IE WG Meaningful Use Stage 3 Recommendations

August 7, 2013

Information Exchange Workgroup

Micky Tripathi

Agenda

- Provider directory recommendation
- Data portability

Provider Directory

Background

- **At July HITPC, the provider directory recommendation was approved but the HITPC asked the Workgroup to revisit its principle on authentication**

- **In follow up WG conversation including S&I Framework staff, the Workgroup reaffirmed its recommendation to include the capability for authentication and further amended the recommendation to also require authentication of the provider directory-holding entity (ie, not just the requesting entity)**
  - Aligns with S&I approach which already included authentication of data source
  - Important to include this protection to guard against spoofing of provider directories

- **The recommendation is solely about the *capabilities* that certified EHR technology should have. The recommendation is not a policy requirement that authentication should be utilized.**

- **Including the capability in certification gives maximum flexibility implementers and policy makers.**
  - The provider directory market and use cases are still evolving
  - We are seeing provider directory implementations utilize authentication in the market today, so making the ability to conduct mutual authentication assures that these capabilities will be available for those who choose to use them

Recommendation on Provider Directories

[Note: No changes from July HITPC version]

- HITPC recommends that:
  - Search for provider: EHR systems have the ability to query external provider directories to discover and consume addressing and security credential information to support directed and query exchange
  - Respond to search: EHR systems have the ability to expose a provider directory containing EPs and EH addressing and security credential information to queries from external systems to support directed and query exchange

Principles for Provider Directories

[Note: No changes from July HITPC version]

HITPC recommends that the following guidelines be used for establishing standards for provider directories:

1. Scope: Standards must address PD transactions (query and response) as well as minimum acceptable PD content to enable directed and query exchange

2. Continuity: Build on Stage 1 and 2 approaches and infrastructure for directed exchange where possible and allow use of organized HIE or cross-entity PD infrastructures where applicable and available (ie, remain agnostic to architecture and implementation approaches)

3. Simplification: Set goal of having PD query and response happen in a single (or minimal) set of transactions

4. External EHR system: An EHR system of another distinct legal entity, regardless of vendor

Principles for Provider Directories (continued)

[Note: Changes from July HITPC version in <- red ->]

5. Transactions:

   A. Querying systems must have ability to:

      1. Present authenticating credentials of requesting entity
      2. -> Validate authenticating credentials of provider directory holding entity <-
      3. Present provider-identifying information
      4. Securely transmit query message

   B. Provider directory must have ability to:

      1. Validate authenticating credentials of requesting entity
      2. -> Present authenticating credentials to requesting entity <-
      3. Match provider
      4. Respond with unambiguous information necessary for message addressing and encryption or acknowledgement of non-fulfillment of request

   C. Provider directories must have administrative capabilities to:

      1. Submit updated provider directory information (additions, changes, deletions) to external provider directories
      2. Receive and process provider directory updates from external provider directories

6. Transaction details:

   a. Provider directories should contain minimum amount of information necessary on EPs and EHs to address and encrypt directed exchange and/or query for a patient record messages

   b. Provider directories should contain minimum amount of information necessary on EPs and EHs to disambiguate multiple matches (i.e. same provider at different entities, providers with the same name, etc)

Data Portability

Background

- **There are two key use cases for data portability**
  - Provider-centric: Provider switching from one EHR vendor system to another
  - Patient-centric: Patient requesting migration of records (e.g. to a new PCP)

- **We expect to see rising demand for data portability across vendor systems**
  - This will happen purely as a function of a growing installed base
  - In addition, market surveys suggest that 20-30% of providers could switch vendors in the next 2 years, suggesting that there is some urgency to the issue

- **Currently the difficulty of data migration is a barrier to exit for providers who are switching vendors, and a barrier to continuity of care for patients who are switching providers**
  - Ad hoc process that is highly variable and fraught with potential for errors and lack of continuity in medical record completeness
  - Difficult to include in EHR contracts in a way that is operationally executable when needed
  - Can be difficult or impossible to execute if vendor is not cooperative, system has been highly customized, or if mismatch exists between source and receiving system capabilities

Background (continued)

- **Data or information can be lost, rendered operationally inaccessible, stripped of context/meaning, or misplaced leading to erroneous context/meaning**
  - Safety – records attached to wrong patient, data placed in wrong fields, etc
  - CQMs and CDS – loss of data important to measurement and decision support, such as look-back periods, exclusions, etc can cause disruption in performance improvement efforts
  - Administrative – loss of data important to revenue cycle can cause disruption in revenues

- **A standard for data portability would set a common baseline for medical record continuity that will be vital as the EHR user base grows and matures, and the industry comes to increasingly rely on electronic medical records and MU-related EHR functions.**
  - A challenge will be that it is difficult to completely specify data migration requirements because needs may vary locally for a variety of reasons including record retention laws, provider/patient preferences, and provider documentation patterns
  - However, setting a floor will inspire greater market dynamism by lowering barriers to exit for providers and patients, and promote safety and continuity of care by reducing opportunities for errors

Recommendation

HITPC recommends:

- Data Portability: EHR systems have the ability to electronically export and import medical record and administrative information across EHR vendor systems to enable migration of patients’ records without significant or material loss of clinical or administrative data

Principles for Data Portability

HITPC recommends that the following principles be used for establishing requirements and standards for data portability across EHR vendor systems:

1. Consistency: Build on CCDA approach in alignment with general HITECH direction. Perhaps consider CCDA templates specific to "Cross-System Data Portability"?
2. Content: Should encompass all clinically and administratively-relevant information that can be reasonably transferred across systems without loss of essential patient, clinical, and administrative context or meaning
    - Clinical data should:
        - Include at least MU Stage 2 data requirements: Common MU Data Set, encounter diagnoses, immunizations, cognitive status
            - Ambulatory only: reason for referral and referring or transitions providers name and office contact information
            - Inpatient setting only. Discharge Instructions
        - Retain structuring of discrete data (e.g., discrete lab results)
        - Include and retain structure/context of notes (e.g., textual notes in specific sections of EHR)
        - Allow transfer of attached documents and retain attachment to patient (e.g., scanned documents such as Advance Directives)
    - Administrative data should:
        - Retain claims transactions for reasonable time period covering transition
        - Retain scheduling and appointment information for reasonable time period covering transition
        - Retain audit log meta-data or reports for medical-legal purposes

Principles for Data Portability (continued)

3. Add flexibility
   1. Time horizon: Should allow user-configurable setting of time period to cover legal medical record retention requirements as well as to support look-back periods for decision support, CQMs, and care management (e.g., last 10 years only)
   2. By Encounter: Should allow user-configurable setting to create CCDAs based on a particular encounter and/or types of encounter (e.g., face-to-face visits but not telephone encounters)
   3. By Patient: Should allow export and import of a single patient in order to facilitate patients bringing “their entire record” with them (e.g. to a new PCP)