Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

January 14, 2011

David Blumenthal, MD, MPP
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Blumenthal:

The HIT Policy Committee (Committee) gave the following broad charge to the Information Exchange Workgroup (Workgroup):

Broad Charge for the Information Exchange Workgroup:

- The Workgroup is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee on policies, guidance governance, sustainability, and architectural, and implementation approaches to enable the exchange of health information and increase capacity for health information exchange over time.

Since September 2010, the Workgroup conducted a number of public meetings on Entity-level Provider Directories (ELPDs) in support of Meaningful Use Stage 1 transactions, and, in particular, characteristics of ELPDs to support more rapid adoption of health information exchange (HIE) functions. On November 19, 2010, the Workgroup reported and discussed its findings with the Committee, which were subsequently approved.

This letter provides recommendations to the Department of Health and Human Services (HHS) on Entity-level Provider Directories.

Background and Discussion

The American Recovery and Reinvestment Act of 2009 (ARRA) established the HIT Policy Committee as a Federal Advisory Committee. The Committee is charged with recommending to the National Coordinator a policy framework for the development and adoption of a nationwide health information technology infrastructure that permits the electronic exchange and use of health information. Provider directories can facilitate the rapid adoption and exchange of electronic health information. Stage 1 of Meaningful Use includes requirements to exchange identifiable clinical information among providers for treatment purposes, and these exchange requirements are expected to increase with the advent of Stage 2 and 3. Therefore, the Information Exchange Workgroup focused on recommendations on the characteristics of ELPDs to support more rapid adoption of HIE functions, per the recommendations outlined below. In addition, the Information Exchange Workgroup made recommendations on policy levers to establish an ELPD.

RECOMMENDATIONS

I. Recommendations on the Characteristics of ELPDs

Recommendation 1: The following entities should be listed in the ELPD

- Health care provider organizations (i.e., hospitals, clinics, nursing homes, pharmacies, labs, etc)
- Other health care organizations (i.e., health plans, public health agencies)
- Health Information Organizations (i.e., regional HIE operators, health information service providers)
- Other organizations involved in the exchange of health information (business associates, clearinghouses)

See Appendix 1 – Terminology for definition of key terms

Recommendation 2: ELPDs should support the following functionality

- Support directed exchanges (send/receive as well as query/retrieve)
- Provide basic "discoverability" of entity
- Provide basic "discoverability" information exchange capabilities (i.e., CCD, HL7 2.XX)
- Provide basic "discoverability" of entity's security credentials

Use Cases and Value of ELPDs:

- *See Appendix 2 - Matrix of use cases and support/value ELPDs provide*

Recommendation 3: ELPD content should be limited to the following categories of information

- Entity 'demographics' and identification information
  - Name, address(es)
  - Other familiar names
  - Human level contact
- Information Exchange Services
  - Relevant domains (as defined by each entity); relevant website locations
  - Protocols and standards supported for Information Exchange (SMTP, REST, CCD/CDA, CCR, HL7 2.x.x, etc)
  - Two Options:
    - Include a 'pointer' in the directory to the entity's information *(recommended)*
    - Include the entity-level information in the directory
  - General Inbox location, if applicable (for message pick-up/drop-off)
- Security
  - Basic information about security credentials (i.e., type, location for authentication)

Recommendation 4: Business model and operating approach

- Internet-like model (nationally coordinated, federated approach)
  - Certified registrars: registrars are 'registered' and certified to receive/process/accept entities in the ELPDs
  - National guidelines: Registrars follow national guidelines for who to accept, validation of application, addressing
  - Registrar reciprocity and Publication to National Registry System:
    - Entities registered by one registrar are 'recognized' across system (no need to register again at different registrars)
    - Each registrar publishes directory information into a national provider directory registry system that, like DNS, will support identification of entities across registrar domains
  - ELPDs: maintained by registrars; cross-referenced through system (similar to DNS)
  - Possible roles of federal government:
    - National standardization and harmonization
    - Some agencies could be registrars themselves (i.e., Medicare, VA)
    - Build on existing national/federal tools (i.e., PECOS, NPPES, NLR, others)
- Benefits:
  - National scalability; interoperability across regions/HIEs; relatively simpler to implement
- Issues:
  - Data management; conformance across industry

II. Recommendations on Policy Levers to Establish an ELPD

Recommendation 1

- The HITSC should be directed to identify technology, vocabulary, and content standards that will create an ELPD with multiple registrars and a single, nationwide, registry
  - The single, nationwide registry must be accessible by EHR systems
  - Acquisition of a security credential (certificate) and discoverability of this credential using the ELPD must be included in the technical approach
  - The technical approach must also include a process for certification of ELPD functionality in EHRs and accreditation of registrars
  - Recognizing that some policy questions may still be unanswered, the HITSC should consult the HITPC as necessary during standards development to assure alignment of standards with policy
  -

Recommendation 2

- The federal government should use the strongest available levers to require registration in, and encourage use of, the nationwide ELPD

- ELPD registration and use should be incorporated in MU Stage 2/3 and in NHIN participation requirements
- The MU Working Group should work jointly with the IE WG to determine the best approach for incorporating ELPD registration and use in MU Stage 2/3
- ELPD governance and participation should be included as part of NHIN "Conditions of Trust and Interoperability" and used as a lever to establish NHIN Governance
    - Require ELPD registration for participation in NHIN Exchange and Direct
    - Create an accreditation process for registrars within the context of other similar processes (e.g., certificate issuance)

Recommendation 3

- State-level HIE and Beacon programs should be required to incorporate the national registry in addressing their provider directory needs
    - ONC should require conformance with ELPD standards and technical guidelines
    - ONC should encourage state-level HIE program grantees to become accredited registrars and to promote the establishment of accredited registrars in their states and regions

We appreciate the opportunity to provide these recommendations on Entity-level Provider Directories, and look forward to discussing next steps.

Sincerely yours,

/Paul Tang/

Paul Tang
Vice Chair, HIT Policy Committee

Appendix 1
Terminology

ELPD Recommendation: Basic Common Terminology

Provider Directory:

- An electronic searchable resource that lists all information exchange participants, their names, addresses and other characteristics and that is used to support secure and reliable exchanges of health information.
- Entity-Level Provider Directory (ELPD): A directory listing provider organizations
- Individual-Level Provider Directory (ILPD): a directory listing individual providers

Entity:

- Any organization involved in the exchange of patient health information, including submitters, receivers, requesters and providers of such information.
- Organizational entities: The legal organization involved in the exchange
- Technical entities: The systems/services that can interact with people through displays, etc., send and receive messages in standardized ways, etc.

Individual Provider/Clinician:

- Individual health care provider (per HIPAA/HITECH definition)

Sender:

- Authorized final end-point organizational entities or their employees or proxy technical entities that generate and send directed exchanges.

Receiver:

- Authorized organizational entities or their employees or proxy technical entities that receive directed exchanges.

Routing:

- Process of moving a packet of data from source to destination. Routing enables a message to pass from one computer system to another. It involves the use of a routing table to determine the appropriate path and destination

Query/Retrieval:

- The process of requesting and obtaining access to health information. It also refers to the process of request and obtaining provider directory information

Security Credentials:

- A physical/tangible object, a piece of knowledge, or a facet of an entity’s or person's physical being, that enables the entity/person access to a given physical facility or computer-based information system. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items.

Discoverability

- The ability of an individual/entity to access and obtain specific information about another entity, including demographic information, information exchange information and security credentials information.

Administrative-related functions

- Register/edit/delete: Processes executed by authorized individuals or entities to add or modify entries (entities and individuals) in a provider directory based on national and local policies. They may involve attestation, verification and/or validation of the information provided about the entities and individuals.
- Access control: Prevention of unauthorized use of information assets (ISO 7498-2). It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises (OASIS XACML)
- Audit: Review and examination of records (including logs), and/or activities to ensure compliance with established policies and operational procedures. This review can be manual or automated

Sources: IHE Provider Directory Profile; HITSP Glossary; NIST Technical Documents

Appendix 2
ELPD Use Cases

Scenarios	Value of Entity-Level Directory

Scenario: Clinician Orders Test from Lab & Lab Sends Results
• Clinician from Clinic X sends Lab Order to Laboratory
• Clinic X's EHR generates lab order message and sends it to Laboratory
• Laboratory Information System (LIS) received lab order
• After lab sample is processed and results are entered, LIS generates a lab results message and sends back to ordering clinician
	• Generally, exchanges with laboratories might be well-known to the clinic and pre-established
	• Clinic X will use the entity-level directory to obtain the organization-level 'address' of the laboratory, and other information exchange features supported by the lab (port information, formats supported, security credential locations) which allows Clinic X to establish a connection, open a defined port, and drop a message to the lab
	• The entity level directory provides two benefits:
	  • Establishing a first-time connection with the lab and have the path be defined
	  • Afterwards, to ensure that changes to the address of the lab from changes the lab might experience (moved, purchased, etc) will be resolved
	• Lab sends back results to Clinic X to the declared 'address' included in the electronic lab order
	• Lab may also use entity-level directory to support 'copy-to' function to send results to a non-ordering provider
	• Using the directory, the digital credentials of both the sending and receiving computers are used to validate identities.
	• Prior to sending the transaction, the sending computer checks the I.E. services that the receiving computer uses and determines whether the transaction can be sent.

Scenario: Patient Summary from PCP to Specialist • PCP from Clinic X is sending a Patient Summary to Specialist in Clinic Y • Clinic X's EHR sends patient summary (i.e. CCD) to Clinic Y's EHR • Clinic Y EHR system receives the patient summary and incorporates data into the patient's record in the EHR • Clinic Y EHR sends an alert to specialist that new information about Patient is available	• Clinic X will use the entity-level directory to identify the organization-level 'address' of Clinic Y and other information exchange features supported by Clinic Y (port information, formats supported, security credential locations) • In the message header or inside the message is where the information about the patient, the provider (specialist) resides, which will be used by the EHR of the recipient to incorporate data, issue alerts to providers about new data available • Using the directory, the digital credentials of both the sending and receiving computers are used to validate identities. • Prior to sending the transaction, the sending computer checks the I.E. services that the receiving computer uses and determines whether the transaction can be sent.

Scenarios	Value of Entity-Level Directory
Scenario: Hospital Discharge Summary (or ED Visit Summary or Surgical Report Summary) • Hospital discharge summary (i.e. CDA) of a patient is sent from hospital information system (EHR) to the clinic EHR where patient's primary care provider practices and the patient's record resides • Clinic's EHR system receives the discharge summary and incorporates data into the patient's record in the EHR • Clinic's EHR sends an alert to primary care provider that new information about Patient X is available	• Hospital will use the entity-level directory to identify the organization-level 'address' of the clinic the data is intended to, and other information exchange features supported by the clinic (port information, formats supported, security credential locations) • In the message header or inside the message is where the information about the patient, the provider (specialist) resides, which will be used by the EHR of the recipient to incorporate data, issue alerts to providers about new data available • Using the directory, the digital credentials of both the sending and receiving computers are used to validate identities. • Prior to sending the transaction, the sending computer checks the I.E. services that the receiving computer uses and determines whether the transaction can be sent.
Scenario: Hospital X Request for Information from Hospital Y • Patient outside of their home geography appears in hospital for emergency or acute care • Hospital X needs additional clinical information prior to treatment • Patient knows familiar name of home Hospital Y; Hospital X needs to look up complete address for Hospital Y • Hospital X sends request for patient information to Hospital Y • Hospital Y sends CCD summary to Hospital X	• Hospital X will use the entity-level directory to search for the organization-level 'address' of the Hospital Y to be able to send query for patient information • Hospital Y will use the entity-level directory to discover location of security credentials (as applicable) of Hospital X • Hospital Y will send CCD the know address of Hospital X, based on the query • In the message header or inside the message is where the information about the patient, the provider (specialist) resides, which will be used by the EHR of the recipient to incorporate data, issue alerts to providers about new data available • Using the directory, the digital credentials of both the sending and receiving computers are used to validate identities. • Prior to sending the transaction, the sending computer checks the I.E. services that the receiving computer uses and determines whether the transaction can be sent.
Scenario: Patient Request for Site of Referral • PCP wants to refer patient for specialist consult or diagnostic testing • PCP (or patient?) searches Directory for specialists or diagnostic test centers • Patient chooses from among available choices • PCP sends CCD referral summary or diagnostic test order	• The entity level directory is used to make sure that the CCD is sent to the correct organization. • The header or message content contains information about the patient identity and, also, the specialist, if appropriate. • *** It is not necessary for this directory to describe services that are provided, because that information should be available from other sources. The primary purpose of the entity-level directory is routing.

Scenarios	Value of Entity-Level Directory
Scenario: Public Health request for data from provider • Public health agency needs to obtain information about a patient from a provider (clinic, hospital), in support of public health functions • Public health seeks provider, sends query with request for information • Provider received query, process it and submits data to public health agency	• Public health agency uses entity-level provider directory to identify the 'address' of the clinic/hospital to send the query • Entity-level directory provides other information exchange features supported by the clinic/hospital (port information, formats supported, security credential locations) • Public health agency sends query to clinic/hospital • In the message header or inside the message is where the information about the patient resides, which will be used by the clinic/hospital to search/extract data needed
Scenario: HIO to HIO routing • A regional HIO X needs to send clinical information to regional HIO Y	• HIO X uses entity-level directory to search for the organization's 'address' of HIO Y