Participation in a prototype federated system for sharing medical content

Paul R Dexter, MD¹, Lonnie Blevins¹, Clement McDonald, MD², Marc Overhage, MD¹
¹Regenstrief Institute, Indianapolis, IN; ²Lister Hill National Center for Biomedical Communications, Bethesda, MD

Abstract

As part of the Markle Foundation’s Connecting For Health (CFH) Reference Implementation Project, Regenstrief Institute participated in the design, creation, and public distribution of server and client code that allows for the secure electronic exchange of protected health information between disparate computer systems.

We describe implementation at Regenstrief Institute of CFH’s architecture for communication of protected health information between community sub-network organizations (SNOs) on a Nationwide Health Information Network (NHIN). Built on CFH’s Common Framework, we implemented a Record Locator Service (RLS) to locate patient records, as well as an Inter-SNO Bridge (ISB) within the Indiana Network for Patient Care (INPC).

An ISB server securely exchanged patient electronic medical data with remote ISBs, using Computer-to-Computer Messaging (“T2”) message structures. Underlying technologies included TCP/IP, SOAP, Web Services, HL7/NCPDP messaging standards, LOINC codes, NDC codes. Regenstrief successfully tested that exchange with colleagues in Mendocino County, California and in the Mass Share project in Massachusetts.

The initial portion of the ISB code was a “Record Locator Service” (RLS), based on our existing patient matching algorithms. That service finds all of the local patient registrations that it considers to be for the same patient, so that patients within our database can be “found” by remote system queries. The matching algorithm was repeatedly tested as part of our efforts. For the ISB, we developed a Disburser/Aggregator – disbursing the query to the relevant resources and aggregating the data before returning it.

Regenstrief also created a prototype INPC database with cleansed data from the production INPC server. We anonymized the patient demographic information by replacing it with patient demographics provided by the Mass Share group. We cleansed the medical reports by removing all free text and shifting the dates by a random amount of days per patient. We then reloaded some specific text reports that were reviewed by hand to insure that nothing confidential would be exposed, while still having textual reports in our prototype database.

We also created a client “viewer” application. The user enters patient identification data plus a query definition (what type of data, from when, etc.) into the viewer application. The viewer queries one or more ISBs to obtain all of the requested data and then displays that data to the user. This viewer responds within a couple of seconds for almost every query.

We subsequently created and implemented a web service for using these messages to print an patient “abstract” document with data merged from disparate computer systems, enhanced both the demonstration data and the demonstration viewer software for looking at patient data online, and continue to work on an NHIN standard interface for sending electronic data to a public health department.