# Privacy and Security Tiger Team

## Report to the Health IT Policy Committee: June 24th Hearing on Non-Targeted Query

July 9, 2013

# Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, Martin, Blanck, and Associates
- **Judy Faulkner**, Epic
- **Leslie Francis**, University of Utah College of Law
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **David McCallie**, Cerner Corporation
- **Wes Rishel**, Gartner
- **Micky Tripathi**, Massachusetts eHealth Collaborative
- **Kitt Winter,** Social Security Administration

# Purpose of Virtual Hearing

- An effort to understand what sort of policies are deployed to ensure that a “non-targeted query” for a patient record is appropriate, legal, and authorized.
- Focus of the hearing was on policy, and not security methodologies or identity management issues.
- Such policies may include limitations on who can conduct the query, the purposes for which a query can be conducted, geographic or other limits and parameters intended to help assure proper access, and also intended to help demonstrate that the requester is authorized to access a patient’s records.

# Purpose of Virtual Hearing

- The Tiger Team was particularly interested in environments where there are limitations placed on access to the record via query. Examples include, but are not limited to, partial access to the record, geographic limits and purpose, such as limiting queries to those for direct treatment. Some HIEs may have inherent limitations, based on factors such as geography in the case of a regional HIE. The TT was also interested in hearing of instances where limiting policies were considered but not adopted.
- The Tiger Team also wanted to learn about the thought processes behind the development of any such policies.

# Scope: Non-Targeted Queries

- The Tiger Team's focus was on queries between disparate entities [Does not include queries within an integrated delivery system (IDN) or organized health care organization (OCHA)]
- In this scenario, a patient's other providers may not all be known in advance.
- Thus, non-targeted query involves looking for a patient's record using information about the patient (versus querying for a patient's record by asking one or more specific provider organizations).

# Scope of Non-Targeted Queries

- Involves use of an “aggregator,” such as a record locator service (RLS), data element access service (DEAS), or health information exchange (HIE).
- In deliberating on query/response, the Tiger Team focused on use cases involving direct treatment relationships, but were interested in hearing about how non-targeted queries are used for other purposes.

# Panelists (1 of 2)

- Nebraska Health Information Initiative
  - Deb Bass, CEO
  - Sara Juster, Vice President, Compliance for the Nebraska Methodist Health System and Privacy Officer for NeHII
  - Connie Pratt, Program Manager, Bass Inc.

- HealtheWay
  - Mariann Yeager, Executive Director
  - Martin Prahl, Health IT Consultant, Social Security Administration

- Rochester (NY) Regional Health Information Organization
  - Ted Kremer, Executive Director

- Indiana Health Information Exchange
  - John P. Kansky, Vice President of Strategy and Planning

# Panelists (2 of 2)

- Rhode Island Quality Institute’s CurrentCare
  - Laura Adams, CEO and President
  - Charlie Hewitt, Director of HIE Program Management

- Surescripts
  - Paul Uhrig, Executive Vice-President, Chief Administrative & Legal Officer, Chief Privacy Officer

- ClinicalConnect
  - Christian Carmody, President, ClinicalConnect HIE and Vice-President, UPMC Enterprise Infrastructure Services
  - Tracy Crawford, Program Director

- SMRTNet
  - Joanna Pardee-Walkingstick, Director of Member Services

# Questions (1 of 2)

1. How have you operationalized non-targeted queries? Please describe the process.
2. How long have you been operational with your approach and how many patients are involved?
3. Is there an inherent scope limitation associated with your entity that affects providers' ability to perform non-targeted queries (e.g. geography)?
4. What additional limits are placed on non-targeted queries (e.g., who can query, for what purpose and scope of query)?
5. What roles do patients have in limiting queries? Are there circumstances in which patient preferences are over-ridden? If so, how does that process work and have there been any problems?

# Questions (2 of 2)

6. How do patients exercise “meaningful choice” as to whether their records are included in your “aggregator service”? Does this extend to the release of the data or does that require additional consent?
7. How do you address exchange of sensitive information in a non-targeted query model?
8. What information is returned to a requester as a result of a non-targeted query?
   A. If you exchange sensitive information, is there a difference in what is returned when such information is involved?
9. In what environment and for what providers have non-targeted queries proven to be the most effective? Please provide appropriate metrics if available.
10. What challenges/problems have been created by your approach? What adjustments have you or do you plan to make to your approach?
11. Would having widely applicable policy (or guidance) on providers’ ability to perform non-targeted queries be helpful? If so, what should those policies be?