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

August 7, 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

Agenda

- Final recommendations on
  - Non-Targeted Query
  - Meaningful Use Attestation for Security

Background

- Query scenarios (all involving queries among disparate organizations):
  - Scenario 1: Query to one or more specific providers (“targeted”), HIPAA controls
  - Scenario 2: Query to one or more specific providers (“targeted), data covered by additional law requiring patient consent or authorization prior to PHI disclosure)
  - Scenario 3: Query based on patient demographics, using aggregator to find patient (“non-targeted”)

Background

- In April, the HIT Policy Committee approved recommendations from the Tiger Team on targeted queries for treatment, aimed at creating an environment where providers can have reasonable assurance for responding to external queries, consistent with their professional ethical and legal obligations.
- Those April recommendations also included some additional recommendations for non-targeted queries, including providing individuals with meaningful choice re: listing with an aggregator.
- In May, we followed up those recommendations with a preliminary conclusion that the overall query recommendations were sufficient to address non-targeted queries as well.

Background

- The HITPC responded stating 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.
- Recommendations today re-affirm previous conclusions.

Existing Obligations for Query/Response

- Data Holder (Response)
  - 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 (Query)
  - 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

Previous Recommendations (Summary)

- Data holders may be reasonably assured of a requester’s identity through, for example, the use of DIRECT certificates, membership in a trusted network or a pre-existing relationship (examples are not exhaustive – see full recommendation at slide 32).

- The data holder may be reasonably assured of a requester’s treatment relationship with a patient if, for example, there is prior knowledge of the relationship, the relationship can be confirmed within a network or if the requester provides some communication of consent (examples are not exhaustive – see full recommendation at slide 33).

Previous Recommendations (cont.)

- Data holder may make a 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).
- 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.

(See Slides 34-35 for recommendations)

Previous Recommendations (cont.)

- A requester's query should, ideally, present no more (but also no less) PHI that what is necessary to match to a record. Available demographics should be used prior to more specific information. Previous recommendations on matching should be implemented** (see slides 36-38 for full recommendation)
- 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.) (see slide 39 for full recommendation)

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

Previous Recommendations (cont.)

- Data holders should log both the query from an outside organization and the response, regardless of its content. Requesters should also log the query. The information should be available to patients upon request. (see slide 40 for full recommendation)
- With respective to sensitive data: 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. (see slides 42-45 for full recommendation)

Previous Recommendations (cont.)

- Patients should have meaningful choice re: whether or not they are included in an aggregator that permits queries from external providers. (See slide 46 for full recommendation)

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

Key Themes (1 of 4)

- 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.

Key Themes (2 of 4)

- For sensitive data, most depend on the data partner to withhold data requiring additional consent, or other types of sensitive data. One network made 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).

Key Themes (3 of 4)

- 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.

Key Themes (4 of 4)

- Most have some either inherent or express geographic limits. There is the possibility to do nationwide health information exchange, but right now, only exists for limited data sets.
- 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.

Recommendations

- The previous recommendations, initially considered in the context of targeted query, also apply to non-targeted query.
- We considered whether additional policies were needed for non-targeted queries.
- We held a virtual hearing on June 24, 2013, where we received testimony from 8 operational models of non-targeted query and the policies governing those queries.

Recommendations

- In hearing the testimony, the Tiger Team recognized the great care and effort the HIEs took in crafting policies and operations that worked for their particular communities. And again, we thank the panelists for their testimony.
- Based on the results of the hearing, we reaffirm our previous statement that existing recommendations on meaningful choice and targeted query are sufficient in addressing non-targeted queries, and that no additional policy is needed at this time
- As always, we reserve the option to revisit these recommendations in the future as conditions change.

Additional Thoughts

- Virtual 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.
- Concern that record holders may withhold data for business reasons. Ultimately, the data should go where the patient goes.
- Other issues may include payer access, public health and governance.

PSTT04 Summary: MU Attestation for Security

- **What, if any, security risk issues (or Health Insurance Portability and Accountability Act (HIPAA) Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3?**
- The Tiger Team formed a subgroup to deliberate on this question; recommendations were vetted by the Tiger Team membership.
- Instead of selecting additional HIPAA Security Rule provisions for emphasis in Stage 3, we instead want to improve accountability for complying with the existing meaningful use security measures – in particular, the requirement to perform a security risk analysis and correct identified deficiencies.

Recommendations (1 of 3)

- For MU Stage 3, CMS should emphasize that when an entity attests to having conducted or reviewed a security risk analysis with respect to its certified EHR technology, the entity is attesting to compliance with the HIPAA Security Rule with respect to such analysis.
- To achieve compliance with this objective, entities must:
  - Conduct a security risk analysis or review an existing risk analysis and
  - Document the results of the risk analysis or review, including the actions taken (or the schedule for actions planned to be taken) to correct any deficiencies identified during the analysis or review.

Recommendations (2 of 3)

- Add an accountability measure, requiring entities to identify the individual(s) who is/are responsible for conducting and documenting the risk assessment.
- Link attestation to specific MU objectives, rather than present as a single, stand-alone measure. Specifically:
  - Require attestation that a risk analysis has been performed on any new functionality provided as a result of deploying the 2014 or subsequent MU criteria (those for 2014 focus on exchange and interoperability between organizations, and consumer engagement). Such an attestation would indicate that the entity had complied with the HIPAA Security Rule by performing the required analysis and documenting the results, including correction of identified deficiencies.

Recommendations (3 of 3)

- CMS should provide additional education, such as FAQs, to the meaningful user community on the expectations and importance of conducting <u>and</u> documenting security risk analyses, and correcting deficiencies. For example:
  - Expand FAQs to discuss the availability/use/benefits of third-party assessment tools and services, and of risk analysis checklists, particularly those developed by the regulators.
  - Expand FAQs to clarify that a component of the risk analysis process includes the requirement to correct any deficiencies that impact compliance with the HIPAA Security Rule
  - Highlight also (for larger entities with the requisite resources) the option/value of having internal auditors leverage OCR’s audit program protocol to conduct substantive pre-audits.

Query/Response

BACK-UP

Questions

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

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?

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 is on policy, and not security methodologies or identity management issues.

Purpose of Virtual Hearing

- 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.
- We are 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. We are also interested in hearing of instances where limiting policies were considered but not adopted.
- The Tiger Team also wants to learn about the thought processes behind the development of any such policies.

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 (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:
  1. Some or all of the requested content
  2. 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.

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

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