Privacy and Security Tiger Team

Report to the Health IT Policy Committee Meeting

March 14, 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 reporting to the Health IT Policy Committee on the approach we are taking and the status of our discussions to date. We aim to present final recommendations on this topic at the April meeting.**

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

Scenario 1 (Direct Treatment and HIPAA)

- **Scenario 1**: A provider has requested PHI from another provider about a particular patient for direct treatment purposes. The query and response in this scenario is only subject to HIPAA.

Scenario 1 (Direct Treatment and HIPAA)

- **Existing Obligations**
  - For **data holder**, needs some reasonable assurance of requester's identity and existence of direct treatment relationship with patient; must make decision about whether to release data (consistent with law); must send data on right patient and send securely.
  - For **requester,** need to present identity credentials, must provide assurance of a treatment relationship, and must send identifying information in a secure manner to enable data holder to locate record.

Scenario 1 (Direct Tx and HIPAA) Questions

1) **What supports "reasonable" reliance, by the data holder, that the requester is who they say they are?**
   - DIRECT certificate, Network membership that data holder trusts, or 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 is authorized to obtain data?**
   - Data holder's knowledge of requester, network attestation, patient consent, or known existing relationship.

Scenario 1 (Direct Tx and HIPAA) Questions

3) **Does it matter if the data holder makes the decision to disclose as opposed to the response being automated (set by data holder or automatic by participation, as in a network)?**

- Yes. Data holder should adopt policies to govern when automated response is appropriate.

3b) **To what extent does automation trigger need for meaningful choice by patients?**

- Data holders can automate their decisions (i.e. through an algorithm) if they have the ability to make decisions on when to disclose PHI. Meaningful choice recommendations apply when data holder no longer has capacity to decide on record disclosure.

Scenario 1 (Direct Tx and HIPAA) Questions

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. Rely on previous recommendations re: matching accuracy (e.g., use of particular data field not required; providers, institutions and HIEs should evaluate their data matching strategy accuracy on an ongoing basis; etc.).

5) **How should data holders respond to a query?**
   - 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. (DURSA)

Scenario 1 (Direct Tx and HIPAA) Questions

6) **Should there be a requirement to account for and log query and/or disclosures, 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. This information should be available to the patient upon request.

- Should the requester also log the query?

Additional Scenarios

- **Scenario 2:** Targeted queries for direct treatment purposes will be subject to HIPAA and other laws and policies requiring consent before PHI disclosure.

- **Scenario 3:** Non-targeted query for direct treatment purposes assume that the patient's previous providers are not known. A record locator service or master patient index may be used to find possible sources of the record.