HIT Policy Committee: Privacy and Security Tiger Team

Non Targeted Query Hearing: Healtheway Testimony

6/24/13

Introduction

My name is Mariann Yeager and I am the Executive Director of Healtheway, the non-profit, public-private collaborative chartered to support the eHealth Exchange. I am pleased to have the opportunity to offer this testimony to the HIT Policy Committee's Privacy and Security Tiger Team on issues related to non-targeted query for documents. The Tiger Team has asked Healtheway to provide testimony regarding the eHealth Exchange experiences to date in supporting large-scale deployment of query-based exchange, as well as the important work that still lies ahead. Since Healtheway has previously provided testimony to the HIT Policy Committee and HIT Standards Committee regarding the eHealth Exchange in January 2013, my testimony today will provide a brief overview regarding use of query-based exchange by eHealth Exchange participants. The remainder of my testimony will be organized around the specific questions posed by the Tiger Team.

Uses of eHealth Exchange

The eHealth Exchange (eHEX) is a policy, security and technology platform to support a range of health transactions including, query/retrieve, document submission (push) and publish/subscribe services. The platform enables Participants to use the eHEX for a variety of use cases including continuity of care and transitions of care. Secure and trusted exchange requires a significant shared effort. For that reason, the eHEX believes that it can be better provided with cohesive and integrated approach for sharing data across the eHEX community, than independent implementations of individual transactions. The eHEX facilitates sharing of data among private sector Participants, as well as, between private sector Participants and Federal agency Participants. A few examples highlight the current level of activity and the value being derived.

eHEX is being used by the Social Security Administration (SSA) to obtain medical evidence for disability determinations from over eighteen (18) private-sector Participants. In 2012, SSA made requests with a patient's authorization using the eHEX with 18 participants in 16 states (CA, HI, ID, IN, MA, MI, MN, NC, NM, OH, OR, PA, TX, VA, WA, WI). As of the end of 2012, SSA has made approximately 64,000 requests for medical records and received just over 45,000 CCDs electronically via the eHEX. SSA is also seeing rapid increase in utilization as connectivity grows and matures, with an increase of more than 250% in the number of medical records received electronically compared to 2011. While the volume of records received via the eHEX is still ramping up, it has already shown good potential to enhance the speed and effectiveness of SSA's disability decision-making process. For example, when records are obtained electronically:

- Initial case processing times are approximately 20-22 days quicker.
- Medical decisions for three percent of cases are decided within just 48 hours.

- Social Security is able to gather medical records more quickly and apply decision support logic to the disability determination process. This has the potential to increase efficiencies in the disability program to help offset increasing workloads and staffing constraints, while dramatically improving service to the public.
- This enhanced disability determination process has also shown positive financial impact for providers, with a documented impact of over $2M for just one health system in Richmond, VA.

The EHEX is also being used by VA and DoD to support its Virtual Lifetime Electronic Record (VLER) initiative. This important initiative includes:

- 13 VA Medical Centers and 14 eHEX partners
- 60,262 Veterans opted in for sharing their Veteran's health record
- VA has retrieved 4,583 Veteran health records from eHEX partners
- eHEX partners have retrieved 11,788 Veteran health records from the VA

In various conferences over the past few years, we have heard moving testimony from the families of our wounded warriors about the enormous burden upon their loved ones when the capability for electronic exchange of health records does not exist. As others, such as Tim Cromwell, can so powerfully communicate, we can and should do better for those who have sacrificed for our country. VLER and eHEX is a big step in the right direction.

The Centers of Medicare and Medicaid Services (CMS) is also using the eHEX in support of its End Stage Renal Disease, and we look forward to their expanded participation in the future.

The eHEX's objective over the next two years is to grow the community of eHEX participants, increase the quantity and quality of data available and accessible, increase utilization of the connectivity and gradually expand the use cases supported by the eHEX. We also will continue to refine, mature, and build capabilities to support broader connectivity and nationwide data exchange.

Responses to Tiger Team Questions

Following are responses to the questions posed by the Privacy and Security Tiger Team.

1. How have you operationalized non-targeted queries? Please describe the process.

Targeted and non-targeted queries are operationalized using a common technical and trust framework:

- Participants who wish to support query-based exchange are required to comply with a set of technical and testing requirements.
    - These requirements include standards-based implementation-level specifications regarding security, transport, discovery of patient records, as well as query and retrieval of documents.

        - Participants are required to test to verify that their standardized, technical interfaces satisfy these requirements.

- Non-targeted queries are also operationalized as part of the overarching eHealth Exchange (eHEX) trust framework, which includes a trust agreement and operating policies that further specify Participant obligations in the conduct of exchange.
    - Participants who query data for treatment purposes also have a duty to respond to authorized requests for data for treatment purposes, either with a copy of the data or with a standardized response that data are not available. Participants may respond to requests for other purposes.
    - Participants who submit data are responsible for submitting the data in compliance with applicable law. Participants further represent that the message is:
        - for a Permitted Purpose;
        - sent by the Participant who has requisite authority to do so;
        - supported by appropriate legal authority, such as consent or authorization, if required by Applicable Law; and
        - sent to the intended recipient.

2. How long have you been operational with your approach and how many patients are involved?

The eHEX has been operational since February 2009. There are currently 40 participants in production, including 4 federal agencies, 6 states, 8 beacon communities and approximately 2 dozen private HIEs.

eHEX participants connect hundreds of hospitals, tens of thousands of physician practices and hundreds of millions of patients in all 50 states. The eHEX is experiencing rapid growth and uptake, with an additional 100 organizations (including 29 states) in various stages of planning or proceeding with onboarding to the eHEX.

3. Is there an inherent scope limitation associated with your entity that affects providers' ability to perform non-targeted queries (e.g. geography)?

The eHealth Exchange has been deployed, to date, in geographic clusters around the US that are largely bound by region. As a result, the participants who query data have, by default, limited their queries based upon geography / service area.

As the eHealth Exchange grows, additional parameters will be needed to narrow the scope of the queries.

The eHealth Exchange architecture and policy framework were never intended to promote unbound "broadcast queries". Now that participation in the eHEX is reaching critical mass, we are developing additional guidance to help providers find the most likely sources of documents regarding their patients. To that end, we also welcome work define policies and guidance to help focus provider behaviors in narrowing queries to the relevant circumstances and the most likely places where a patient's records are expected to be found.

4. What additional limits are placed on non-targeted queries (e.g., who can query, for what purpose and scope of query)?

The eHEX has robust functionality to support policies related to who can query, including the purpose and scope of the query. Participants include policy statements / assertions to accompany the message (i.e. the query). These statements provide important information and enable a responder to determine whether / how to respond to a request. These policy assertions are sent using an international OASIS standard, called Standard Access Markup Language (SAML).

SAML provides the receiver with policy information about the user making the query and the policy or policies that they are asserting in the request.

Attributes used in the SAML assertion include information about the user, authentication information about the user, organizational information, the user's role, and the purpose of use. The patient identifier from the requesting organization is optional, as it may not be needed in cases where the request is not specific to a patient (e.g. population health query).

An Access Consent Policy or Policies may be included asserting the policy that requestor has regarding the disclosure of the patient's information. Lastly, the SAML assertion is signed to support the integrity, authentication and non-repudiation of the assertion.

It was very important for eHealth Exchange Participants to be able to apply their organizational policies and have an automated way to determine whether/how to respond to requests based upon the assertions / rules supplied with the Message. Without these automated policy statements, providers would be forced to manually verify the policy requirements prior to responding to queries for data (whether targeted or untargeted). This was one of the core reasons that both SOAP transport and SAML were selected as core standards for the eEHX.

Participants are required to also provide accurate and true assertions as a condition of the trust agreement. The eHEX accountability measures in place if a participant provides inaccurate or untrue assertions when sending a query, which are implemented contractually and via an oversight committee.

The standards and policies employed in the eHealth Exchange were designed to enable the requestor to narrow the scope of the query (e.g. based upon dates of service, etc.) to reflect the type of information needed and to declare these to the responding organization.

Only participants and users who have the requisite authority under Applicable Law to request the data may do so.

All submissions of data among eHEX participants are restricted to a narrowly defined set of Permitted Purposes, which are defined as follows:

> ***Permitted Purpose*** *shall mean one of the following reasons for which Participants or Participant Users may legitimately Transact Message Content:*
>
> *1. Treatment of the individual who is the subject of the Message;*
>
> *2. Payment activities of the Health Care Provider for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Health Care Provider to a Health Plan.*
>
> *3. Health Care Operations of either*
>
> *.01. the Submitter if the Submitter is a Covered Entity;*
>
> *.02. a Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or*
>
> *.03. the Recipient if (i) the Recipient is a Health Care Provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such Health Care Provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such Health Care Provider;*
>
> *4. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e);*
>
> *5. Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-4 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102; and*
>
> *6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.*

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?

Participants and their users are obligated to comply with Applicable laws, including but not limited to HIPAA. Participants determine, at a local level, whether/how to address an individual's right to restrict access and whether to obtain an individual's consent and authorization. Healtheway observes that, while not universal, some level of individual choice is generally supported by eHEX participants as a matter of good practice.

An individual's rights for choice, as well as the right to restrict access / queries, are addressed by the laws and regulations that apply to Participants, including HIPAA Privacy and Security Rules. How these are implemented are addressed at a local level and are not dictated by the eHealth Exchange rules of the road at a national level.

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?

Healtheway does not function as an aggregator. As a result, this question does not pertain to the eHEX.

7. How do you address exchange of sensitive information in a non-targeted query model?

All information transacted among eHEX participants, Message Content, is subject to equal protections under the DURSA. Each participant is obligated to comply with Applicable Law, including laws that establish additional protections related for sensitive information.

In some instances, "sensitive information" may be comingled with other data in an EHR. In this scenario, eHEX participants, as a matter of standard practice, obtain an individual's express consent or authorization prior to the release any information to other eHEX participants.

8. What information is returned to a requester as a result of a non-targeted query?

The response may either be:

- a standardized, generic response (e.g. "Data Not Found"); or
- if information is available and if the responding organization's policy and applicable law permit the release, a copy the requested document.

The eHEX standards allow for policy information to be submitted along with the requests for records (i.e. in the SAML assertions) so that responding organizations can make an informed decision regarding whether and how to respond.

9. If you exchange sensitive information, is there a difference in what is returned when such information is involved?

This question deserves greater clarification. Most health information is sensitive and we have already described differing messages that can be provided. As a "network of networks", the eHEX is supporting a variety of practices across all 50 states, and in accordance with appropriate polices and transactions of independent health information exchange and systems.

10. In what environment and for what providers have non-targeted queries proven to be the most effective? Please provide appropriate metrics if available.

We have seen great success in using non-targeted queries universally across various environments and use cases. For example:

- Request for records to support the Social Security Administration (SSA) disability benefits program – where the beneficiary indicates where they have received care, enabling a more narrowed query, based upon geography.

- Request for records for treatment purposes, care coordination and referrals across care settings by health systems or regional or state HIOs.
    - Providers typically know the most likely places where their patients may have been treated in the treatment service area, based upon where they typically refer for care. As a result, they will naturally limit the scope of their queries to a limited set of providers based upon their knowledge of the most likely places where their patients may have been treated.
    - Health systems / HIOs are joining the eHealth Exchange with an express intent to share data with others in the trading area or in adjacent communities.
    - We typically do not see these organizations sending broadcast queries throughout the network.

Health systems that have a presence across a large number of states train their users on how best to use the eHEX connectivity, including the parameters for querying for records. Healtheway does not have specific examples to share at this time, but could envision learning from the multi-state providers who are already addressing these guidelines as they roll out eHEX connectivity to their entire system.

We believe the Tiger Team may be informed from studying how frequently providers are unaware of where their patients' data reside. In our experience, the provider community already understands where their patients are most likely to receive care.

11. What challenges/problems have been created by your approach? What adjustments have you or do you plan to make to your approach?

Healtheway does not believe that challenges / problems were created by using a query-based approach per se. Participants, to date, have largely limited their queries based upon service area and the specific circumstances / use case at hand.

We do, however, believe additional guidance and shared services may be needed to offer enhanced functionality to support more automated and promote narrowly-scoped queries as connectivity grows. We will look to national-level guidance, as available, to inform constitute nodes and look forward to recommendations developed by the Tiger Team.

12. Would having widely applicable policy (or guidance) on providers' ability to perform non-targeted queries be helpful? If so, what should those policies be?

We recognize the good work the Tiger team has accomplished to this point. We believe that developing policies and guidance for non-targeted queries can be challenging if done in abstract concepts, can often focus on the "worst common denominator". We encourage the Tiger team to continue to advance discussions in this and other areas, but also encourage as much specificity as can be achieved. We also believe that this is an area that warrants more in-depth involvement of the implementation community, since they have already developed and implemented policies and approaches in this area.

The richness of the eHealth Exchange policy and standards framework allows for greater segmenting of query purpose and process. We hope that these discussions more fully develop the differences in query circumstances and the specific issues that are being addressed before policies are advanced.