Department of Health & Human Services
Office of the National Coordinator for
Health Information Technology

Privacy and Security Tiger Team

Report to the Health IT Policy Committee Meeting

April 3, 2013

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, Epic
- **Leslie Francis**, University of Utah; NCVHS
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **David McCallie**, Cerner Corp.
- **Wes Rishel**, Gartner
- **Latanya Sweeney**, Carnegie Mellon University
- **Micky Tripathi**, Massachusetts eHealth Collaborative
- **Kitt Winter,** Social Security Administration

Tiger Team Query/Response Background

- Query and response actions among different providers are a regular occurrence in health care. What new challenges and questions are raised when automating this process?
- HIPAA and other laws regulate when most health care providers are permitted to disclose identifiable protected health information (PHI), including in response to a query or request.
- The rules *permit, but do not require,* providers to release PHI in a range of circumstances.

Tiger Team Query/Response Background

- Tiger Team’s goal is to reduce potential real or perceived barriers – such as through clarification regarding provider liability for responding to a query – to enable them to respond to external queries consistent with their professional ethical obligations and the law.
- Today we are presenting recommendations on query and response for consideration by the Policy Committee.

Tiger Team Query/Response Scenarios

- **Addressing three scenarios to achieve goal.**
  - ✓ **Scenario 1:** Targeted Query for Direct Treatment, controlled by HIPAA
  - ✓ **Scenario 2:** Targeted Query for Direct Treatment, controlled by stronger privacy laws
  - ✓ **Scenario 3:** Non-targeted Queries. (Tiger Team is finalizing recommendations.)

Scenario 1: Targeted Query for Direct Treatment Purposes Among Covered Entities

- HIPAA controls
- Assumptions
  - Patient Z is being seen by Provider A
  - Provider A has knowledge that Patient Z has been seen by Provider B
  - Provider A queries Provider B for records (targeted query in a trusted environment for direct treatment purposes)

Scenario 1: Existing Obligations

- Data Holder (Provider B)
  - Needs some reasonable assurance as to the identity of the entity requesting the data.
  - Needs some reasonable assurance that querying entity has, or is establishing, a direct treatment relationship with the patient.
  - Makes decision about whether to release data, and if so, what data, consistent with law
  - If responding, needs to send back data for right patient, needs to properly address request, needs to send securely.
- Requester (Provider A)
  - Needs to present identity credentials
  - Must demonstrate (in some way) the treatment relationship
  - Must send patient identifying information in a secure manner to enable data holder to locate the record

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions

1) What supports "reasonable" reliance, by the data holder, that the requester is who they say they are (identity)?

Possible answers that support reasonable reliance:

a) Use of DIRECT certificate (when issued at entity level, expectation is that entities have id proofed & authenticated individual participants per HIPAA)

b) Membership in a network (HIO, vendor network, IDS, VPN) that the data holder trusts

c) Requester is known to data holder (such as through a pre-existing relationship)

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

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?

a) Data holders own knowledge/history with requester

b) Capability to confirm within network/IDS

c) Network that data holder trusts has rules providing accountability for false attestation

d) 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) Known existing treatment relationship with patient (e.g. there already exists prior requests for the patient from the external provider)

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

3) Does it matter if data holder makes the decision to disclose or if the data holder's response is automated (set by data holder or automatic by participation, such as in a network)?

Yes. Data holder may make decision to automate response and should adopt policies to govern when automatic response is appropriate. Such policies should be linked to the degree of assurance data holder has about Q1 (identity) or Q2 (legal authority to disclose data, which in this scenario is based on the existence of a direct treatment relationship).

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

3b) To what extent does automation trigger our previous recommendations on the need for meaningful choice by patients (see backup slides for reminder)?

- 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, our previous recommendations requiring "meaningful choice" for the patient apply.

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

4) What patient identifying information should be presented as part of the query?
   - Ideally no more (but also no less) than what is needed to accurately match.
   - Start with available demographics

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

Policy Committee previous recommendations on patient matching should be implemented:

1. A standardized format for data matching fields is needed
   - HITSC should propose such standard formats
   - EHRs should be tested and certified for interoperability re: standard data fields
   - HITSC should develop recommendations on missing data
   - HITSC should consider benefits of a USPS validation/normalization
2. Health care organizations/entities should evaluate the effectiveness of their matching strategies to internally improve matching accuracy
3. Matching accuracy should be enforced through governance. HIEs should be required to establish programs that ensure matching accuracy by participants and how to respond if incorrectly matched.

**Source: Feb 2011 HITPC Patient Matching Recommendations
http://www.healthit.gov/sites/default/files/hitpc-transmittal-letter-priv-sectigerteam-020211.pdf

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

4. ONC should establish a program(s) to develop and disseminate best practices in improving data capture and matching accuracy.
5. Increase patient access to their health information and establish audit trails to track where information has been accessed. Set simple process for reporting corrections to their information.

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

5) Data holders should respond to queries consistent with their professional and legal obligations. (Note that even acknowledgement of the existence of a record is PHI.)

- Data holders have a duty to respond to queries in a timely manner by either providing:
    i. Some or all of the requested content
    ii. A standardized response indicating the content requested is not available or cannot be exchanged (DURSA).

Scenario 1 (Targeted Direct Treatment, HIPAA): Relevant Questions (cont.)

6) Should there be a requirement to account for and log query and/or disclosure, and to share the log with a patient upon request?

- Yes. The data holder should log both the query from an outside organization and the response, regardless of its content. The requester also should log the query. This information (query and response logs) should be available to the patient upon request.

Scenario 2 (Targeted Direct Treatment, Sensitive Data)

- Similar to Scenario 1 in terms of actors and transactions
- Difference is that Targeted Query for Direct Treatment Purposes will fall under not only HIPAA, but other law or policy requiring consent before PHI disclosure

Scenario 2 (Targeted Direct Treatment, Sensitive Data)

- Recommendations:
  - Data holders and requesters must comply with the laws or policies that apply to each. In some cases requesters must obtain the patient's consent/authorization prior to a query; in some cases the data holder must have the patient's consent/authorization prior to releasing PHI.
  - The form of consent must comply with applicable law – i.e., the requester must have a form that satisfies their legal requirements (if applicable), and data holders must have the form that satisfies their legal requirements (if applicable). These forms may not be the same.

Scenario 2 (Targeted Direct Treatment, Sensitive Data)

- Recommendations:
  - 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 42 CFR Part 2 (substance abuse treatment regulations) may need to communicate restrictions on “redisclosure.”

Scenario 2 (Targeted Direct Treatment, Sensitive Data)

- Recommendations:
  - The Standards Committee should give further thought to technical methods for giving providers the capacity to meet their needs re: complying with applicable patient authorization requirements or policies. This may be an area where “one size fits all” is neither possible nor desirable given current technologies. Entities may also choose to use a service to meet their needs in this area.

Scenario 2 (Targeted Direct Treatment, Sensitive Data)

- 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.** 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.

**Source: Sept 2010 HITPC Recommendations to ONC
http:// www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

Scenario 3: Non-Targeted Query for Direct Treatment Purposes

- Assumes patient’s previous providers are not specifically known, so this is an initial query to find the locations of a patient’s record(s).
- May require use of an aggregator service (such as a record locator, data element access service, master patient or health information exchange) to find possible sources of record.
  - Should patients have meaningful choice re: whether or not they are included in an aggregator service that permits queries from external providers? Yes.

Scenario 3: Non-Targeted Query for Direct Treatment Purposes

- Seeking Policy Committee input on the following question:
  - Should querying entities be required to limit queries (e.g. by geography, list of providers, etc.)?

Query/Response

BACK-UP

Meaningful Choice

- Providers give patients enough knowledge to understand how their information will be shared and with whom. Patient can make informed decision on the exchange of their health information.
  - Decision is made with advanced knowledge/time
  - Not used for discriminatory purposes or as condition for receiving treatment
  - Made with full transparency and education
  - Commensurate with circumstances for why PHI is exchanged
  - Consistent with patient expectations
  - Revocable at any time

**Source: Sept 2010 HITPC Individual Choice Recommendations
http:// www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

Meaningful Choice Triggers

- Meaningful choice can be triggered in circumstances when the provider (or provider's organized health care arrangement, or "OHCA") does not have control of the decision to disclose or exchange the patient's identifiable health information.
  - Examples:
    - A HIO operates as a centralized model, which retains identifiable patient data and makes that information available to other parties
    - A 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.

**Source: Sept 2010 HITPC Individual Choice Recommendations
http:// www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf