June 13, 2011

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. Mostashari:

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.

In January 2011, the Workgroup formed a Provider Directory Task Force (sub-Workgroup) which conducted a number of public meetings on Individual-level Provider Directories (ILPDs). The Provider Directory Task Force discussed how ILPDs can facilitate basic health exchange functions by enabling “discovery” of key individual characteristics and mapping individuals to entity addresses. ILPDs were described as sub-national in scope, in contrast to Entity-Level Provider Directories (ELPDs). The Task Force focused on linking ILPDs with ELPDs to establish a national registry system that is locally flexible but nationally conformant. On May 11, 2011, the Workgroup reported on and discussed its findings with the Committee, which subsequently approved the recommendations as outlined below.

This letter provides recommendations to the Department of Health and Human Services (HHS) on Individual-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 ILPDs linking to ELPDs to support more rapid adoption of HIE functions, per the recommendations outlined below. The recommendations focus both on policy guidance and best practices’ underpinning for a wide variety of ILPD models.

RECOMMENDATIONS

I. **Recommendations on the Content of ILPDs**

**Policy Guidance**

1a) *Individuals* who can be listed in an ILPD should include all individual health care providers who are licensed or otherwise authorized by federal or state rules to provide health care services or support the health of populations.

1b) *Attributes* of those individuals should include:

Demographics: Last and first name, provider type, specialty, name and address of practicing locations, practice telephone number, e-mail address and hospital affiliation.

Identifiers: NPI, DEA, State License #, etc.

Entity-affiliations (mapped to ELPD).

*See Appendix 1 in attached Slide Deck – Terminology for definition of key terms*

**Best Practices**

To serve intended purposes, information should be authoritative—representing all providers of types covered—and accurate.

Existing sources of content (state licensing boards, health plans, vendors, etc.) should be considered as content providers to ILPD operators. Ensuring data integrity will be key to success, it may be necessary to use multiple data sources to populate ILPD content. For instance licensure boards may be authoritative on licensure information but may not be similarly authoritative on practice locations.

Use Cases and Value of ELPDs:

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

II. **Recommendations on Functionality**

**Policy Guidance**

- 2a) “Discoverability” of an individual provider and their practice location(s) in order to support a broad array of HIE functions.

- 2b) Tight mapping to nationwide ELPD to allow seamless electronic addressing, synchronization of ILPD listing(s) with their affiliated ELPD
listing(s), and in general, interactive access to ELPD information about the entities associated with individual providers listed in the ILPD.

**Best Practices**

The service should support querying capability at multiple levels (practice location, provider name, specialty, etc.).

Establish defined policies and procedures and provide a structured and secure mechanism for individual providers to enroll and verify information used to populate the ILPD.

Establish policies and procedures to verify, as appropriate, the information provided by individuals enrolling in the ILPD.

Data elements included should at least meet the minimum data set recommended by ONC (per recommendations from the HIT Policy and Standards Committee); data elements should follow national standards definitions for content.

Ensure that the ILPD is able to interoperate with other ILPDs developed and operated in a manner that follows these recommended standards.

**III. Recommendations on Security, Access, Audit**

**Policy Guidance**

3a) Access to an ILPD's content should include clinicians and support and administrative staff. Well defined roles and rules-based access policies for users and operators of ILPD services should be put into place. These policies should be set at the local level and consider federal and state law, regulation and accepted practices.

3b) Sensitive content (state license and DEA numbers, etc.) needs to be restricted and user access to this information limited.

3c) Data integrity policies should ensure that that a) data contained in the ILPD is appropriately protected from unauthorized changes; b) individuals or their authorized delegates have ability to maintain their own data.

3d) Audit trail policies and procedures to track data provenance, access and use, and to support investigation of inappropriate use and breaches.

**Best Practices**

Provide a mechanism for individuals listed in the ILPD or their delegated authority (for instance staff or entity administrators supporting providers who practice in their institution) to correct/update listed information. An update and resolution process and change-control policies should be put into place by ILPD operators to manage a change request process.
Establish policies that require individuals listed in the ILPD to update periodically their information (at least three times per year) or as individual provider changes practice locations and affiliations.

Ensure that there is accountability and a shared responsibility in managing provider listings; delegating much of the responsibility of maintaining the currency of the listings to the providers (or their delegated entities).

**IV. Recommendations on Immediate Policy Levers**

**Policy Guidance**

4a) Technical interoperability standards (including messaging and content standards) for ILPDs should be recommended to the ONC by the HITSC consistent with the HIT Policy Committee recommendations on ILPDs and ELPDs and with ONC’s S&I Framework.

4b) The NwHIN governance rule should include any ELPD/ILPD standards adopted by ONC/CMS as appropriate.

4c) NLR and PECOS content should be made available by CMS for ILPD services funded through the State HIE Cooperative Agreement program.

4d) State HIE Cooperative Agreement funds to establish state-level ILPDs should be directed to adhere to ONC/CMS adopted ELPD/ILPD standards and policies.

4e) HHS should consider how State Medicaid agencies and others could be required to incorporate ILPD/ELPD use in their Medicaid Health IT Plans, MITA, and state EHR incentive programs.

**Best Practices**

Without sharing responsibility for maintaining the currency of the directory listings the cost for keeping the content current can become insupportable. Operators should consider models where providers or their delegated entities are accountable for the accuracy of their listings.

ILPDs have limited intrinsic value in themselves, ILPD operators need to consider what services are needed and valued in the market and how the ILPD supports that service and increases its value proposition.

Services outside of what may be required to fulfill meaningful use requirements that require an authoritative directory (credentialing, research, etc.) should be considered by ILPD operators.
The HIT Policy Committee appreciates the opportunity to provide these recommendations on Individual-level Provider Directories, and look forward to discussing next steps.

Sincerely yours,

/s/
Paul Tang
Vice Chair, HIT Policy Committee

Attachment: May 11, 2011, Information Exchange Slide Deck with Appendices
HIT Policy Committee

Information Exchange Workgroup
Final Recommendations on Individual-Level Provider Directory (ILPDs)

Micky Tripathi, Massachusetts eHealth Collaborative, Chair
David Lansky, Pacific Business Group on Health, Co-Chair

Provider Directory Task Force Members

Co-Chair: Jonah Frolich, Manet Health Solutions
Co-Chair: Walid Smaoui, Kaiser Permanente

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hunt Blye</td>
<td>Vermont Medicaid</td>
</tr>
<tr>
<td>Dennis Davis</td>
<td>DHHS</td>
</tr>
<tr>
<td>Paul Eigenman</td>
<td>DHHS</td>
</tr>
<tr>
<td>Judy Fackler</td>
<td>DHHS</td>
</tr>
<tr>
<td>Seth Finley</td>
<td>DHHS</td>
</tr>
<tr>
<td>Dave Gladis</td>
<td>Department of Health</td>
</tr>
<tr>
<td>James Goldin</td>
<td>HealthProperties</td>
</tr>
<tr>
<td>John Hampson</td>
<td>HealthBridge</td>
</tr>
<tr>
<td>David Hearn</td>
<td>CMSI</td>
</tr>
<tr>
<td>John Husted</td>
<td>Integration Health Management</td>
</tr>
<tr>
<td>George Gysinick</td>
<td>Massachusetts Medicaid</td>
</tr>
<tr>
<td>Lisa Khabie</td>
<td>Federation of State Medical Boards</td>
</tr>
<tr>
<td>Steven Shattuck</td>
<td>Intermountain HealthCare</td>
</tr>
</tbody>
</table>

Background: ELPDs

HITPC approved recommendations on Entity-Level Provider Directory (ELPDs) (approval letter attached)

A Nationwide ELPD Registry comprising multiple, federated ELPDs

Characteristics of ELPDs

National in scope, federated "internet-of-things" architecture

Information maintained at the entity-level

Used to facilitate discovery of key entity characteristics (HE capabilities, security credentials, gateway address, etc.) and delivery of messages "to the kernel" of the entity

Operated by certified registrars who perform registry management functions in accordance with national guidelines

Operationalizing ELPDs

HITPC to create standards for single national registry with multiple registries

Incorporate ELPD use into IHE Profiles 2.0 and NHN participation requirements

Require a consistent and standard IHE profile to integrate with individual-level ELPD
Background: Individual-Level Provider Directories

Whereas the ELPD was defined to be national in scope, ILPDs are sub-national.

Many ELPDs already exist, in both public and private entities.

Many will be built through state-level HIE and Beacon programs, as well as by health care and public health agencies.

Most local variation in uses, content, and structure.

Common characteristics of ELPD include:
- Maintaining individual, identifiable information, through the scope of the information available on an individual varies with the intended use.
- ILPDs facilitate secure health exchange activities by enabling "discovery" of key individual characteristics and linking individuals to entity addresses.
- ILPDs will be enabled to meet security needs for health exchange transactions, whereas others may be used for additional uses such as medical decision-making, health plan participation, etc.

Security credentials — either individual or entity-level, as per relevant policies.

The ELPD will need to support the level of security credentials required by the exchange participants.

Linking ILPD with ELPD will establish a national registry system that is securely federated but nationally-channelized.

Map individuals in ILPD with entities in ELPD to the extent possible.

Likely to be complex with many-to-many mappings and data gaps early on.

ILPD Use Cases and Link to ELPD

- Possible scenarios:
  - Clinical/Exchange - Patient and Physician
  - Hospital-to-Hospital - Patient and Physician
  - Public Health and Health Information - Patient and Physician
  - Lab-to-Hospital Exchange - Patient

- Common Workflow access scenarios:
  - Submitter needs to send a message to an individual provider.
  - Provider may view information on individual but does not have information on other entities.
  - ELPD is used to identify all possible locations.
  - Use information exchange to identify information location.
  - ELPD may be used to obtain security credentials/digital certificate/hardcopy location of secondary service vendors.
  - Submitter sends data to individual provider at the identified location.

- Privacy and Security Considerations:
  - All use cases must consider all federal and state privacy laws and rules.
  - Use case relies on extra layer of complexity that requires a strong focus on following selected privacy laws and rules.

- See Appendix J for description of use case scenarios.
Two Types of Recommendations in Four Domains

Two Types of Recommendations

Policy Guidance
Areas related to domain creation of national directory system.

Best Practices
- Governance should be comprehensive to establishing and operating an ELPD in the best interest of the public.
- Want to give helpful direction to local ELPD development scale and sharing advice for tailoring to most local needs.

Four Domains

1. Content
   - What content data should be included in ELPD? (individual, attributes)

2. Functionality
   - What data elements should be included in ELPD? (Eligibility, registration, content, data integrity, audit)

3. Security, access and audit
   - What attributes should be adopted by ELPD? (privacy, confidentiality, data integrity, audit)

4. Immediate policy issues
   - What policy issues should address? (ELPD, policy, data sharing, content, data integrity, audit)

Areas that our recommendations do not cover

Our recommendations provide a policy and best practices underpinning for a wide variety of models.

High-level view of Provider Directory Approach

Individual ELPDs:
- Local variation in specific sets of attributes desired for right ELPD mapping.
- ELPD mapping tool.

National ELPD Registry:
- Rapid performance for search and query.
- NPI/DSN, State/Local/County.

Entity Mappings:
- Entity ID mapping.

Domain 1: Content

Policy Guidance
1. Individuals who can be listed in an ELPD should include all eligible health care providers who are licensed or otherwise authorized by federal or state rules to provide health care services or access the health of populations.
2. Attributes of those individuals should include:
   - Demographics: Last and first name, provider type, specialty, name and address of the provider, telephone number, e-mail address and hospital affiliation.
   - Identifiers: NPI, DSN, State Licensure, etc.

Best Practices
To serve shared purposes, information should be authoritative—representing all providers of types covered—and accurate.

Existing sources of content (state licensing boards, health plans, vendors, etc.) should be considered as content providers to ELPD operators. Ensuring data integrity will be key to success. It may be necessary to use multiple data sources to populate ELPD content. For instance, licensing boards may be authoritative on licensure information but may not be similarly authoritative on practice locations.
Domain 2: Functionality

Policy Guidance

2a) "Compliance" of an individual provider and their practice location(s) in order to support a broad array of HIE functions.

2b) Identify gaps in standards (EPO) to allow seamless electronic addressing, synchronization of LPO logins with their affiliated EPO logins, and in general, interactive access to EPO information about the entities associated with individual providers listed in the EPO.

Best Practices

The service should support varying capability at multiple levels (practice location, provider name, specialty, etc.)

Establish defined policies and procedures and provide a structured and secure mechanism for individual providers to enroll and verify information used to populate the EPO.

Establish policies and procedures to verify, in an appropriate way, that information provided by individuals enrolled in the EPO.

Ensure that the EPO is able to coordinate with other LPOs developed and operated in a manner that follows these recommended standards.

Domain 3: Security, Access, Audit

Policy Guidance

3a) Access to an EPO's content should be limited only to support and administrative staff. Policies should be based on role-based access control for data. Such policies should be consistent with the organization's formal policies and procedures.

3b) Security and access policies should be in place to prevent unauthorized access to the EPO. These policies should be consistent with the organization's formal policies and procedures.

3c) The system's access and data must be limited to those who have been authorized to access the EPO.

Best Practices

Provide a means for the individual to identify the LPO for their delegated authority. The EPO should notify all system administrators of any changes to access rights. The EPO should have mechanisms to verify the identity of all authorized users before granting access.

Enable mechanisms that ensure that only those authorized to access the EPO can view, update, or access information. Access should be limited to the minimum necessary for the purpose of the access.

Enable mechanisms to manage change records. The EPO should have mechanisms to manage change records, including the creation, modification, and deletion of access rights. The EPO should have mechanisms to manage change records, including the creation, modification, and deletion of access rights.

Domain 4: Immediate policy levers

Policy Guidance

4a) Technical interoperability (including messaging and control standards) for LPOs should be consistent with the organization's formal policies and procedures.

4b) The technical standards adopted by the EPO should reflect the organization's formal policies and procedures.

4c) The technical standards adopted by the EPO should reflect the organization's formal policies and procedures.

4d) The EPO should consider the technical standards adopted by the organization's formal policies and procedures.

Best Practices

Without sharing responsibility for maintaining the security of the directory, the LPO should be accountable for keeping the content and data secure. The LPO should be accountable for maintaining the security of the directory, the LPO should be accountable for keeping the content and data secure. The LPO should be accountable for maintaining the security of the directory, the LPO should be accountable for keeping the content and data secure.

Appendix A

Terminology

- LPO: Local Patient Registry
- HIPAA: Health Insurance Portability and Accountability Act
- EHR: Electronic Health Record
- HIE: Health Information Exchange
- PCC: Patient-Centered Care
**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.

**End-Level Provider Directory (ELPD):** A directory listing provider organizations involved in End-Level Provider Directory (ELPD); a directory listing technical providers.

**Entity:**
Any organization involved in the exchange of health information, including submitters, receivers, requesters, and providers of such information.

**Organizational entities:** The legal organization involved in the exchange.

**Technical entities:** The systems/environments that can interact with people through displays, etc., send and receive messages in standardized ways, etc.

**Individual Provider/Clinician:**
Individual health care provider (as HIPAA/TECH definition)

**Sender:**
Authorized end point organizational entity or the employees of a technical entity that generates and sends an exchange.

**Receiver:**
Authorized organizational entity or its employees or proxy technical entities that receive and/or accept the exchange.

**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.

---

**Appendix 2 Use Cases**

**ILPD Use Cases 1. Clinic to Clinic Exchange - Push Scenario**

**Exchange Need**
- A POC in Clinic X wishes to send a clinical document about a patient to a specific individual provider, a Specialist in Clinic Y.
- Submitter has some information about the individual provider (e.g., name, specialty) but does not have individual provider's location information.

**ILPD Functionality**
- Submitter uses ILPD to identify locations where the individual provider practices.
- The ILPD provides a listing of potential locations where the specialist practices.
- Submitter identifies appropriate location to send information.
- ILPD associates physical location with ILPD address.
- Using ILPD, the digital certificate is signed and the sending and receiving computer are used to validate identity.

**Achieving Exchange**
- Clinic X's EH subsystem sends patient summary (e.g., CCD) to Clinic Y's EH subsystem.
- Clinic Y's EH subsystem receives the patient summary and incorporates data into the patient's record in the EH subsystem.
### ILPD Use Cases

#### 2. Clinic to Clinic Exchange - Pull Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Specialist in Clinic X needs to get a patient summary document from a</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 3. Hospital to Clinic Exchange - Push Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Specialist in Clinic Y uses ILPD to look up potential locations for</td>
<td>Hospital sends an EHR summary (e.g., CCD) to Clinic X's EHR</td>
<td>Hospital receives the request and validates the need.</td>
</tr>
<tr>
<td>the physician in Clinic X who is seeing the patient.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 4. Hospital to Clinic Exchange - Pull Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Hospital needs to retrieve data about patient from Clinic X.</td>
<td>Establishes relationships with EHRs of the Clinic X to pull data.</td>
<td>Thomas identifies patient data and sends it to the hospital.</td>
</tr>
<tr>
<td>A Hospital only knows the patient’s name.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 5. Clinical Lab to Clinic Exchange - Push Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Lab wants to send results about Patient X to ordering provider and</td>
<td>Hospital receives the result and sends it to Clinic X's EHR.</td>
<td>Hospital receives the result and sends it to the patient's EHR.</td>
</tr>
<tr>
<td>others on Clinic X team.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Notes:**
- ILPD = Interoperable Laboratory Data
- EHR = Electronic Health Record
- CCD = Continuity of Care Document
- COA = Clinical Office Actuation
- ILPD = Interoperable Laboratory Data
## ILPD Use Cases

### 6. Public Health Alerts - Push Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public health agency needs to send an alert to selected individual providers.</td>
<td>Public health agency uses ILPD to identify individual providers and location.</td>
<td>Public Health Institution sends alerts to providers' EHR systems.</td>
</tr>
<tr>
<td>(Communicable disease, drug or device issue, etc.)</td>
<td>ILPD needs to provide flexible alerts that identify providers for various types of</td>
<td>Provide EHR systems receive alerts and incorporate into the EHR.</td>
</tr>
<tr>
<td>Public health agency has some information on individual provider(s), but</td>
<td>alerts. ILPD lists potential locations of providers where it wants to send alerts</td>
<td>Providers' EHR systems may send alerts to providers and potentially trigger additional actions as necessary.</td>
</tr>
<tr>
<td>does not have individual provider's location information.</td>
<td>Public Health Institution identifies proper locations (potentially automatically).</td>
<td>Public Health agency has some information on the individual provider(s) of these patients but does not have individual provider's location information.</td>
</tr>
<tr>
<td></td>
<td>Using the ILPD, the digital credentials of both the sending and receiving computers are used to validate identities when the results are delivered.</td>
<td></td>
</tr>
</tbody>
</table>

### 7. Public Health Query - Pull Scenario

<table>
<thead>
<tr>
<th>Exchange Need</th>
<th>ILPD Functionality</th>
<th>Achieving Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public health agency needs additional information from the EHR of patients with a reportable condition (e.g., communicable disease, drug or device issue).</td>
<td>Public health agency uses ILPD to identify individual providers' locations.</td>
<td>Public Health Institution sends requests to providers' EHR systems.</td>
</tr>
<tr>
<td></td>
<td>ILPD lists potential locations of providers where it wants to send alerts.</td>
<td>Providers' EHR systems receive requests and incorporate into the EHR.</td>
</tr>
<tr>
<td></td>
<td>Public Health Institution identifies proper locations (potentially automatically).</td>
<td>Providers' EHR systems may send queries to providers and potentially trigger additional actions as necessary.</td>
</tr>
<tr>
<td></td>
<td>Using the ILPD, the digital credentials of both the sending and receiving computers are used to validate identities when the results are delivered.</td>
<td>Public Health agency requests additional clinical information from the EHR for a patient with a reportable condition.</td>
</tr>
</tbody>
</table>