A Connecting for Health RLS Prototype in Mendocino County, California[1]

22 May 2006

Mendocino Health Records Exchange

Mendocino County[2] is a mountainous region on the Pacific Coast of California. Located 100 miles north of San Francisco, this sparsely populated county covers 3,500 square miles. Like a lot of rural America, small towns in Mendocino County are separated by long distances and by limited access to high speed Internet service. Local ambulatory patient care occurs in solo practitioner offices, at community clinics or in the emergency rooms of three small rural hospitals. With no integrated delivery networks, and no tertiary care trauma centers, health care in Mendocino County lacks the capital resources and enterprise information technology of large scale urban medicine. Like most other rural counties in America, health care in Mendocino County operates with a minimally capable information technology infrastructure.

MendocinoHRE[3] ("Health Records Exchange") is a community-based effort to enable the deployment of interoperable electronic health records in Mendocino while operating within the constraints of a typical rural county. Mendocino HRE has developed in a gradual process.

(1) In 2003 Mendocino SHARE[4] was formed as a collaboration among safety net health care sites to demonstrate a health information exchange. In April 2004 Mendocino SHARE hired Browsersoft, Inc.[5], a Kansas City software developer, to build an open source toolkit for the health information exchange. In August 2004 the software was released as OpenHRE[6] ("Open Health Records Exchange"). In 2005 Mendocino SHARE decided to transition the health information exchange to a successor entity.

(2) In 2005 Redwood MedNet[7] was formed as a new non profit by local physicians and technologists to develop health information technology solutions for the local health care community. Redwood MedNet proposed Mendociono HRE as a successor to the Mendocino SHARE project. In 2005 Redwood MedNet also began development of a clinical messaging infrastructure, planned for deployment in the fourth quarter of 2006.

---

[1] This project was generously supported by the Markle Foundation, the Robert Wood Johnson Foundation, and the Tides Foundation. This document may be freely redistributed based on the license terms on page 11.

[2] http://www.co.mendocino.ca.us/

[3] http://www.mendocinohre.org

[4] http://www.ruralcommunityhealth.org/projects/msp.html

[5] http://www.browsersoft.com/

[6] http://www.openhre.org/

[7] http://www.redwoodmednet.org/

(3) Also in 2005, Mendocino HRE, with technology partner Browsersoft, worked together on the Connecting for Health RLS Prototype[8] to demonstrate how small communities with minimal access to technology can securely exchange electronic health records with sophisticated health information exchange networks such as Indiana and Massachusetts.

Connecting for Health

Connecting for Health[9] is a public-private collaborative made up of leaders and innovators from more than 100 organizations representing a diverse array of private, public and not-for-profit groups. The members of Connecting for Health believe that the private, secure and nationwide exchange of health information is essential to the well-being of patients and those who care for them; that health information technology must be designed at the outset to achieve privacy and security goals; and that policy objectives should determine technology solutions, not the other way around. The Connecting for Health Common Framework (see Table 1) provides integrated guidelines which weave together a set of technical specifications, recommendations on key policy issues to protect patient privacy, and a model contract template.

The Common Framework: Overview and Principles	
Policy Guides: How Information is Protected	Technical Guides: How Information is Exchanged
[P1] The Architecture for Privacy in a Networked Health Information Environment	**[T1]** The Common Framework: Technical Issues and Requirements for Implementation
[P2] Model Privacy Policies and Procedures for Heath Information Exchange	**[T2]** Health Information Exchange: Architecture Implementation Guide
[P3] Notification and Consent When Using a Record Locator Service	**[T3]** Medication History Standards
[P4] Correctly Matching Patients with Their Records	**[T4]** Laboratory Results Standards
[P5] Authentication of System Users	**[T5]** Background Issues on Data Quality
[P6] Patients' Access to Their Own Health Information	**[T6]** Record Locator Service: Technical Background from the Massachusetts Prototype Community
[P7] Auditing Access to and Use of a Health Information Exchange	
[P8] Breaches of Confidential Health Information	
Model Contractual Language	
[M1] Key Topics in a Model Contract for Health Information Exchange	**[M2]** A Model Contract for Health Information Exchange

Table 1 -- The Connecting for Health Common Framework, released in April 2006

[8] http://www.connectingforhealth.org/news/pressrelease_060105.html

[9] See http://www.connectingforhealth.org to download the entire Connecting for Health Common Framework.

The technical and policy guidance of the Connecting for Health Common Framework functions as an integrated and comprehensive architecture for privacy and security.

- Policy and legal agreements are established between all parties to each health record transaction, including patients and clinical and administrative staff at each health care facility
- Technical recommendations are carefully crafted to respect and protect privacy and security
- Policy agreements and technology solutions apply to any participant responsible for user administration, system security, operating uptime, data redundancy, circuit provisioning and transport services at each stage in the record exchange process

The technical and policy architecture constructed by the Common Framework is inexpensive, loosely coupled, flexible, creates immediate value, and reinforces current institutional authority for health records accuracy, trust and security. In short, it provides current care delivery organizations (CDO) with clear and simple steps to develop an environment for secure sharing of health information.

The Connecting for Health Common Framework is based on non-proprietary technical and policy standards that work with information systems already in place, regardless of local variations in hardware and software. The Common Framework encourages the adoption of standards, and leaves it to local implementers to adapt their solutions to the standards. By leveraging standards, the Connecting for Health Common Framework enables health records to interoperate between any two care delivery organization via the networking standard. This incremental approach allows immediate progress towards interoperable electronic health records, and provides a decentralized architecture for record exchange. Decisions on the sharing of health information remain with patients and their health care providers. Records are stored locally and can be shared electronically if authorized. The Connecting for Health Common Framework respects the autonomy of current institutions, involves them in data accuracy and trust relationships, and does not require the creation of a new central bureaucracy.

Record Locator Service

The technical architecture identified by the Connecting for Health Common Framework can be illustrated in a single prototype transaction: an authorized user at Clinic B queries a Record Locator Service (RLS) first to discover a record location, and second uses that location to retrieve the record from Clinic A. (See Figure 1) This two stage process (i.e., first discover the location of the record, then retrieve the record) has profound architectural implications, requiring shared standards for identity disambiguation, for data and message format, for user authentication, for secure access, and for transport protocols.

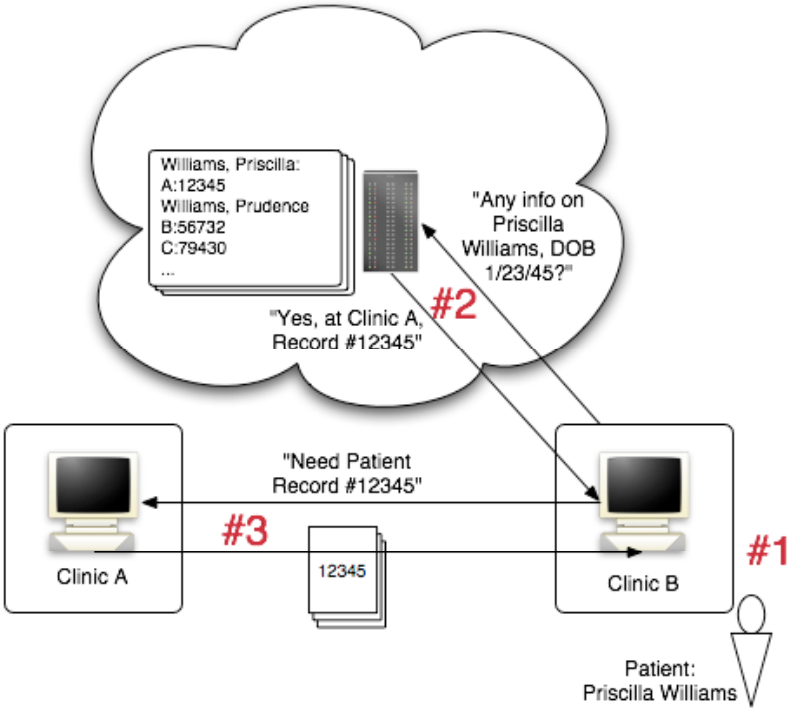

Figure 1 -- Two stage retrieval of remote patient health record (Courtesy of Connecting for Health, 2005)

The RLS knows about the location of patient records, but does not contain clinical details beyond patient demographic and the record location details. The lack of clinical data in the RLS is an explicit security and privacy feature of the Connecting for Health Common Framework. The RLS functions as a Master Patient Index (MPI) constrained by the strict policies of the Common Framework to protect privacy and security.

RLS Prototype Demonstration

In June 2005 the Connecting for Health Technical Workgoup launched a project to build a prototype of the RLS operating across separate communities nationwide. Three sites participated in the Connecting for Health RLS Prototype:

(1) Boston, Massachusetts (MA-SHARE[10])

(2) Indianapolis, Indiana (IHIE[11])

(3) Mendocino County, California (Mendocino HRE)

[10] http://www.mahealthdata.org/ma-share/

[11] http://www.ihie.org/

The technology design principles of the Connecting for Health Common Framework did not require a single specific software application for a nationwide RLS. Instead, each participating community built a solution based on the local health information technology infrastructure. The Boston software solution was built on Microsoft Windows servers running .NET, while Indiana and Mendocino each developed separate software solutions in Java running on Linux servers. The Mendocino HRE solution was built with open source software.

Inter SNO Bridge

Each of the three participating communities in the RLS prototype is what Connecting for Health calls a Sub Network Organization[12] (SNO). To enable a two stage query and exchange process between SNOs, the Connecting for Health RLS prototype created an Inter SNO Bridge (ISB). The ISB was exposed as a secure service pairwise between SNOs. (See Figure 2) The ISB is a web service that acts as an enterprise application, taking queries and returning locations

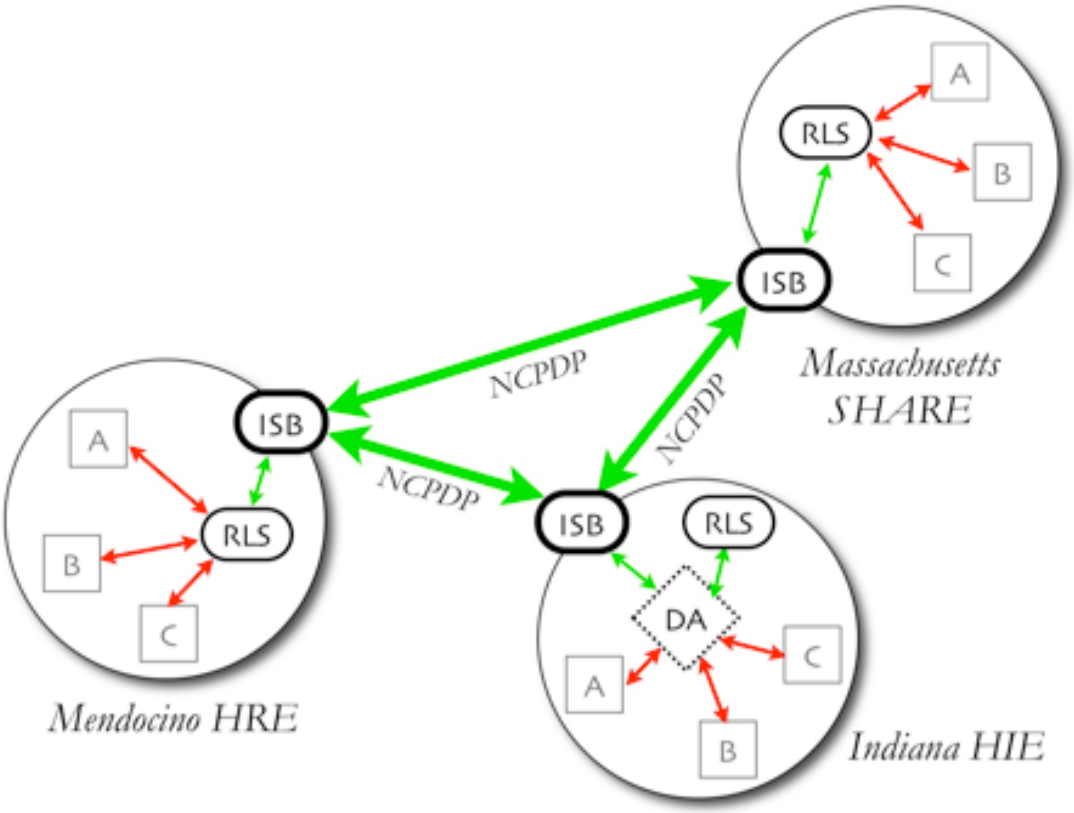

Figure 2 -- Inter SNO Bridge (Courtesy of Mendocino Informatics, 2005)

[12] SNO and RHIO ("Regional Health Information Organization") are equivalent terms for a health information exchange service that participates directly in the Nationwide Health Information Network (NHIN). Connecting for Health eliminates "Region" so that the term "SNO" becomes inclusive enough to recognize networks which extend beyond the boundary of a single region (e.g., pharmacy or hospital chains, the Veterans Health Administration, state Public Health Departments, the CDC, national disease registries, etc.)

of patient records. The web service can optionally aggregate returned records from multiple locations, and assemble a longitudinal presentation.

As the sole gateway in or out of the SNO, the ISB maintains an audit log of all transactions and provides a defensible security perimeter for protected health information crossing boundaries between SNOs. In the absence of a nationwide top level domain, pairwise trust relationships are negotiated between SNOs to enable the secure exchange of health information across the ISB. Developing the ISB is a necessary next step in the evolution of a scalable architecture for the Nationwide Health Information Network (NHIN).

The Mendocino demonstration of the two stage process, with the RLS discovering records to be retrieved across an ISB, was built with the OpenHRE software suite. OpenHRE performs the exchange by transforming local patient record content into common standards, by transporting the data with standard Internet protocols, and by using secure electronic sessions between known clinical partners with clear chain of trust relationships. The OpenHRE solution demonstrates how a rural region such as Mendocino, with a minimal technical infrastructure, can build and operate a fully functional health information exchange that conforms to the policy and technical guidelines of the Connecting for Health Common Framework.

OpenHRE

The OpenHRE software toolkit provides a standards-based, scalable, multi-level record locator service (RLS), with a federated records exchange service (RES) and secure access controls. (See Figure 3) OpenHRE is open source[13] software that conforms to the technical and policy guidelines of the Connecting for Health Common Framework. This is a modern, modular architecture in active development by Browsersoft, Inc. under contract with the Office of the National Coordinator[14] (ONC) as part of the Nationwide Health Information Network[15] (NHIN) prototype development work.

The OpenHRE system architecture utilizes three services:

(1) Record Locator Service (RLS)

(2) Record Exchange Service (RES)

(3) Authentication and Access Control Service (AACS)

As a software application suite assembled from open source components, OpenHRE provides configurable patient matching, secure caching, message transformation, security and integration services for a community or enterprise health records exchange infrastructure.

---

[13] http://www.opensource.org

[14] http://www.os.dhhs.gov/healthit/

[15] Browsersoft is a subcontractor of the Computer Sciences Corp. NHIN prototype contract with ONC.

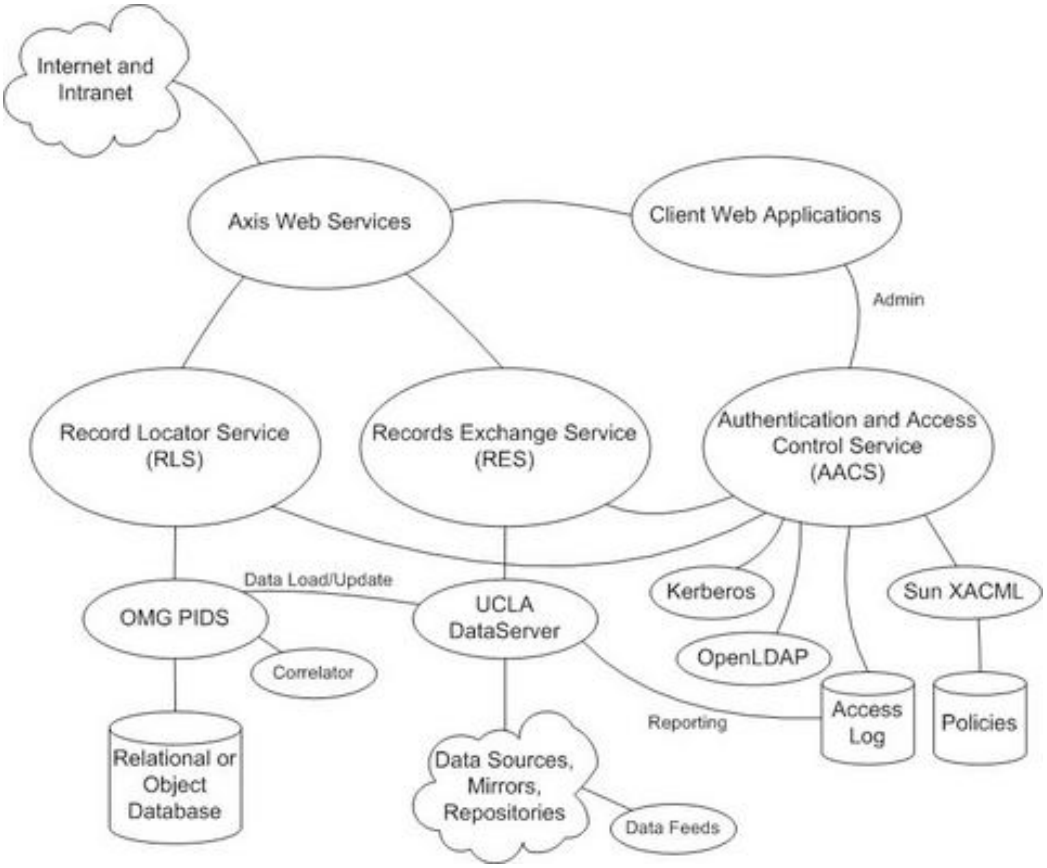

Figure 3 -- OpenHRE Architecture (Courtesy of Browsersoft, Inc., 2006)

Indexing Patient Records

OpenHRE uses a Patient ID Server[16] (PIDS) to build an index of patient demographic and record location details. Each individual health record contains a local Medical Record Number (MRN), patient identity demographic fields (e.g., name, date of birth, etc.) and appropriate clinical record location details, but not the actual clinical data. Data streams are set up for both the initial PIDS data load and for incremental updates to the PIDS. Any relational or object database can host the PIDS data. The PIDS repository maintains a complete historical record of all data changes.

[16] As specified by the Object Management Group

Matching Patient Records

OpenHRE can be configured to match patient data from one or more PIDS repositories. A combination of pre-processing steps and on-the-fly analysis can produce a match from PIDS data. The service can produce positive matches even with irregularities in the source data. The following tools enable an OpenHRE implementation to be tuned to the variable demographic characteristics of local populations.

Data Cleaning

Standardization

Transformation

Comparison

Probabilistic Weighting

Deterministic Algorithms

Blocking

Results Classification

Detailed instructions for each of these features are provided in the OpenHRE implementation guide.[17]

Hierarchy of Identity

OpenHRE can utilize a hierarchy of PIDS or other patient index repositories to correlate patient health records. (See Figure 4) PIDS repositories can work on one or multiple levels. Each PIDS repository can roll up to a next level to create an index containing the contents of all subsidiary PIDS records. PIDS repositories can index a single enterprise with multiple patient data silos (e.g., using Medical Record Number to link patient data in separate radiology and

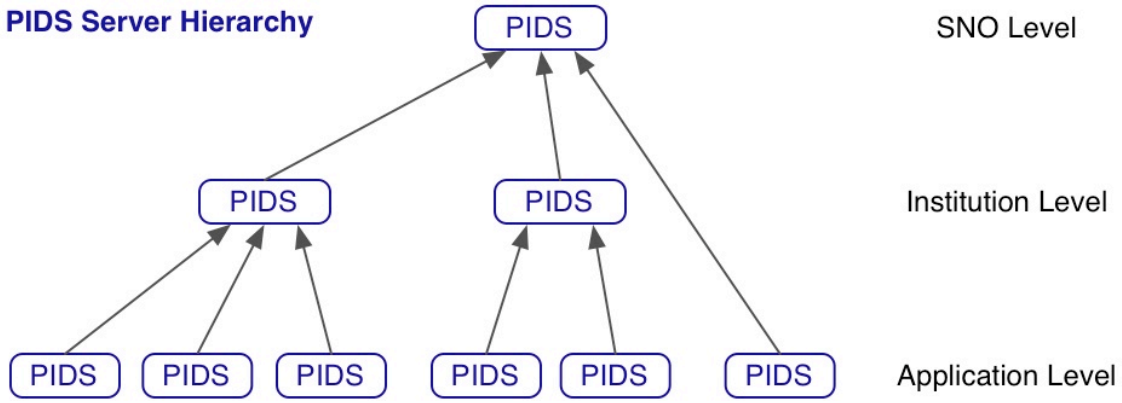

Figure 4 -- PIDS Hierarchy (Courtesy of Browsersoft, Inc., 2005)

[17] http://www.openhre.org

pharmacy applications at the same institution). PIDS repositories can also roll up to a next level to create a community MPI (e.g., from site level MRN at one ambulatory clinic to an Enterprise Record Number across multiple clinics at the level of a SNO).

Federated RLS Queries

In the event that a single top level MPI is not desired, OpenHRE can perform a top level query across a federation of PIDS nodes before correlating the results to determine matches. This approach deploys OpenHRE as a loosely coupled discovery based federated cluster which functions as a just in time record locator service.[18] This implementation allows a SNO to protect an entire downstream PIDS repository while accepting targeted searches by authorized users. As a security precaution, a SNO may expose external ISB queries only to a federation of PIDS nodes, and allow only internal SNO queries to access the local PIDS.

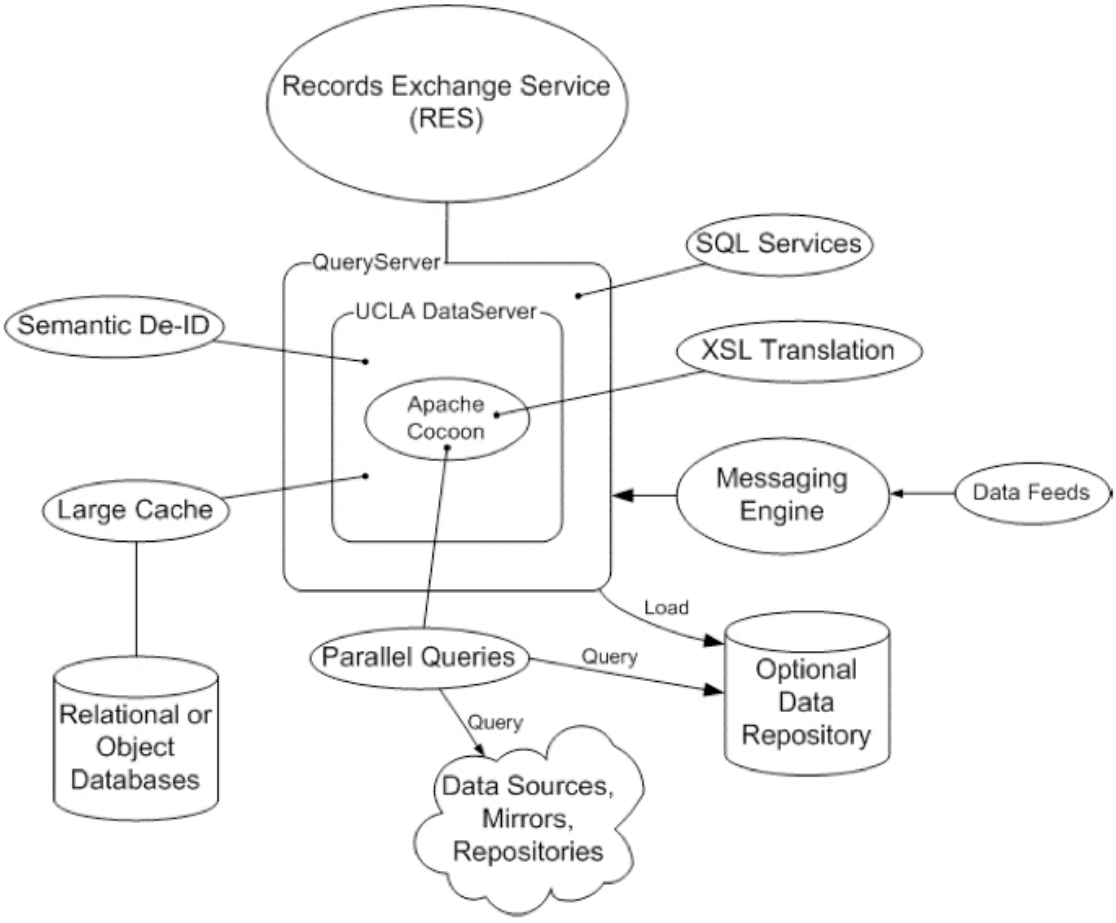

Figure 5 -- Record Exchange Service, or "RES". (Courtesy of Browsersoft, Inc., 2005)

[18] OpenHRE can also be deployed in a centralized topology, with strict and persistent identity linking across the enterprise.

Record Exchange Service (RES)

The RES (See Figure 5) allows a user to request and retrieve a patient health record whose location has been disclosed during an authorized RLS query. The RES supports numerous storage and retrieval topologies, from central repositories to federated access of distributed record systems. The RES can retrieve a single record or a multiple records. The RES also performs transformations of retrieved data into presentation formats conducive to clinical analysis.

The RES for OpenHRE is built on Apache Cocoon[19], an open source message processing system with advanced facilities for parallel data queries and complex transformations. OpenHRE uses the UCLA DataServer implementation of Cocoon. DataServer, developed and maintained by UCLA Medical Imaging Informatics, adds to Cocoon the ability to handle very large data caches, potentially extending across multiple relational or object databases. DataServer also contains algorithms which enable a semantic analyzer to locate and de-identify protected health information (e.g., patient name in text or graphic file).

In addition to the native features of the UCLA DataServer and the Cocoon environment, two additional features have been added by Browsersoft.

- Configuration-based SQL services to allow the RES to originate complex pull-based queries, or to drive additional push based reporting functionality
- A JMS compliant messaging engine which consumes a wide range of transport formats (e.g., FTP, SSL, WS, etc.)

The RES toolkit environment provided by OpenHRE is basically pass-through middleware for processing clinical health information, with a robust caching capability for large amounts of session data. One or more back end systems can be queried and results formatted into XML or HTML using Apache Cocoon, an XSL translation pipeline system. Optionally, if data persistence is desired by the participants, then the RES can feed an XML based repository to expedite future queries.

Authentication and Access Control Service (AACS)

Patient centric security policies require more than Role Based Access Control. OpenHRE provides an extensive authentication and access control service to implement complex security policies.[20] Data specific to OpenHRE users is stored on an LDAP server protected by Kerberos. The Sun XACML access control engine automates execution of complex security policies, including policies sensitive to data content. OpenHRE includes a Security Administration web application with a GUI to edit user attributes and configure XACML policies to match local .

[19] http://cocoon.apache.org/

[20] The production implementation of OpenHRE in Mendocino implements three factor authentication security.

Summary

The OpenHRE software toolkit, envisioned by Mendocino SHARE, developed by Browsersoft and demonstrated by Mendocino HRE, is standards based, robust, secure and adaptable. As further OpenHRE implementations are brought on line, stress testing will lead to optimization opportunities for the code base. OpenHRE is a comprehensive and affordable open source technology solution within reach of any SNO, no matter how small or thinly capitalized. Access to an affordable public domain solution such as OpenHRE democratizes the deployment of interoperable health record solutions, removing one major technical obstacle to community adoption. OpenHRE provides small and rural communities with a ready and adaptable technology option. The only missing ingredient is community wide policy alignment to facilitate stakeholder collaboration. For this, the Connecting for Health Common Framework is a perfect roadmap to follow, even in a community with a minimally capable technology infrastructure.

For Further Information

Mendocino Health Records Exchange -- http://www.mendocinohre.org/

Connecting for Health -- http://www.connectingforhealth.org

OpenHRE -- http://www.openhre.org

- - - - - - - -

Glossary

AACS -- Authorization and Access Control Service

CDO -- Care Delivery Organization. Any local site providing health care.

Connecting for Health -- A public-private collaborative jointly funded by the Markle Foundation and the Robert Wood Johnson Foundation

ERN -- Enterprise Record Number

GUI -- Graphical User Interface

ISB -- Inter SNO Bridge

Mendocino SHARE -- A collaboration among 13 safety net organizations in Mendocino County, begun in 2003, ended in 2006

Mendocino HRE -- A community health records exchange project initiated in 2005 in part as a successor entity to Mendocino SHARE. Mendocino HRE is sponsored by Redwood MedNet.

MPI -- Master Person (or Patient) Index

MRN -- Medical Record Number

NHIN -- Nationwide Health Information Network

ONC -- Office of the National Coordinator for Health Information Technology, part of the U.S. Department of Health and Human Services

Open HRE -- Open Health Records Exchange, an open source software suite which conforms to the Connecting for Health Common Framework

PIDS -- Person Identity Service

Redwood MedNet -- A community-based 501(c)(3) non-profit in Mendocino County formed to help interconnect all health care providers in Lake and Mendocino Counties, California

RHIO -- Regional Health Information Organization

RES -- Record Exchange Service

RLS -- Record Locator Service

SNO -- Sub Network Organization