Linking Patient Records
John D. Halamka MD
• 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 \[\text{Not RLS function}\]
- 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
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

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

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

Supporting processes are required for:
- Security administration
- Registration and identity management
- 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
   a. senderside certificate used to sign message and receiver certificate used to establish SSL/TLS connection
   b. access logged
3. Matching patient record locations looked up
   a. remote system authenticated against registry
   b. access logged
4. Matching records from CMPI returned
   a. senderside 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
   a. remote system authenticated against registry
   b. access logged
8. Patient clinical records retrieved
9. Clinical records returned to user
   a. senderside 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

<table>
<thead>
<tr>
<th>Service Layer</th>
<th>Prototype Platform</th>
<th>Alternatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Services</td>
<td>ASP.NET</td>
<td>JSP, PHP</td>
</tr>
<tr>
<td>Business Application Services</td>
<td>.NET components</td>
<td>Java Servlets, EJB Session Beans, PHP / Python / Perl</td>
</tr>
<tr>
<td>Data Management Services</td>
<td>ADO.NET using .NET framework services</td>
<td>EJB Entity Beans, PHP / Python / Perl</td>
</tr>
<tr>
<td>Data Storage Services</td>
<td>Microsoft SQL Server 2000</td>
<td>Oracle / DB2, MySQL / PostgreSQL</td>
</tr>
<tr>
<td>Integration Broker Services</td>
<td>Microsoft BizTalk Server 2004</td>
<td>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)</td>
</tr>
<tr>
<td>Custom components built on BizTalk framework</td>
<td></td>
<td>Packaged adaptors from Integration broker vendors</td>
</tr>
<tr>
<td>Custom .NET components using .NET framework</td>
<td></td>
<td>IBM WebSphere MQ</td>
</tr>
<tr>
<td>Systems Management Services</td>
<td>Custom .NET components using .NET framework</td>
<td>CA Unicenter, IBM Tivoli, Microsoft Management Services</td>
</tr>
<tr>
<td>Security Services</td>
<td>Custom .NET components using simple database table for user identities / credentials</td>
<td>Novell Odyssey, Sun ONE, CA eTrust</td>
</tr>
</tbody>
</table>
Screen Flow

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

Forget 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
Required Fields when empty marked *
Screen Flow

Record Locator Service - DEMO

Patient Identification

Required Data:

Name
- John
- Clark

First

Last

Gender
- Male
- Female

DOB
- 4
- 1
- 1927

ZIP Code
- 02139

Enter data to search.
Screen Flow – Exact Match

**Patient Identification**

**Required Data:**

- **Name:** John Clark
- **Gender:** Male
- **DOB:** 1/4/1927
- **ZIP Code:** 02139

...search complete.

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

<table>
<thead>
<tr>
<th>Select</th>
<th>Gateway Location</th>
<th>MRN</th>
<th>Name</th>
<th>Gender</th>
<th>Birthdate</th>
<th>Zipcode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General Hospital</td>
<td>41188</td>
<td>JOHN CLARK</td>
<td>M</td>
<td>1/4/1927</td>
<td>02139</td>
</tr>
</tbody>
</table>

Get Summary Records
Screen Flow – Probabilistic Match with Score

**Patient Identification**

Required Data:

- **Name**: John Clark
- **Gender**: Male
- **DOB**: 4/1/1927
- **ZIP Code**: 02139

...search complete.

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

<table>
<thead>
<tr>
<th>Select</th>
<th>Gateway Location</th>
<th>MRN</th>
<th>Name</th>
<th>Gender</th>
<th>Birthdate</th>
<th>Zipcode</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General Hospital</td>
<td>41188</td>
<td>JOHN CLARK</td>
<td>M</td>
<td>1/4/1927</td>
<td>02139</td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td>General Hospital</td>
<td>40661</td>
<td>JOHN CLARK</td>
<td>M</td>
<td>1/1/1906</td>
<td>02126</td>
<td>1.7</td>
</tr>
<tr>
<td></td>
<td>General Hospital</td>
<td>24913</td>
<td>JOHN CLARK</td>
<td>M</td>
<td>12/4/1992</td>
<td>02126</td>
<td>1.7</td>
</tr>
<tr>
<td></td>
<td>General Hospital</td>
<td>19631</td>
<td>JOHN CLARK</td>
<td>M</td>
<td>1/30/1938</td>
<td></td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>General Hospital</td>
<td>43376</td>
<td>JENNY CLARK</td>
<td>F</td>
<td></td>
<td>02124</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Get Summary Records

Threshold set low
Fetching Patient Encounters - pending

Select Patient Encounters List

Messages

1 requests have been submitted.

• JOHN CLARK (41188) from General Hospital

Fetch Status

Pending

[Refresh]
Select Patient Encounters List

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

Messages
37 encounters were found.

Fetching Encounters
- BOY BOYKINS (294474) from General Hospital
Screen Flow – Configure Search Engine
ADMIN Site

Search Engine Configuration

Search Type:  
- Exact match
- Probabilistic

Server: CEIDE5
Port: 18000
Threshold: 1.0 (0.0 - 10.0)

Update
Screen Flow – Publish Add

**Publish Add**

Required Data:

- **MRN**: 999888777
- **URI**: cdxgw.chicagohope.org
- **Name**: Michael
- **Gender**: Male
- **DOB**: 1 / 6 / 1958
- **ZIP Code**: 02125

Medical record number for patient
Web address of institution where record is stored. (excludes Web Service name, but include path; e.g. https://medical.institution.org/public)
Name
Gender
DOB
ZIP Code

Enter data to Add.
Screen Flow – Search found newly added record

Patient Identification

Required Data:

Name: Michael Clark
Gender: Male
DOB: 6/1/1958
ZIP Code: 02125

Search complete.

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

<table>
<thead>
<tr>
<th>Select</th>
<th>URI</th>
<th>MRN</th>
<th>Name</th>
<th>Gender</th>
<th>Birthdate</th>
<th>Zipcode</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>21</td>
<td>MICHAEL CLARK</td>
<td>M</td>
<td>6/1/1958</td>
<td>02125</td>
<td>8.9</td>
</tr>
<tr>
<td>☐</td>
<td>cdxgw.chicagohope.org</td>
<td>999988777</td>
<td>Michael Clark</td>
<td>M</td>
<td>1/5/1958</td>
<td>02125</td>
<td>5.6</td>
</tr>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>491482</td>
<td>MICHAEL CLARK</td>
<td>M</td>
<td>6/21/1945</td>
<td></td>
<td>4.5</td>
</tr>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>250153</td>
<td>MICHAEL CLARK</td>
<td>M</td>
<td>9/1/1941</td>
<td>02131</td>
<td>1.8</td>
</tr>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>291590</td>
<td>MICHAEL CLARK</td>
<td>M</td>
<td>8/5/1965</td>
<td>02126</td>
<td>1.8</td>
</tr>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>253112</td>
<td>MICHAEL CLARK</td>
<td>M</td>
<td>2/20/1931</td>
<td>02131</td>
<td>1.8</td>
</tr>
<tr>
<td>☐</td>
<td><a href="http://www.csc.com">www.csc.com</a></td>
<td>195926</td>
<td>JEFFREY CLARK</td>
<td>M</td>
<td>5/22/1958</td>
<td>02125</td>
<td>1.7</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Rec#</th>
<th>Name</th>
<th>Address</th>
<th>Phone</th>
<th>DOB</th>
<th>SSN</th>
<th>Example Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>John Q Public</td>
<td>1043 W. Easy St, Phoenix, AZ.85535</td>
<td>5556060</td>
<td>10-24-1950</td>
<td>482891822</td>
<td>20.0</td>
</tr>
<tr>
<td>102</td>
<td>Jon Public</td>
<td>1043 W. Easy St, Phoenix, AZ.85535</td>
<td>5556060</td>
<td>10-24-1950</td>
<td>482891822</td>
<td>18.0</td>
</tr>
<tr>
<td>103</td>
<td>J Public</td>
<td>1043 W. Easy St, Phoenix, AZ.85535</td>
<td>5553232</td>
<td>10-25-1950</td>
<td>482891822</td>
<td>11.0</td>
</tr>
<tr>
<td>104</td>
<td>John Q Long</td>
<td>552 Green Dr, Phoenix, AZ.85535</td>
<td>5552745</td>
<td>10-24-1950</td>
<td>48289244</td>
<td>5.0</td>
</tr>
<tr>
<td>105</td>
<td>Danny Smith</td>
<td>1028 W. Easy Ave, Phoenix, AZ.85535</td>
<td>5552489</td>
<td>10-24-1950</td>
<td>48289428</td>
<td>5.0</td>
</tr>
</tbody>
</table>

• 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