Health IT Policy Committee

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

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 follow these recommended standards.

III. Recommendations on Security, Access, Audit

Policy Guidance

3a) Access to an ILPDs 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

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 Frohlich, 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

3

Background: ELPDs

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

A Nationwide ELPD Registry comprising multiple, federated ELPDs

Characteristics of ELPDs

National in scope; federated "internet-style" architecture

Information maintained at the entity-level

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

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

Operationalizing ELPDs

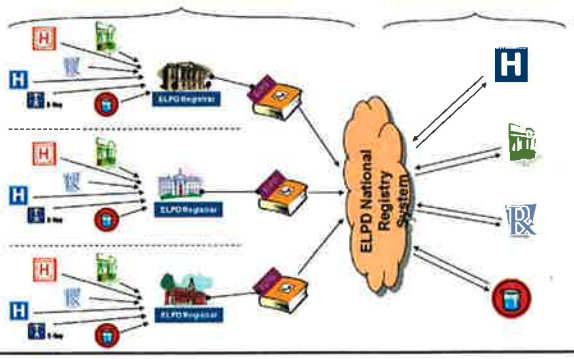
HITSC to create standards for single national registry with multiple registrars

Incorporate ELPD use in MU Stages 2/3 and NHIN participation requirements

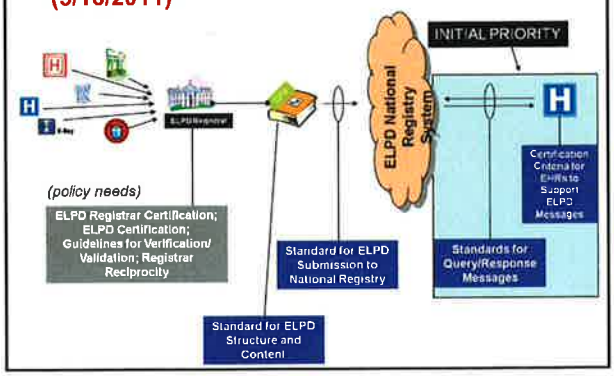
Require Beacon and state-level HIE programs to integrate with national-level ELPD

4

Background:
Slide from HITSC Privacy & Security WG (3/16/2011)



Background:
Slide from HITSC Privacy & Security WG (3/16/2011)



Background: Individual-Level Provider Directories

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

Many ILPDs already exist in the market

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

Much local variation in uses, content, and structure

Common characteristic is that ILPDs maintain individual, clinician-level information, though the scope of the information available on an individual varies with the intended use

ILPDs facilitate basic health exchange functions by enabling "discovery" of key individual characteristics and mapping individuals to entity addresses

Could be key enablers of Direct transactions by allowing discovery of security credentials

Some ILPDs may be used solely for health exchange transactions, whereas others may layer on additional uses such as medical credential verification, health plan participation, etc

Security credentials – either individual or entity-level, as per relevant policies. The ILPD will need to support the level of security credential required by the exchange participants

Linking ILPDs with ELPD will establish a national registry system that is locally flexible but nationally conformant

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

7

ILPD Use Cases and Link to ELPD

- **Possible Scenarios**
  - Clinic-to-Clinic Exchange – Push and Pull
  - Hospital-to-Clinic Exchange – Push and Pull
  - Public Health Alert & Investigation – Push and Pull
  - Lab-to-Clinic Exchange – Push
- **Common Workflow 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**

8

Two Types of Recommendations in Four Domains

Two Types of Recommendations

Policy guidance

Areas required to enable creation of national directory system

Minimum level of standardization needed to link ILPDs with each other and with the national ELPD-based national registry system

Best practices

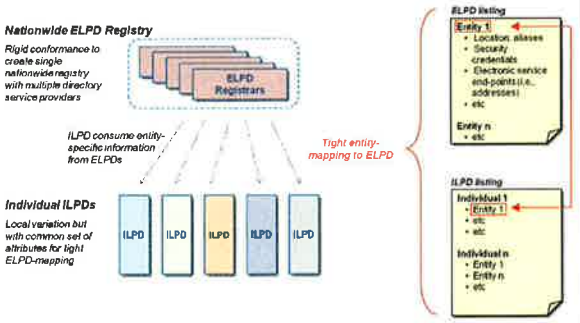
- Items that should be considered in establishing and operating an ILPD, in the best judgment of the IE WG
- Want to give helpful direction to local ILPD development while still allowing flexibility for tailoring to meet local needs

Four Domains

1. **Content**
   - What minimal data should be included in all ILPDs? (Individual, Attributes)
2. **Functionality**
   - What core functions should all ILPDs support? (Discoverability, Tight Mapping to ELPD)
3. **Security, access, and audit**
   - What protections should be adopted by all ILPDs? (Access, Sensitive Content, Data Integrity, Audit)
4. **Immediate policy levers**
   - What policy levers should Federal and State governments use to facilitate ILPD creation and sustainability? (Interoperability, EHR certification, NLR/PECOS, State HIE programs, Medicaid)

9

High-level view of Provider Directory Approach



10

Areas that our recommendations do not cover

Workgroup deliberations were driven by growing sense of urgency from funded state-level activities embarking on directory approaches

Policy recommendations developed to identify immediate policy levers to harmonize provider directory activities without slowing them down

Create a framework for linking and building on existing private- and public-sector directories – no organization should have to rip and replace

Many moving parts in federal and state policy arenas prevent making more specific recommendations in the following areas at this time:

Organization

Who should be responsible for driving creation of a national provider directory service (ELPDs/ILPDs), and how should it be operationalized in the market?

Design, launch, operations and maintenance

Business models

How should a national provider directory service be paid for?

Fixed costs, recurring costs, public vs. private

Governance

How should the national provider directory service be governed, and by whom, and with what authorities?

Relationship to NwHIN governance, relationship to state/regional HIE governance

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

11

Domain 1: Content

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)

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

12

Domain 2: 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 follow these recommended standards

13

Domain 3: Security, Access, Audit

Policy Guidance

3a) Access to an ILPDs 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).

14

Domain 4: 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.

15

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

20

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

Exchange Need	ILPD Functionality	Achieving Exchange
• A Specialist in Clinic X 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

21

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

22

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

23

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