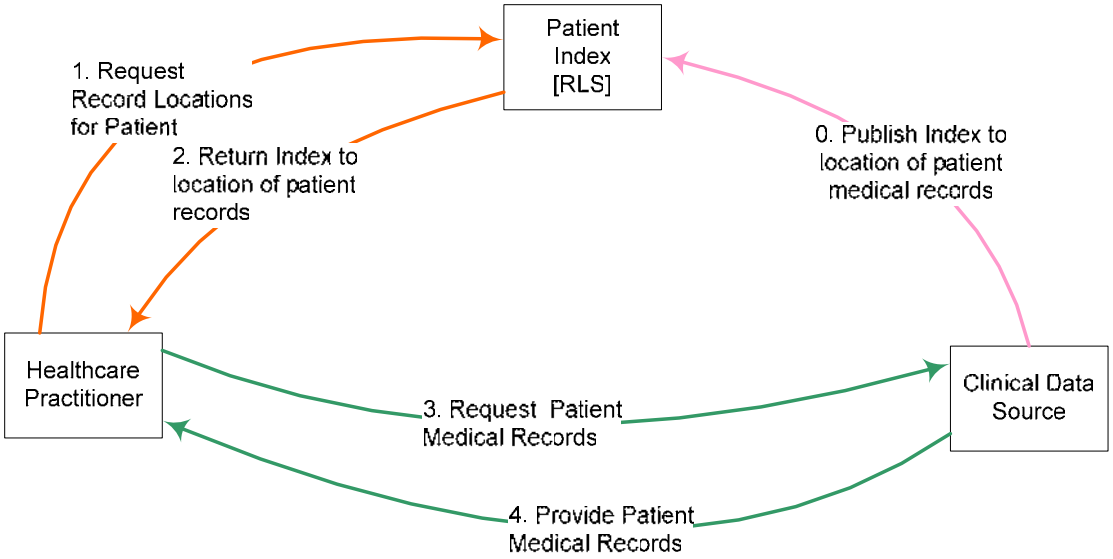
Linking Patient Records
John D. Halamka MD

Agenda

- RLS Architecture
- Security Architecture
- Prototype Demonstration Screen shots
- Patient Linking and Matching

High Level Functional Architecture

- Publish patient index (record location) from local data source to central registry
- Acquire address (record location) of EHR system and local patient index from central registry
- Retrieve medical data directly from data source on peer-to-peer basis [***Not RLS function***]
- Conforms to Web-services interop pattern: Publish/Find/Bind



✦ Adapted from: Linking Healthcare Information: Proposed Methods for Improving Care and Protecting Privacy, Carol Diamond, Connecting for Health, Markle Foundation, HIMSS 2005

Use case scenario / workflow

1

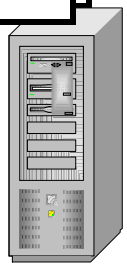
1. Patient visits physician / practitioner and person / visit-related information is entered into local clinical system
2. Patient consents for (selective) release of information to others
3. System produces a record of the person / visit
4. Person / visit record is "published" for other utility users

Source Clinical Data System Gateway

Clinical Data Exchange

2

1. Patient index entry is created at community level
2. Index = Patient demographics + source system address + patient source system identifier



4

1. Exchange receives patient lookup request
2. Reads previously populated patient index to determine where medical records may reside
3. Patient is identified in patient index and matching patient index information with record locations returned
4. Returned data logged

Secure Internet / Leased Private Network

6

1. Source with releasable medical records (of type requested) receives request for records
2. Request is authenticated and checked for release consent
3. Cached or source records are retrieved and formatted to standards
4. Request and return are logged for auditability
5. Records are returned to requestor
6. Returned data logged

3

1. Patient visits another utility user
2. Utility user logs on, is authenticated and queries patient index: enters patient demographics to search for and retrieve electronic medical records
3. Request is logged for auditability

Requesting Clinical Data System Gateway

5

1. One or more patients with releasable records are presented to user for selection
2. User selects patient records (if human disambiguation is required and allowed), or record requests are automatically sent to source systems
3. Request logged

7

1. Returned records are aggregated, if required
2. Business logic is applied to records
3. Records are presented for viewing or formatted for other purposes (integration with legacy / core systems, use in business process, additional workflow, etc.)
4. Returned data logged

= Publish patient index

= Locate patient records

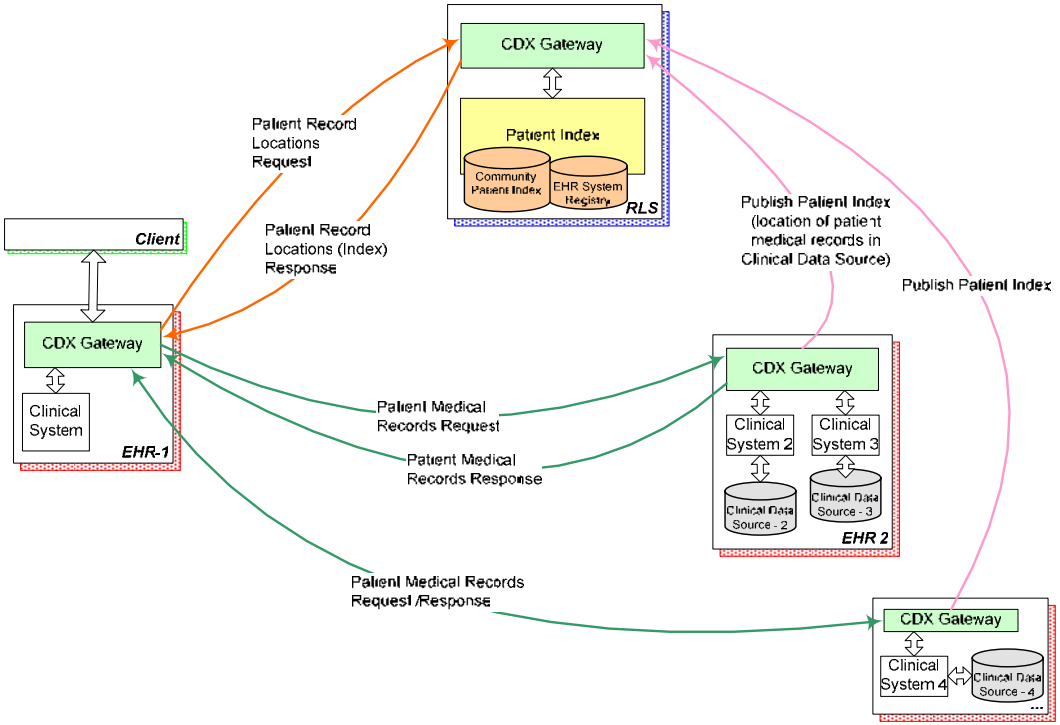
= Retrieve patient records

Supporting processes are required for:

- Security administration
- Registration and identity administration
- Consent management, access control, logging, and audit - tracking inquiry, access and use

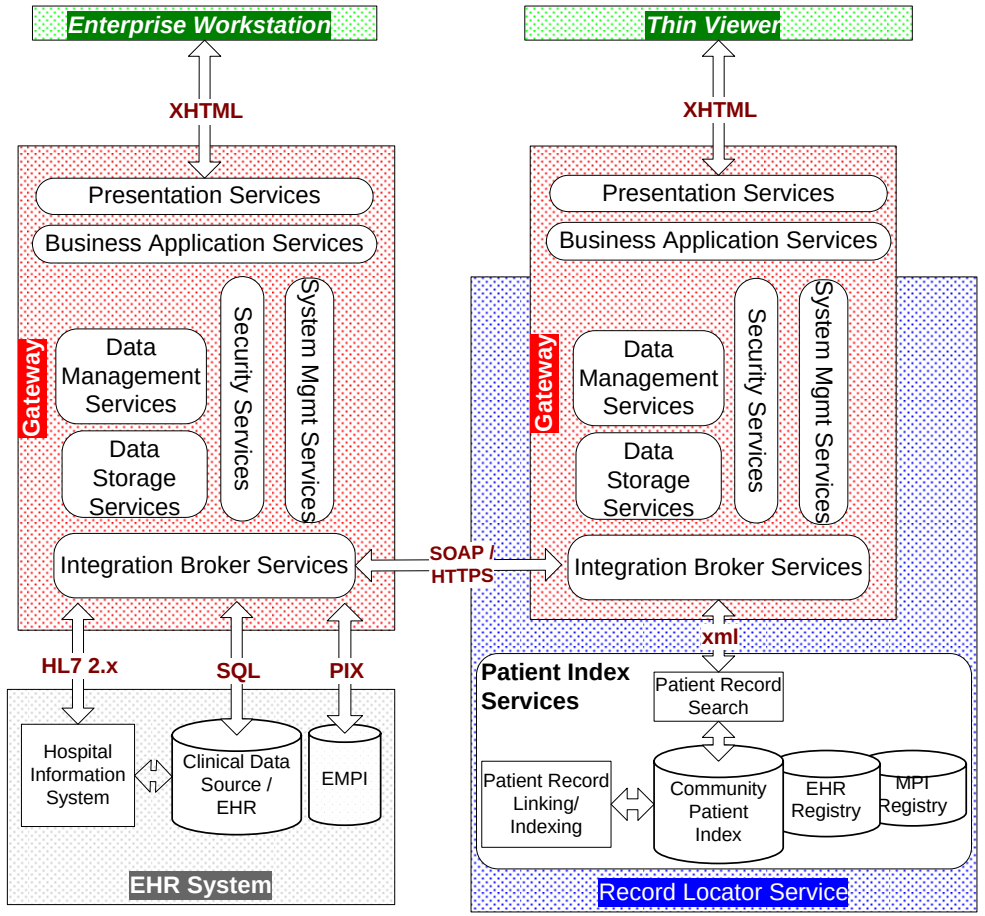
RLS Technical Architecture using Gateway

- RLS: index and registry
  - Returns record locations of patients matching demographics search criteria entered by authorized healthcare practitioner
  - Maintains contract between providers & consumers
  - CMPI with record linking algorithm matches patients from different EHRs
- Gateway: secure, standards based data interchange
  - Encapsulate:
    - Service gateway (agent) to consume web services without changing consuming application
    - Service interface to wrap disparate legacy applications with web service interface
    - Mapping service to transform message formats
    - Security and Systems Management Services
  - Abstract both RLS and EHR (legacy) systems to enable standards based communication between disparate systems
  - Extensible to clinical data exchange (CDX)



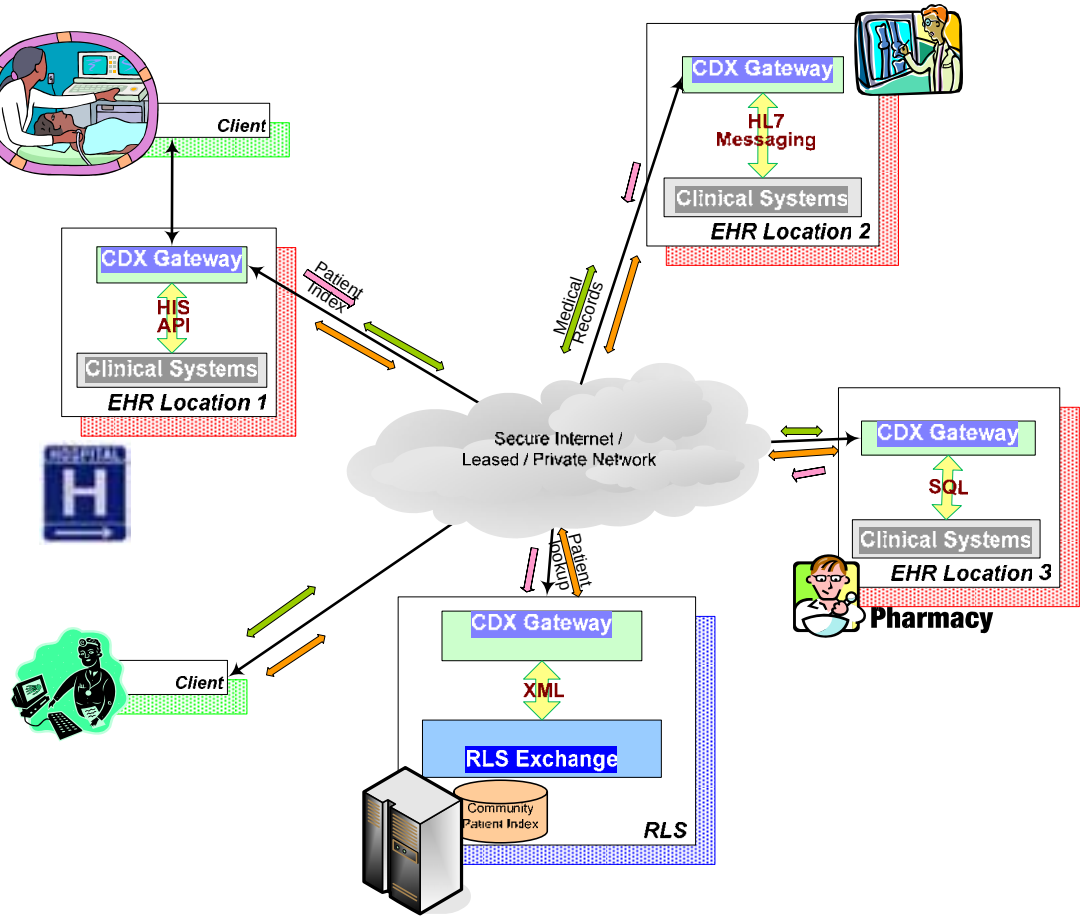
Service-Oriented Application Architecture

- RLS: composite application made up of loosely coupled, coarse grained services
  - Core Service: Patient Index Service
  - Central registry of distributed EHR systems and other CMPIs / EMPIs
- Gateway: provides common infrastructural (plumbing) services
  - Systems management including logging, auditing, service management
  - Security: authentication, policy, consent management
  - Integration services: messaging, transformation, orchestration, adaptor
  - Presentation/Business services for user interface
- Common services reused across RLS and Gateway



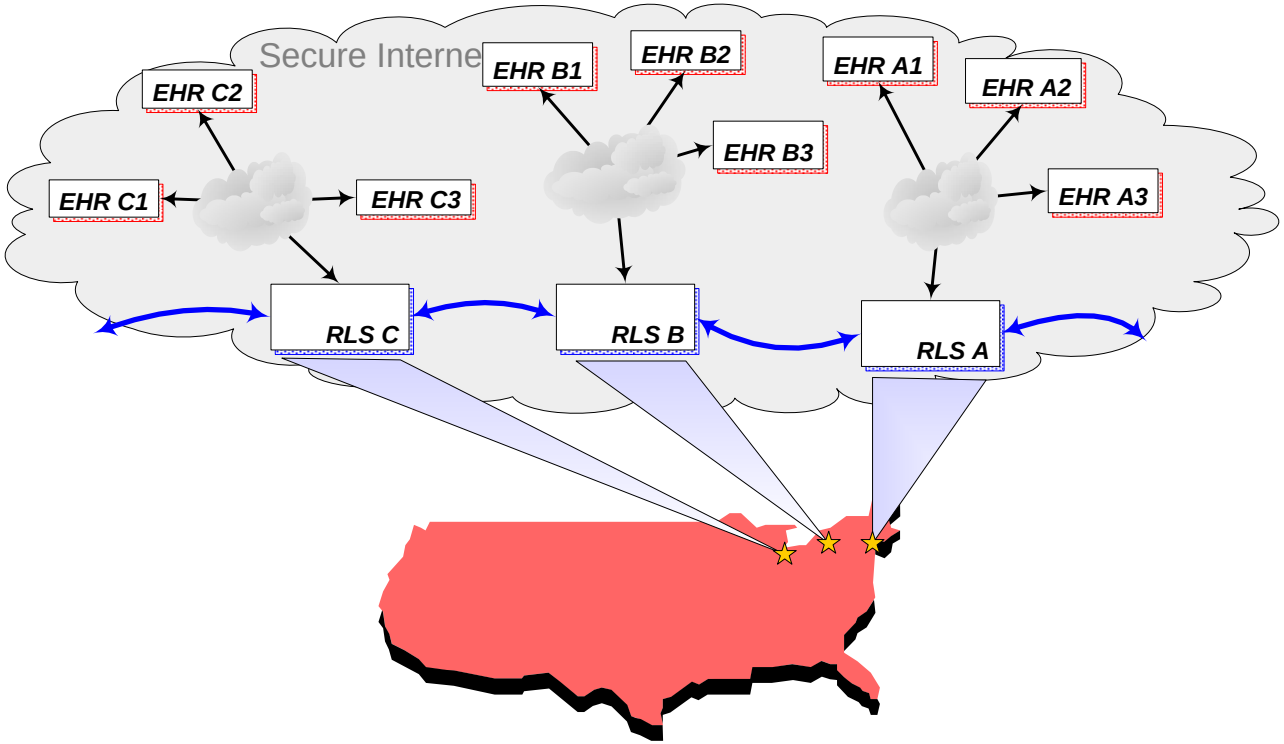
Gateway Web-service enables legacy systems

- Gateway provides interface layer between clinical systems using
  - HL7
  - SOAP
  - XML
  - https
- Abstracts differences between application interfaces
- Gateway at RLS
  - Hosted Gateway implementation
  - Enables direct client access to remote clinical systems
  - Low cost solution for small providers
  - Minimal requirement: Web browser



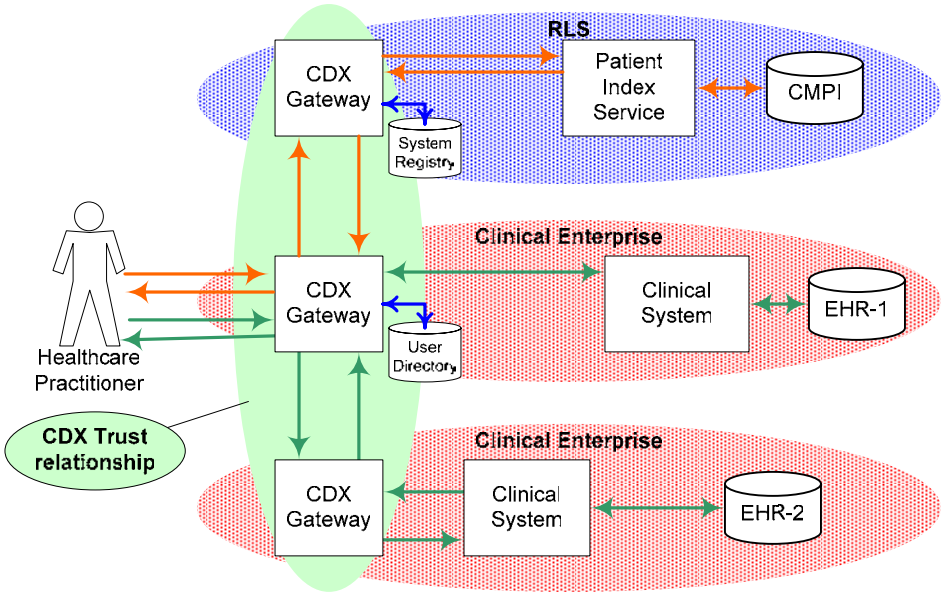
Architecture supports communication between RLSs

- RLS maintains registry of other MPIs and can pass on patient lookup request to other RLSs
  - Enabling a network of RLS communities / RHIOs
- Data sharing possible between EHRs attached to different RLSs
  - EHRs are 'web-addressable' via Internet
- Security and contracts coordination more direct through RLS



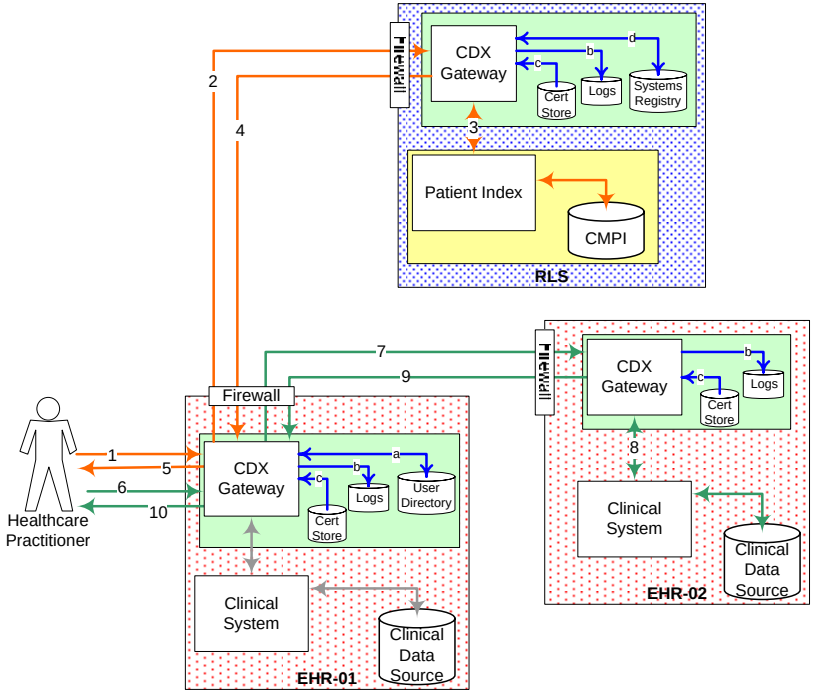
RLS Prototype Security Architecture

- Overlapping Trust Relationships
  - Security services embedded in CDX Gateway
  - Gateway is part of local Enterprise Application security architecture
    - Enterprise integration enables coordinated identity provisioning and single sign-on
  - User identities authenticated locally
    - Username communicated in each message but are not authenticated by message receiver
  - Local user roles to be mapped to common (RLS/CDX) roles and messaged along with user credentials
  - Gateway to Gateway trust relationships
    - Technologies and standards exist
    - Implementation challenges remain with distributed credentials management to support secure peer-to-peer data exchange
  - Comprehensive message logging at each gateway supports auditing of all data access



Distributed Authentication / Authorization in RLS Prototype

- Human users authenticated at edge
  - Follow enterprise security standards
- Direct trust relationship between Gateways using security tokens
  - SSL/TLS uses server-side X.509 certificates to authenticate receiver and encrypt data traffic
  - Sender authentication possible with security tokens:
    - Username / password
    - Digital certificates (X.509) with private/public keys
    - Kerberos ticket
  - Certificate management overhead in real world
  - Use application firewall to block access by unknown network entities
- Position architecture to leverage SAML / Federation standards as they mature



Patient Lookup

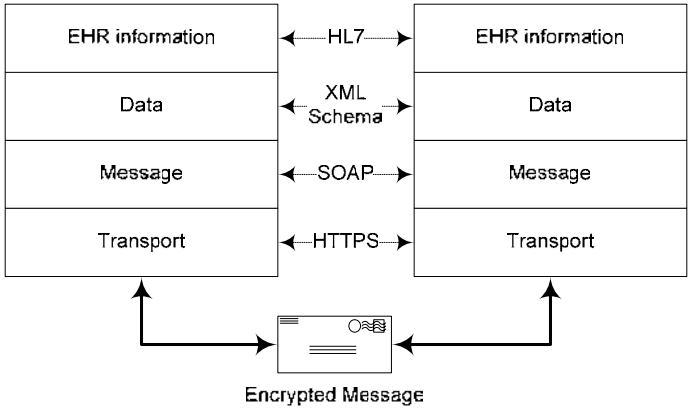
1. User logs in / enters patient lookup query (demographics)
   a. authenticated against directory
   b. access logged
2. Request for patient record locations in SOAP envelope with user identity / roles over
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL/TLS connection
3. Matching patient record locations looked up
   d. remote system authenticated against registry
   b. access logged
4. Matching records from CMPI returned
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL/TLS connection
5. Patient record locations displayed for user selection

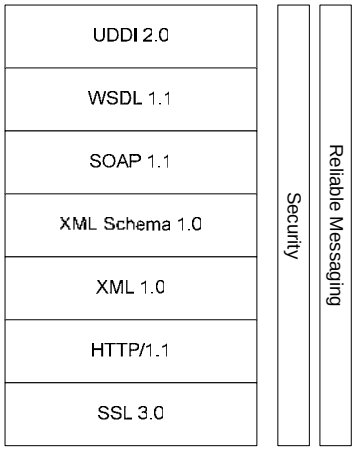
Medical Records Retrieval

6. Patient clinical records query entered
7. Request for patient medical records request in SOAP envelope with user identity / roles, and server key
   d. remote system authenticated against registry
   b. access logged
8. Patient clinical records retrieved
9. Clinical records returned to user
   c. sender-side certificate used to sign message and receiver certificate used to establish SSL/TLS connection
10. Clinical records aggregated and displayed to user

Data, Messaging, Transport Standards

- HL7
  - HL7 RIM 2 based data standards
  - HL7 Version 3.0 versus 2.x
    - XML notation recommended over EDI style
    - Canonical message format between gateways reduces many-to-many translation load
    - Version 3.0 offers semantic interoperability benefits
- Web services
  - Follow WS-I Basic Profile interop standards
    - SOAP 1.1 / WSDL 1.2 / UDDI 2.0
  - ebXML based messaging has some advantages over WS-*
    - Interoperation with DoD and CDC PHIN
    - RLS architecture does not preclude data interchange with eb-Message Services
- Security
  - Distributed user authentication and SSL based server authentication and transport level encryption
  - Message-based security in future releases using SAML, XML Signatures etc.





Prototype Components / Layers Platforms

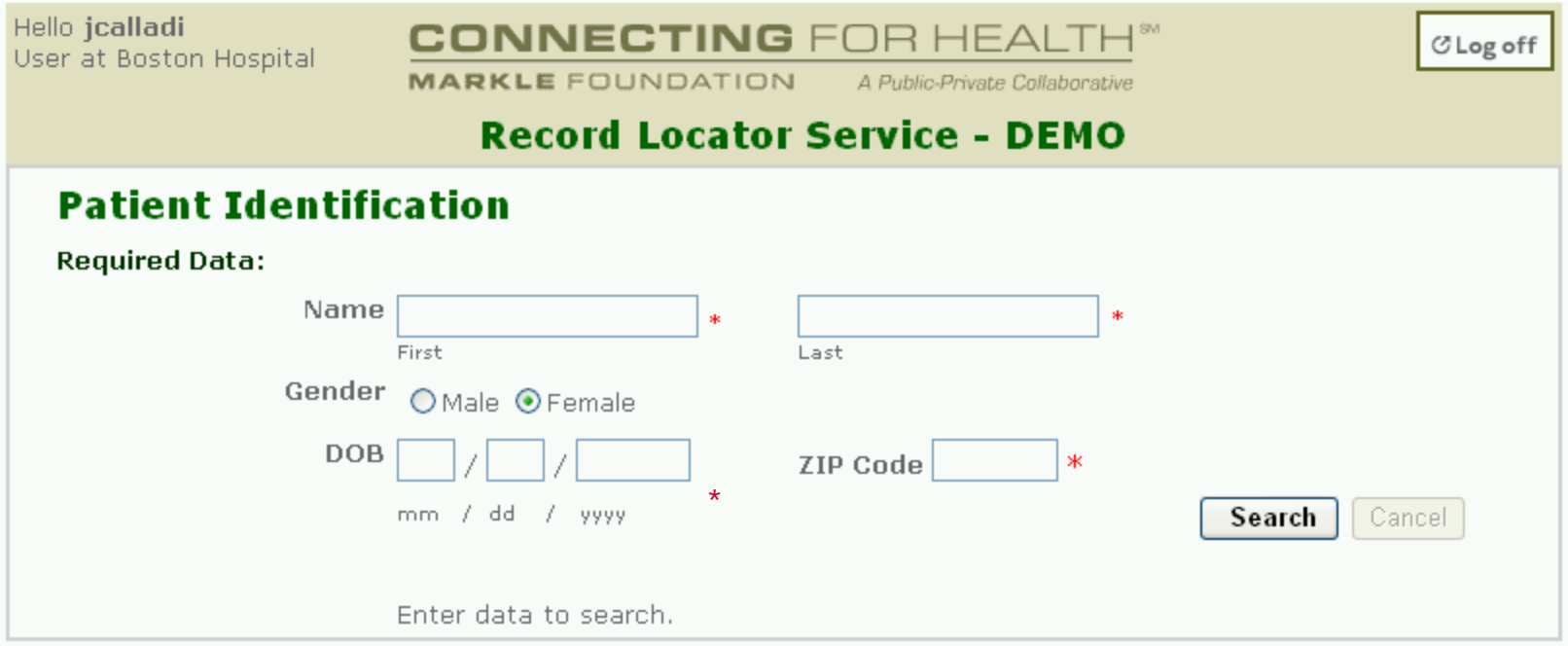
- Prototype platform choices based on expediency and rapid development capabilities
  - Post-prototype Implementation / deployment on alternate platforms
- Interoperability through adherence to open standards
  - HL7
  - SOAP
  - WSDL
  - XML

Service Layer	*Prototype Platform*	*Alternatives*
Presentation Services	ASP.NET	* JSP * PHP
Business Application Services	.NET components	* Java Servlets * EJB Session Beans * PHP / Python / Perl
Data Management Services	ADO.NET using .NET framework services	* EJB Entity Beans * PHP / Python / Perl
Data Storage Services	Microsoft SQL Server 2000	* Oracle / DB2 * MySQL / PostgreSQL
Integration Broker Services (includes messaging, orchestration, transformation and adaptor services)	Microsoft BizTalk Server 2004	* BEA WebLogic Integrator * IBM WebSphere / Mercator * InterSystems Ensemble * Orion Symphonia * SeeBeyond eGate * A combination of an Enterprise Service Bus (Sonic MQ) and an XML utility (Altova XML Suite)
	Custom components built on BizTalk framework	* Packaged adaptors from Integration broker vendors
	Microsoft BizTalk Server 2004, which uses MSMQ	* IBM WebSphere MQ
Systems Management Services	Custom .NET components using .NET framework	* CA Unicenter * IBM Tivoli * Microsoft Management Services
Security Services	Custom .NET components using simple database table for user identities / credentials	* Novell Odyssey * Sun ONE * CA eTrust

Screen Flow

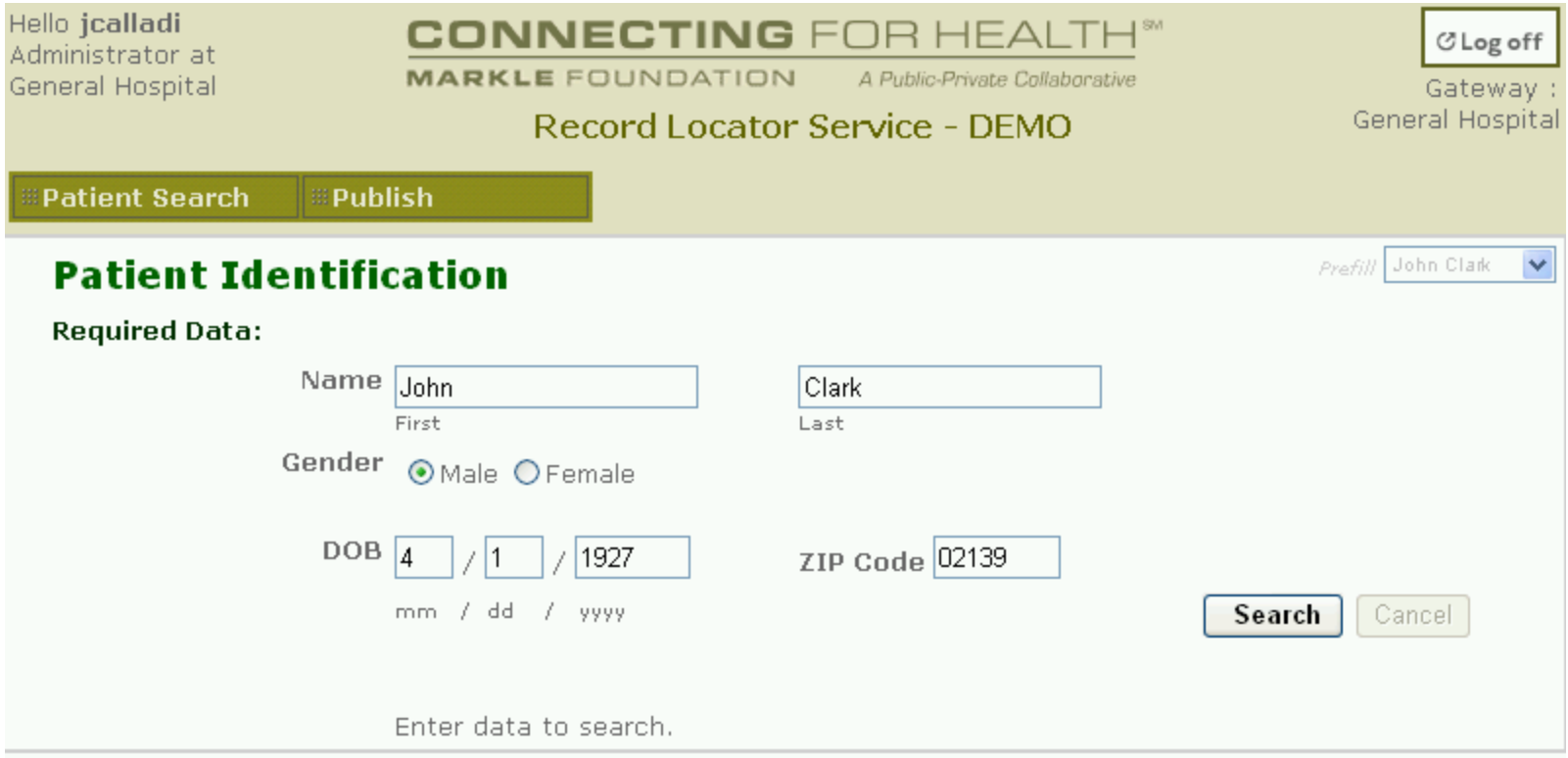

CONNECTING FOR HEALTH℠
MARKLE FOUNDATION
A Public-Private Collaborative
Record Locator Service - DEMO
Log In
User Name
jcalladi
Password
Security Disclaimer
Access to this website is for authorized users only. All access (including time and IP address) is tracked, logged and monitored. If you do not have permission to be here, you should leave immediately. This information is made available to the users by other healthcare entities. Any unauthorized use may result in hospital discipline and/or legal repercussions.
Log In:
Enter
Forgot login? Contact your administrator.
Use and disclosure of this information must comply with all applicable State and Federal privacy and security laws and regulations.
© Markle 2005
Powered by:
5/3/2005 3:39 PM | Version Strawman 0.20

Screen Flow



Required Fields when empty marked *

Screen Flow


Hello jcalladi
Administrator at
General Hospital
CONNECTING FOR HEALTH℠
MARKLE FOUNDATION
A Public-Private Collaborative
Record Locator Service - DEMO
Log off
Gateway :
General Hospital
Patient Search
Publish
Patient Identification
Prefill
John Clark
Required Data:
Name
John
First
Clark
Last
Gender
Male
Female
DOB
4
/
1
/
1927
mm / dd / yyyy
ZIP Code
02139
Search
Cancel
Enter data to search.

Screen Flow – Exact Match

Patient Search | Publish

Patient Identification

Prefill: James Abate

Required Data:

Name: John (First) Clark (Last)

Gender: (•) Male ( ) Female

DOB: 1 / 4 / 1927 (mm / dd / yyyy)

ZIP Code: 02139

Search | Cancel

...search complete.

1 record(s) found. Elapsed Time: 3 seconds.

Select	Gateway Location	MRN	Name	Gender	Birthdate	Zipcode
☐	General Hospital	41188	JOHN CLARK	M	1/4/1927	02139

Get Summary Records

Screen Flow – Probabilistic Match with Score

Patient Search | Publish

Patient Identification

Prefill: John Clark

Required Data:

Name: John (First) Clark (Last)

Gender: Male Female

DOB: 4 / 1 / 1927 (mm / dd / yyyy)

ZIP Code: 02139

Search | Cancel

...search complete.

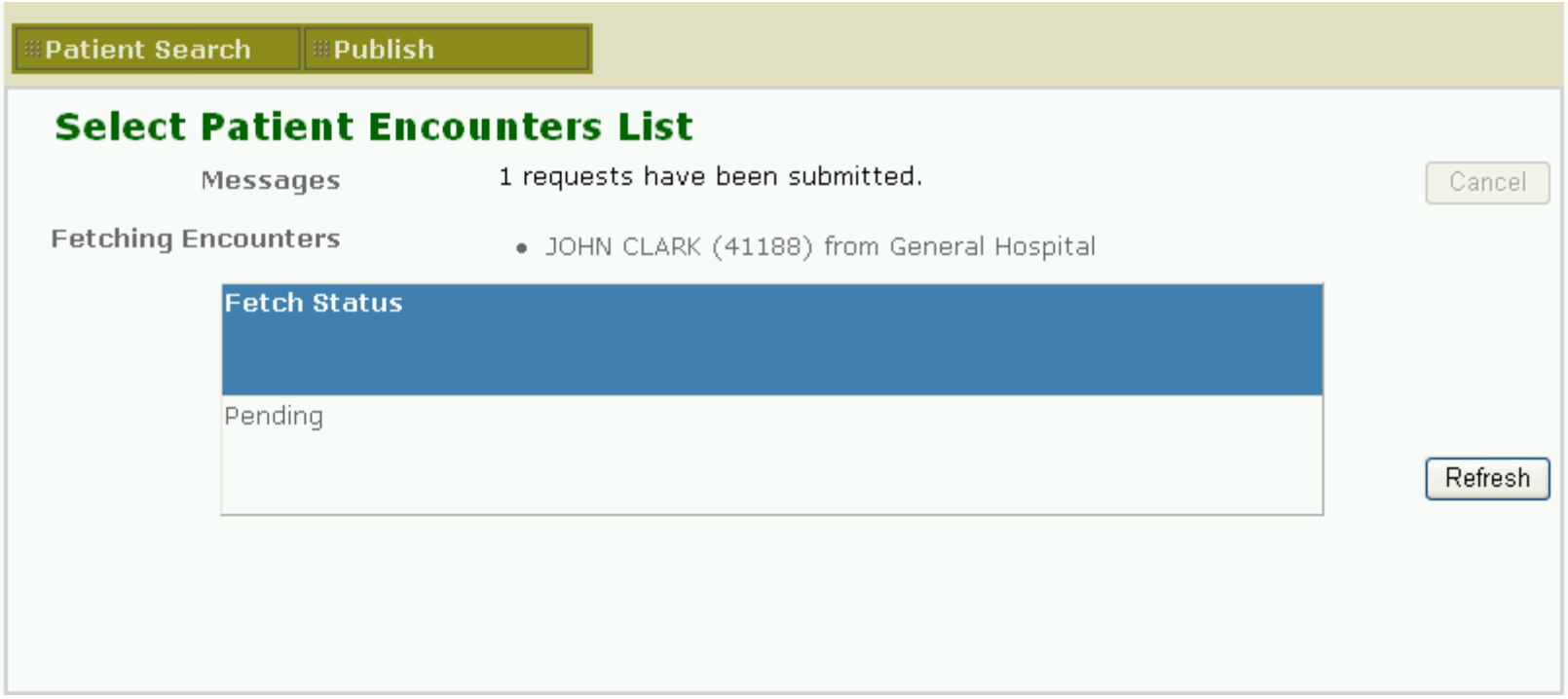
5 record(s) found. Elapsed Time: 2.35 seconds.

Select	Gateway Location	MRN	Name	Gender	Birthdate	Zipcode	Score
☐	General Hospital	41188	JOHN CLARK	M	1/4/1927	02139	6.2
☐	General Hospital	406611	JOHN CLARK	M	1/1/1906	02128	1.7
☐	General Hospital	24913	JOHN CLARK	M	12/4/1992	02126	1.7
☐	General Hospital	196314	JOHN CLARK	M	1/30/1938		1.2
☐	General Hospital	433763	JENNY CLARK	F		02124	1.1

Get Summary Records

Threshold set low

Fetching Patient Encounters - pending



Fetching Patient Encounters - found

Patient Search | Publish

Select Patient Encounters List

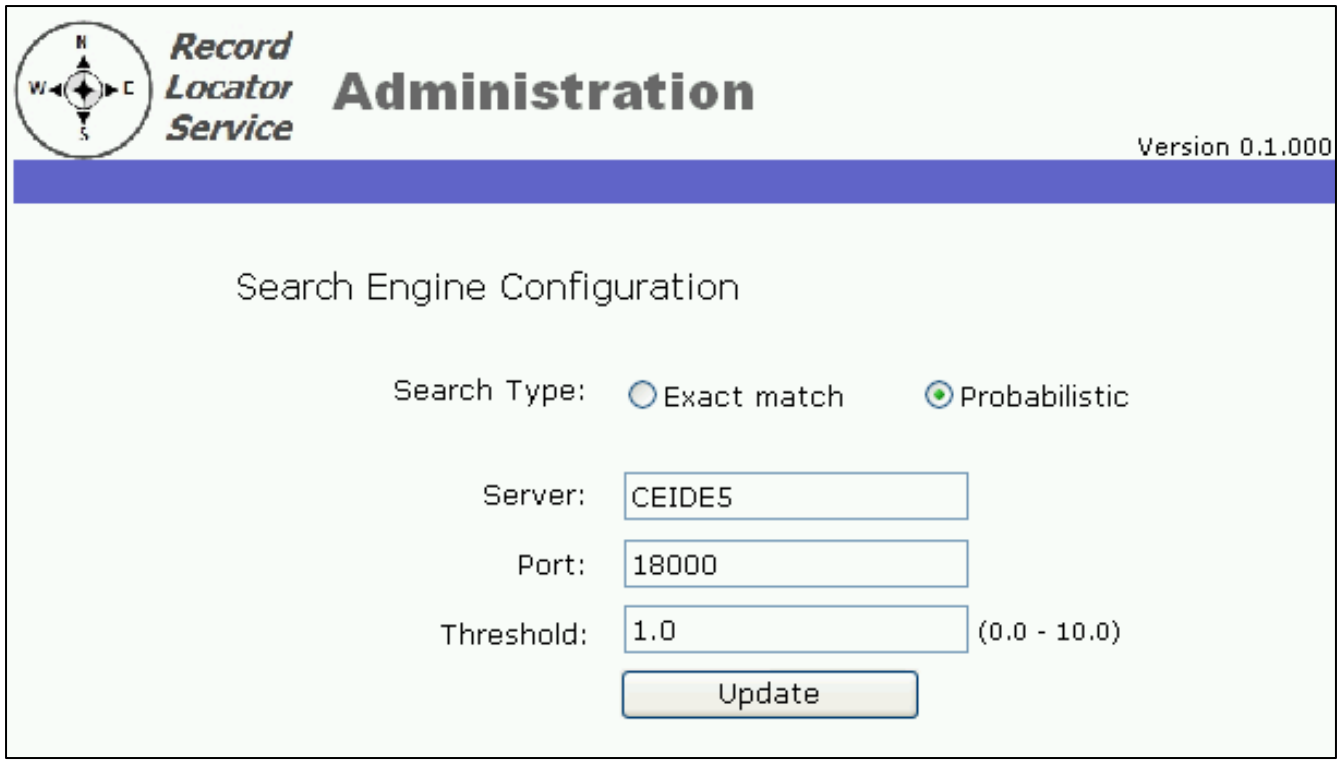
Messages 37 encounters were found.

Fetching Encounters

- BOY BOYKINS (294474) from General Hospital

Select	Act Id	Act Type	Act Date	Fetch Status
☐	246251	SPECIMENS	5/5/2000	Completed
☐	178940	SPECIMENS		Completed
☐	237690	SPECIMENS		Completed
☐	246250	SPECIMENS	5/5/2000	Completed
☐	170796	SPECIMENS		Completed
☐	178938	SPECIMENS		Completed
☐	178939	SPECIMENS		Completed
☐	151066	SPECIMENS		Completed
☐	2339698	ORDER	3/31/2005	Completed
☐	2339699	ORDER	3/31/2005	Completed
☐	48192	OR_CASE	3/15/2001	Completed
☐	2339695	ORDER	3/31/2005	Completed
☐	2339696	ORDER	3/31/2005	Completed
☐	2339697	ORDER	3/31/2005	Completed
☐	2339692	ORDER	3/31/2005	Completed
☐	2339693	ORDER	3/31/2005	Completed
☐	2339694	ORDER	3/31/2005	Completed

Screen Flow – Configure Search Engine
ADMIN Site



Screen Flow – Publish Add

Patient Search | Publish

- New Patient
- Edit Exisiting
- Delete

Publish Add

Required Data:

MRN 999888777 — Medical record number for patient

URI cdxgw.chicagohope.org — Web address of institution where record is stored. (exludes Web Service name, but include path: e.g. https://medical.institution.org/public)

Name Michael (First) Clark (Last)

Gender ◉ Male ○ Female

DOB 1 / 6 / 1958 — Date Of Birth

mm / dd / yyyy

ZIP Code 02125 — Five digit ZIP

Add | Cancel

Enter data to Add.

Deliberate typing error
Transposed mm /dd

Screen Flow – Search found newly added record

Patient Search | Publish

Patient Identification

Required Data:

Name: Michael (First) Clark (Last)

Gender: Male Female

DOB: 6 / 1 / 1958 (mm / dd / yyyy)

ZIP Code: 02125

Search Cancel

...search complete.

7 record(s) found. Elapsed Time: 4.58 seconds.

Select	URI	MRN	Name	Gender	Birthdate	Zipcode	Score
☐	www.csc.com	21	MICHAEL CLARK	M	6/1/1958	02125	8.9
☐	cdxgw.chicagohope.org	999888777	Michael Clark	M	1/6/1958	02125	5.6
☐	www.csc.com	491482	MICHAEL CLARK	M	6/21/1945		4.5
☐	www.csc.com	250153	MICHAEL CLARK	M	9/1/1941	02131	1.8
☐	www.csc.com	291590	MICHAEL CLARK	M	8/5/1965	02126	1.8
☐	www.csc.com	253112	MICHAEL CLARK	M	2/20/1931	02131	1.8
☐	www.csc.com	195926	JEFFREY CLARK	M	5/22/1958	02125	1.7

Newly added record

Patient Linking / Matching Component

- Prototype includes two “swappable” components (configurable via Admin screen or XML config file)
  - **Exact match** (custom built)
    - Compares demographics entered to fields in CMPI table
    - All fields must match exactly.
      - First Name
      - Last Name
      - DOB
      - Gender
      - Zip
  - **Probabilistic match** (using Initiate Systems Identity Hub)
    - NYSIIS soundex (“whyte” and “white”)
    - Allows transpositions (01234 and 01243)
    - Scores based on weighted closeness to original data
    - If total score above a threshold – patient data is returned
    - Threshold is configurable (central admin config file)

Initiate Search Engine – Scoring / Setting Thresholds

Comparison Scoring		*part of Initiate's Identity Hub Software*			www.initiatesystems.com	
		This example from their literature				
Rec#	**Name**	**Address**	**Phone**	**DOB**	**SSN**	**Example Score**
101	**John Q Public**	**1043 W. Easy St, Phoenix, AZ.85535**	**5556060**	**10-24-1950**	**482891822**	**20.0**
102	**Jon Public**	**1043 W. Easy St, Phoenix, AZ.85535**	**5556060**	**10-24-1950**	**482891822**	18.0
103	J **Public**		5553232	**10**-25-**1950**	**482891822**	11.0
104	John Q Long	552 Green Dr, **Phoenix, AZ**.85535		11-15-1962	57265225	5.0
105	Danny Smith		5552745	**10-24-1950**	48289244	5.0
106	Kevin Dohert	1028 **W. Easy** Ave, **Phoenix, AZ** .85535	5554289		48224857	4.0

- Matching threshold is set by RLS implementing organization (e.g. RHIO)
  - Threshold is an installation time parameter, based on security policies re: “false positives” and human disambiguation.
  - Architecture does not preclude specific matching requirements

Discussion

- Questions / follow-up
  - jhalamka@caregroup.harvard.edu