The requester may have previously sent a query for the patient to the data holder.

3a) *Does it matter if the data holder makes the decision to disclose data or if the data holder's response is automated (set by the data holder or automatic by participation, such as in a network)?*
   a. Yes. The data holder may make a decision to automate a response to a query and should adopt policies to govern when automatic responses are appropriate. Such policies should be linked to the degree of assurance the data holder has about identity and the legal authority to disclose data, based on the existence of a direct treatment relationship.

3b) *To what extent does automation trigger our previous recommendations on the need for meaningful choice by patients?*
   a. If the data holder maintains the ability to make decisions on when to disclose a patient's information, they can choose to automate their decisions (following similar policies customarily used to release patient information). However, if data holders do not have discretion over record release policies, the Tiger Team's previous recommendations on "meaningful choice" for the patient apply.

4) *What patient identifying information should be presented as part of the query?*
   a. A requesting provider's query should, ideally, present no more (but also no less) PHI than what is needed to accurately match to a record.
   b. A query should start with available demographics before using more specific information.
   c. The HITPC/Tiger Team's previous recommendations on matching should be implemented.[2] These recommendations called for (1) a standardized format for data matching fields, (2) healthcare organizations/entities to evaluate the effectiveness of their matching strategies as a means of improving accuracy, and (3) matching to be enforced through governance, (4) ONC to establish a program(s) to develop and disseminate best practices in improving data capture and matching accuracy, and (5) increased patient access to their health information and the establishment of audit trails to track where information has been accessed.

5) *How should data holders respond to a query?*

[2] See: http://www.healthit.gov/sites/default/files/hitpc-transmittal-letter-priv-sectigerteam-020211.pdf

    a. Silence is not an appropriate response. Data holders should respond to queries in a timely manner by either providing i) some or all of the requested content or ii) a standardized response indicating the content requested is not available or cannot be exchanged. This approach is based on the provisions of the Data Use and Reciprocal Support Agreement (DURSA), the participation agreement for the eHealth Exchange. (It should also be noted that even acknowledgement of the existence of a record is PHI.)

6) *Should there be a requirement to account for and log query and/or disclosures, and should the log be shared with the patient upon request?*
    a. Yes. The data holder should log both the query from an outside organization and the response, regardless of its content. The requester should also log the query. This information should be available to the patient upon request.

The above recommendations were approved by the Health IT Policy Committee at the April 4 meeting.

Scenario 2 Recommendations: Targeted Query for Direct Treatment Under HIPAA and Other Laws
This scenario has similar actors to scenario 1, but is subject to additional laws. Scenario 2 is defined as targeted queries for direct treatment purposes that are subject to HIPAA and more stringent privacy laws that typically require patient consent or authorization before PHI disclosure. Additional laws may be stronger state privacy laws or other federal laws such as federal substance abuse treatment laws. Recommendations are as follows:

1) Data holders and requesters must comply with the laws or policies that are applicable to them. Patient consent or authorization may be required prior to a query and/or release of PHI.
2) The form of consent must comply with applicable law. The requester and data holder must each have a form that satisfies their legal requirements (if applicable). These forms may not be the same.
3) As a best practice and to assist providers in complying with applicable law and policies, parties to a query/response should have a technical way to communicate applicable consent/authorization needs or requirements, and maintain a record of such transactions. For example, data holders may need to communicate with a querying entity that a particular patient authorization is required before data can be shared; the data holder (and in some cases the requester) may need or want to record the communication and the authorization. As another example, data holders sharing data subject to 42CFR Part 2 (substance abuse treatment regulations) may need to communicate restrictions on "redisclosure."
4) The HIT Standards Committee should further consider technical methods for giving providers the capacity to comply with applicable patient authorization requirements or policies. A "one size fits all" approach may not apply given current technologies. Entities may also use a service to meet their needs in this area.

These recommendations also were approved by the Health IT Policy Committee at the April meeting.

Scenario 3 Recommendations: Non-Targeted Query for Direct Treatment
In this scenario, the patient's providers are not known and the query involves looking for a patient's records using information about the patient as opposed to directing the query to one or more specific, known providers. This scenario may require use of an aggregator service (such as a record locator service, data element access service, or health information exchange) to find possible sources of the record.

At the April Policy Committee meeting, the Tiger Team also recommended, with regard to non-targeted queries, that patients should have meaningful choice as to whether or not they are included in an aggregator service that permits queries from external providers. Meaningful choice can be triggered in circumstances when the provider (or provider's organized health care arrangement or OHCA[3]) does not have control of the decision to disclose or exchange the patient's identifiable health information.[4] For example:

- An HIO operates as a centralized model, which retains identifiable patient data and makes that information available to other parties.
- An HIO operates as a federated model and exercises control over the ability to access individual patient data.
- Information is aggregated outside the auspices of the provider or OHCA and comingled with information about the patient from other sources.

The Tiger Team noted that in a non-targeted query scenario, meaningful choice also may be triggered by network or other participation arrangements that prevent the provider from following his/her/its policies customarily used to release patient information.

The foregoing recommendation regarding meaningful choice also was approved by the Health IT Policy Committee at the April meeting.

In May, the Tiger Team followed up these recommendations with a preliminary conclusion that the recommendations were sufficient to address non-targeted queries as well. At that time, the HITPC advised that it would like to see further deliberation on the matter of policies for non- targeted queries for treatment, recommending that the Tiger Team hear from practitioners in the field on the state of non-targeted query for treatment and reconsider existing query recommendations in light of the information gathered.

---

[3] *Organized health care arrangement* (45 CFR 160.103) means:
(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment a activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
[provisions applicable to health plans omitted]

[4] See September 2010 HITPC Recommendations to ONC, available at:
http://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

Subsequently, the Tiger Team held a hearing on this issue on July 24, 2013, receiving testimony from eight operational models of non-targeted query and the policies governing those queries. A number of themes emerged from the testimony, specifically:

- Access to each network is controlled to members who have executed some sort of participation agreement (binding them to abide by any query limitations or other network policies). These agreements are executed with the data holders and, in some instances, with the EHR vendors.
- Each network provides patients with some choice; most are opt-out but some are opt-in. Many adopt a model where the data is held by the network but is accessible only for those patients who have either opted-in or have not opted out. One network testified that data does not move into the HIE without opt-in consent.
- For sensitive data, most depend on the data partner to withhold data requiring additional consent, or other types of sensitive data. One network made information subject to 42 CFR Part 2 (substance abuse treatment data) available in the HIE (but only to providers who specifically request it, subject to a second consent from the patient, and subject to a second attestation of a treatment relationship; also reminder provided about re- disclosure limits). In many networks, patients who have concerns about access to sensitive data in the HIE are counseled to opt-out (or not to opt-in).
- Many of the networks do have role-based access levels for participants.
- All networks do audits of access/disclosures, but only some make directly available to patients.
- None do an override of patient consent - some have emergency break the glass in circumstances where patient has not yet provided any form of consent.
- All networks limit access to certain purposes -- treatment is common to all; many others also allow for operations and public health reporting purposes; a couple allow for payor/payment access.
- Most have some either inherent or express geographic limits. There is the possibility to do nationwide health information exchange, but right now, this capability is limited. l
- Testifiers expressed some concern about having federal policy potentially disrupting the arrangements they had carefully implemented; however, most expressed a desire for some guidance/common agreement terms that would help facilitate network to network (or HIE to HIE) exchange, and additional guidance on how to handle sensitive data.

The Tiger Team also noted a number of other issues that may warrant further consideration but were outside the scope of deliberations on query/response. Specifically, the hearing highlighted the state of the trust framework upon which current health information exchange occurs. This framework is built upon numerous trust agreements with data holders, some across state lines. In addition, there was concern that record holders may withhold data for variety of business reasons. The Tiger Team believes that ultimately, the data should go where the patient goes to maximize patient care. Other issues may include payer and public health access through query and the adequacy of governance, particularly with regard to HIE to HIE transactions.

In hearing the testimony, the Tiger Team recognized the great care and effort the HIEs and others took in crafting policies and operations that worked for their particular participants and communities. As a

result, the Tiger Team reaffirmed its previous conclusion that existing recommendations on meaningful choice and targeted query are sufficient in addressing non-targeted queries, and that no additional policy was needed at this time. (As always, the Tiger Team reserves the option to revisit these recommendations in the future as conditions change.) This conclusion was presented to the Policy Committee at its August meeting and was approved.

Finally, the Tiger Team seeks to reiterate the complexity of the policy issues triggered by the prospect of sharing more sensitive health information protected by more stringent privacy protections, as articulated by the Tiger Team and the Policy Committee in its August 19, 2010 recommendations to ONC on the issue of consent.[5] Providers frequently raise concerns about the impact of more stringent privacy protections on patient care and workflows; at the same time, patient advocates worry that failure to protect this information would create barriers for patients seeking confidential care for sensitive conditions. Technical methods should ideally help facilitate compliance with existing sensitive health data laws and policies but without adding so much complexity that providers and others involved in facilitating health data exchange leave sensitive data out of exchange altogether.

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

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee

[5] Sept 2010 HITPC Recommendations to ONC, available at:
http://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf