HIT Policy Committee

Information Exchange Workgroup

Summary of Final Recommendations on Individual-Level Provider Directory (ILPDs)

Micky Tripathi, Massachusetts eHealth Collaborative, Chair

David Lansky, Pacific Business Group on Health, Co-Chair

March 2, 2011

Information Exchange WG

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

Name	Affiliation
Hunt Blair	Vermont Medicaid
Jim Buehler	CDC
Connie W. Delaney	University of Minnesota, Nursing
Paul Egerman	
Judy Faulkner	Epic
Seth Foldy	CDC
Donna Frescatore	NY Medicaid
Jonah Frohlich	Manatt Health Solutions
Dave Goetz	Dept. of Finance and Administration, TN
James Golden	Minnesota Department of Health
Gayle Harrell	

Name	Affiliation
Dianne Hasselman	Center for Health Care Strategies
George Hripcsak	Columbia University
Jessica Kahn	CMS
Charles Kennedy	WellPoint, Inc.
Michael Klag	Johns Hopkins School of Public Health
Deven McGraw	Center for Democracy & Technology
George Oestreich	Missouri Medicaid
David A. Ross	Public Health Informatics Institute
Steven Stack	American Medical Association
Walter Suarez	Kaiser Permanente
Latanya Sweeney	Carnegie Mellon University

ONC Staff Lead(s): Claudia Williams, Kory Mertz

Provider Directory Task Force Members

Co-Chair: Jonah Frohich, Manatt Health Solutions
Co-Chair: Walter Suarez, Kaiser Permanente

Name	Affiliation
Hunt Blair	Vermont Medicaid
Sorin Davis	CAQH
Paul Egerman	
Judy Faulkner	Epic
Seth Foldy	CDC
Dave Goetz	Ingenix
James Golden.	Minnesota Department of Health
Keith Hepp	HealthBridge
Jessica Kahn	CMS
JP Little	Surescripts
George Oestreich	Missouri Medicaid
Lisa Robin	Federation of State Medical Boards
Steven Stack	AMA
Sid Thornton	Intermountain Healthcare

ONC Staff Lead(s): Claudia Williams, Kory Mertz

ILPD Framework

Directory Requirements and Options → Recommendations

Participants, Users, Uses	Functions	Content	Operating rqmts	Business models	Policy issues	Policy actions
Who is on an ILPD? Who wants an ILPD? What do they want to use it for?	What functions do users need for their desired uses?	What data will be required in order to enable desired functions?	What operating business requirements will be needed in order for this to be used?	What are possible business models for meeting needs?	Which business models should the government promote? What are the policy issues related to each of the suggested business models?	What policy actions should be taken to address the policy issues?

Final Recommendations to IE WG by February 28; Present to HITPC by March 2

Final Recommendations to IE WG by February 28; Present to HITPC by March 2

ILPD Recommendations

Definitions: ILPD v. ELPD

- **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

See Appendix A for additional terminology

Value Propositions

- Users can identify and verify recipient information and electronic links via ILPD instead of having to contact each recipient
  - Simplified workflow, increased automation potential
- User system no longer responsible for maintaining its own ILPD
  - Shared costs, higher quality information
- User system can determine what information exchange capabilities are available at each recipient
  - Enrich content transfer, enable more automation, reduce errors
- User can potentially query ILPD for additional information, e. g. administrative facts: license, degree, etc.
  - Strong business cases for administrative transactions

Recommendations

- ILPD recommendations generally fall into one of the following categories
  - Recommended practices
    - Items that should be considered in establishing and operating an ILPD
  - Areas required to enable basic interoperability
    - States will have different use cases for ILPDs that will require varying content and functionality. A minimum level of standardization is required to allow for interoperability for the exchange use cases.

ILPD Assumptions and Framing

- Scope of ILPDs is at sub-national level
- Rigid conformance to a comprehensive set of national standards is not necessary; Conformance to a minimum, basic set of standards is needed to support interoperability across ILPDs.
- States are currently implementing ILPDs as we speak. Need to produce recommendations rapidly.
  - Focus on best practices for establishing and maintaining ILPDs (particularly data accuracy)
  - Best practices for local policy levers for incenting participation in ILPDs

ILPD Assumptions Continued…

- ILPD listings would provide enough information to enable resolution of appropriate destination for message, e. g. if ILPD returns multiple listings then knowledge of requester would be sufficient to choose correct location
- ILPD would list location(s) of individual providers
- ILPD would have a relationship (many-to-many) with the ELPD
- Maintenance and updates to ILPD would be managed at the local/regional level – not necessarily managed/supported at national level
- Primary value proposition is the exchange of clinical documents where providers have only basic information about another provider where the patient is seeking care and needs to locate their practice (EHR).

Recommendations: ILPD Participants

Recommendations:

1. Participants are individuals who can be listed in an ILPD and should include all individual health care providers who are licensed or otherwise authorized by a state to provide health care services or support the health of populations
    1. Individuals involved in health information exchange transactions (whether receivers or seekers of information)
    2. That need to be identified at the individual level for purposes of receiving or requesting health information

Recommendations: ILPD Users

Recommendations:

1. Users with access to an ILPD's content should include clinicians and support and administrative staff.
2. 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. (see recommended Operational Requirements)
3. Some sensitive content (state license and DEA numbers, etc.) needs to be restricted and user access to this information limited.

Recommendations: ILPD Uses ➔ Use Case Scenarios

- **Scenarios**
  - Clinic-to-Clinic Exchange – Push and Pull Scenarios (2)
  - Hospital-to-Clinic Exchange – Push and Pull Scenarios (2)
  - Public Health Alert & Investigation – Push and Pull Scenarios (2)
  - Lab-to-Clinic Exchange – Push Scenario (1)

Note: Pull Scenarios are not required transactions in MU

- **Common Threads across Scenarios**
  - Submitter needs to send a message to an individual provider
  - Submitter has some information on individual but does not have individual's location information
  - ILPD is used to identify all possible locations
  - With additional information, submitter identifies/selects appropriate location
  - ILPD links to ELPD to obtain security credentials/digital certificates location of submitter/receiver entities
  - Submitter sends data to individual provider at the identified location
- **Privacy and Security Considerations**
  - All use cases are contingent on following all federal and state privacy laws and rules.
  - Pull use case adds an extra layer of complexity that requires a strong focus on following relevant privacy laws and rules.

See Appendix 2 for Description of Use Case Scenarios

Recommendations: ILPD Content

Recommendations:

1. Individual providers, not entities or organizations should be listed in the ILPD. The individual provider types listed in the ILPD should conform to federal and state rules on who is licensed or otherwise authorized to provide health care services
2. Information needed for an individual provider listed in the ILPD 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
   - *Potentially sensitive identifiers*: NPI, DEA, State License #, etc.
3. To serve intended purposes, information should be authoritative—representing all providers of types covered—and accurate
4. There should be limited access to and tight policies regarding access to potentially sensitive identifiers (such as state license numbers, DEA numbers, etc) to minimize the risk of fraud and identity theft.
5. 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.

Recommendations: ILPD Functional Capabilities

Recommendations, ILPD services should:

1. Support directed exchanges functions (send/receive as well as query/retrieve)
2. Provide basic “discoverability” of an individual provider and their practice location(s). The service should support querying capability at multiple levels (practice location, provider name, specialty, etc.)
3. Provide both basic “discoverability” and tight linkage to an individual provider’s ELPD listing
4. Support audit trail capabilities

Recommendation: ILPD Operational Requirements

Recommendations - ILPD operators should:

1. 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
2. Establish policies and procedures to verify, as appropriate, the information provided by individuals enrolling in the ILPD
3. 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
4. Establish policies and procedures that define who can access and use the ILPD and which data can be accessed (including policies on restricted access to sensitive information)
5. Ensure that the ILPD is able to interoperate with other ILPDs developed and operated in a manner that follow these recommended standards

Recommendation: ILPD Operational Requirements (cont)

Recommendations - ILPD operators should:

6. 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
7. 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
8. Develop and put into place audit trail policies and procedures to track access and use, and investigate inappropriate use and breaches

Recommendation: ILPD Operational Requirements (cont)

Recommendations - ILPD operators should:

9. 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).
10. Develop procedures and a set of policies to establish appropriate linkages between ILPDs and ELPDs, update a provider's ILPD listing(s) with their affiliated ELPD listing(s), and allow interactive access to ELPD information about the entities associated with individual providers listed in the ILPD.
11. Implement security policies and procedures that ensures that a) data contained in the ILPD is appropriately protected from unauthorized changes; b) authorized individuals have access to the data for purposes of updates/changes; and c) access to information contained in the ILPD by external users is appropriately managed

Recommendation: Cost and Business Model Considerations

Recommendations/Considerations:

1. 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
2. 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
3. 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.

Policy Considerations for ILPDs

Recommendations/Considerations:

1. The HITSC should be directed to identify and recommend to ONC technical interoperable standards (including message and content standards) for ILPDs, consistent with the HIT Policy Committee recommendations on ILPDs and working with ONC's S&I Framework to develop new standards needed
2. CMS should make NLR and PECOS content available to ILPD services funded through the State HIE Cooperative Agreement program.
3. States using HIE Cooperative Agreement funds to establish state-level ILPDs should make these provider directory resources and services available to participants in private and publicly sponsored networks
4. CMS should consider how they could require state Medicaid agencies to incorporate ILPD use as they approve Medicaid Health IT Plans and fund state EHR incentive programs.
5. ILPD that choose to use ELPD services will be expected to meet a set of participation requirements

<u>Additional policy opportunities once standards are adopted:</u>

1. State HIE Cooperative Agreement grantees supporting the development of ILPDs are required to follow HITPC and HITSC recommended and ONC/CMS adopted ILPD standards and policies.
2. The federal EHR Certification process incorporates HITSC recommended and ONC adopted ILPD-related EHR certification criteria.

Appendix A
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

ELPD Recommendation: Basic Common Terminology

- **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
Use Cases

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

Exchange Need	ILPD Functionality	Achieving Exchange
• A PCP in Clinic X needs 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	• Submitter uses ILPD to identify locations where 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 ELPD address • Using ELPD, the digital credentials or both the sending and receiving computers are used to validate identifies	• 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

ILPD Use Cases
2. Clinic to Clinic Exchange - Pull Scenario

Exchange Need	ILPD Functionality	Achieving Exchange
• A Specialist in Clinic Y needs to get a patient summary document from a PCP in Clinic Y • Specialist has some information about the individual provider (e.g., name, specialty) but does not have individual provider's location information	• Specialist/Clinic Y uses ILPD to look up potential locations where PCP practices • The ILPD provides a listing of potential locations where the PCP practices • Specialist identifies appropriate location to send request/query • ILPD associates physical location with ELPD address • Using ELPD, the digital credentials or both the sending and receiving computers are used to validate identifies	• Clinic Y's EHR sends request for immediate patient summary delivery (i.e. CCD) to Clinic X's EHR • Clinic X EHR system receives the request and validates the need • 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

ILPD Use Cases
3. Hospital to Clinic Exchange - Push Scenario

Exchange Need	ILPD Functionality	Achieving Exchange
• Hospital needs to send a patient document (discharge summary, ED report, Surgical Report, etc) or utilization event alert to the patient's PCP in Clinic X • Hospital has some information about the individual provider (e.g., name, specialty) but does not have individual provider's location information	• Hospital uses ILPD to look up potential PCP physical locations • ILPD lists potential locations of PCP where patient may receive their care • Hospital identifies correct location • ILPD associates physical location with the PCP's ELPD address • Using the ELPD, the digital credentials of both the sending and receiving computers are used to validate identities	• Hospital discharge summary of a patient or utilization event alert is sent from hospital information system (EHR) to the clinic X EHR where patient's PCP practices and the patient's record resides • Clinic's EHR system receives the hospital report and incorporates data into the patient's record in the EHR

ILPD Use Cases
4. Hospital to Clinic Exchange - Pull Scenario

Exchange Need	ILPD Functionality	Achieving Exchange
• Patient shows up at a hospital ER • Data is scattered across multiple settings • Hospital needs to retrieve data about patient from clinic • Hospital only knows clinicians' names	• Hospital uses ILPD to identify the location(s) of providers • ILPD lists locations (i.e., clinics) of all providers where patient may receive their care • Hospital submits queries to all those locations • Clinics receiving queries use ELPD to identify Hospital requester, obtain security credential information • Clinics validate requester and determines if they have data about patient	• Clinics submit data (i.e., CCD or CDA) to hospital

ILPD Use Cases
5. Clinical Lab to Clinic Exchange - Push Scenario

Exchange Need	ILPD Functionality	Achieving Exchange
• Clinical Lab would like to send results about Patient X to ordering provider and possibly 'cc' others on care team • Clinical lab knows individual provider who ordered test; but does not have individual provider's location information	• Clinical Lab uses ILPD to obtain needed information about order provider and other recipients • ILPD returns locations, electronic address and potentially other relevant information about ordering provider and other recipients • Clinical Lab conducts CLIA verification (may use ILPD information regarding what information exchange capabilities are available at each recipient) • Using the ELPD, the digital credentials of both the sending and receiving computers are used to validate identities when the results are delivered.	• Lab results are sent from Clinical Lab system to Ordering Provider's (or other care team provider) EHR • Ordering Provider's EHR system receives the lab result and incorporates it into the patient's record in the EHR

ILPD Use Cases
6. Public Health Alerts - Push Scenario

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

ILPD Use Cases
7. Public Health Query - Pull Scenario

Exchange Need	ILPD Functionality	Achieving Exchange
• Public health agency needs additional information from the EMR of patients with a reportable condition (e.g., risk factors, disease progression, sequelae, proper treatment/follow up) or post marketing surveillance • Public health agency has some information on the individual providers of those patient; but does not have individual providers' location information	• Public health agency uses ILPD to identify individual providers' locations • ILPD lists potential locations of providers where it wants to send alerts • Public Health Institution identifies proper locations (potentially automatically) • Using the ELPD, the digital credentials of both the sending and receiving computers are used to validate identities when the results are delivered.	• Public Health Institution sends request to providers' EHR systems • Providers' EHR systems receive alerts and incorporate into the EHR • Providers' EHR systems may send queries to providers and potentially trigger additional actions as necessary • Public health agency receives additional clinical information from the EMR for a patient with a reportable condition