Grant Final Report

Grant ID: UC1HS016152

Critical Access Hospital Partnership Health Information Technology Implementation

Inclusive Dates: 09/01/05 - 09/01/09

Principal Investigator:
Donald Wheeler, MHA, FACHE

Team Members:
Guy Hembroff, Professor and Chair, School of Technology, Michigan Technological University

Performing Organization:
Upper Peninsula Health Care Network
Marquette, Michigan

Project Officer:
Not provided

Submitted to:
The Agency for Healthcare Research and Quality (AHRQ)
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
www.ahrq.gov

Abstract

Purpose: The purpose of the project was to design and deploy secure healthcare information exchange system for Michigan's rural Upper Peninsula.

Scope: The scope of the project was to provide secure, authorized and synchronized exchange of patient records between the fourteen hospitals and one regional center that comprise the Upper Peninsula Health Care Network.

Methods: The project methods focused on the design of an HIE solution to meet existing Health Information Exchange standards, and include a security system/architecture that supports rich functionality, strong security, and easy interoperability and scaling across all users.

Results: The project successfully: (a) Developed a patient identification system to accurately identify patients and permit authorized physicians/staff access to patient records; (b) Established database interoperability of disparate systems by developing a system to map received data to each of the selected site's electronic medical record system; (c) Developed a medical documents exchange system between hospitals within the federated domain; and (d) Developed a federated security architecture for accessing, sharing, and transferring various types of medical data.

Key Words: rural health information exchange; electronic health records, master patient index, rural HIT implementation

The authors of this report are responsible for its content. Statements in the report should not be construed as endorsement by the Agency for Healthcare Research and Quality or the U.S. Department of Health and Human Services of a particular drug, device, test, treatment, or other clinical service.

Final Report

Purpose

The purpose of the project was to design and deploy secure Health Information Exchange (HIE) system to enable the communication of patient data between 10 critical access hospitals (CAHs) in Michigan's Upper Peninsula with physicians at Marquette General Hospital -- the region's only medical center. The network is designed to solve a major barrier to improving the quality care for residents of Michigan's Upper Peninsula, where a small population spread over a large geographical area makes access to advanced health care services difficult.
The HIE is designed to improve patient safety and efficiency by:

1. Reducing duplicate tests or other exams when patients are transferred from one provider to another;

2. Improving inpatient transfers between the critical access hospitals and Marquette General;

3. Allowing clinicians to identify which medications a patient is taking when he or she is transferred between emergency departments; and

4. Eliminating the need to send a courier service between hospitals to transport laboratory test results, medical records, x-rays, and other important patient data.

During the course of the 4-year implementation phase of the project, the scope of the project was expanded to include all hospitals involved in the Upper Peninsula Health Care Network (UPHCN), which includes fourteen hospitals and one regional center.

Scope

The rural region targeted by the project included the entire Upper Peninsula region of Michigan. This region contains almost one-third of the land area of Michigan but just three percent of its total population. It includes the only counties in the United States where a plurality of residents claim Finnish ancestry.

The population of the region is comprised of significant numbers of Finnish, Swedish, Norwegian, and Italian descendents, with a primary minority population of Native Americans. The region’s 319,000 residents average a density of nine (9) persons per square mile, as compared to the statewide average of 175 persons per square mile. The land and climate are not very suitable for agriculture. The economy has been based on logging, mining and tourism. Logging remains a major industry.

Nearly all of the region's 15 counties have full or partial Health Provider Shortage Area (HPSA) designation and full dental HPSA designation and several are designated Medically Underserved Areas.

Figure 1. Location of the Upper Peninsula Health Care Network Partner Hospitals

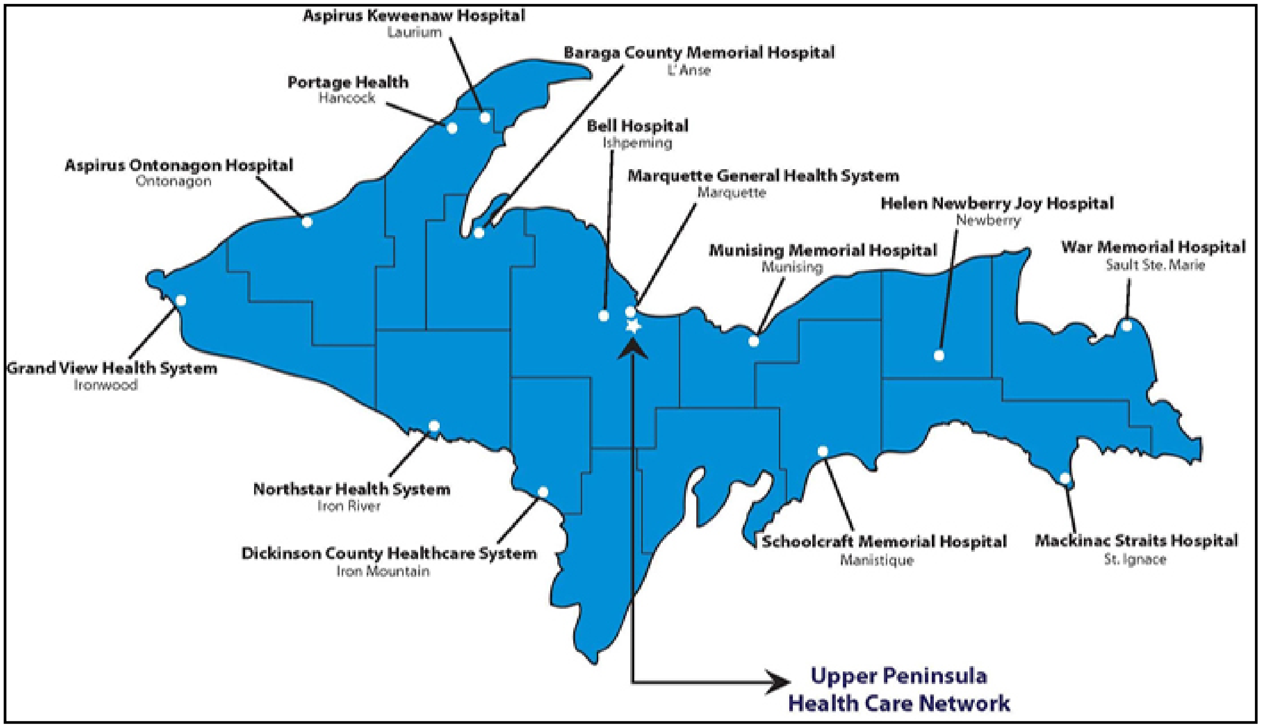


Figure 1 displays the location of the 14 hospitals that serve the region including: one centrally-located regional medical center (Marquette General Health System); three small rural hospitals; and 10 Critical Access Hospitals.

Phase I: HIE Network Planning—October 2004 – September 2005

During 2004, six of the region's Critical Access Hospitals (CAHs) acquired funding from AHRQ to plan the development of a regional Health Information Exchange to: Improve patient safety and quality of care through the regional planning, development, and implementation of Health Information Technologies. Over the 12-month planning grant period, the CAH facilities partnered with the regional referral center (Marquette General Hospital) and the Upper Peninsula Health Care Network to: (1) define areas of focus and Network goals; (2) evaluate and prioritize strategies; (3) define measurable HIT outcomes; (4) agree to the Network's ongoing evaluation process; (5) adopt a final regional HIT plan; and (6) prepare a 3-Year AHRQ Implementation grant application.

The 3-Year implementation grant, approved by AHRQ, was expanded to include 10 CAH facilities, designated through the Upper Peninsula Health Care Network to act as the HIE

Network's governing body. Marquette General Hospital to serve as the Hub for the Health Information Exchange and the developer of the HIE systems.

Phase II: HIE Network Implementation—from October 2005 – June 2008

As part of the planning process, the Upper Peninsula Health Care Network Board adopted the following statement of Purpose for the HIE Network implementation project: To improve patient safety and quality of care through the regional planning, development, and implementation of Health Information Technologies.

The Board next identified the following needs to be met by development of the rural Health Information Exchange:

1. Clinical information sharing to improve care delivery and patient's care experience. The goal is to give the caregiver as much information as possible when caring for the patient and to eliminate duplicate tests and exams when a patient‘s care is transferred from one setting/provider to another.

2. Consolidated Clinical data repository and reporting system to support quality and safety initiatives.

The sole referral medical center in the region, Marquette General Hospital, had already created a web-based, portal / repository application to enable clinical information to be accessed by its own 170 physicians and other health care providers while caring for patients. The initial Network Implementation plan was designed to build upon this existing HIE infrastructure. The AHRQ-funded implementation plan objectives included:

1. Upgrade the Electronic Health Record (EHR) systems within each of the small, rural partner hospitals to support the Network's electronic communication and data storage.

2. Develop a Regional HIE master patient index (MPI) to assign a unique number to each patient and creates a link between this number and the patient's medical record number at each site.

3. Develop a Regional HIE interface engine to receive and send data from each sites' clinical information systems.

4. Develop a Regional HIE clinical data repository to store and report on patient data from all of the participating sites.

5. Develop a web-based Portal Display to enable clinical information to be accessed by authorized providers regardless of where these results originated.

During this 3-year period, 11 of the 13 rural community hospitals (excludes Marquette General Hospital) acquired and installed EHR systems within their facilities.

However, during this same timeframe, KliniTek (the HIE subsidiary established by Marquette General to develop the HIE systems) was unable to expand the Marquette HIE system

(UP-Care) to include other Network facilities. In the fall of 2007, Marquette General Hospital underwent significant top-level management changes. By mid-2008, the new management at Marquette General made a decision to abandon the KliniTek UPCare HIE system and install a McKesson EHR system for their medical center.

After considerable project staff exploration for alternative HIE solutions, an alternative HIE solution was presented to the UPHCN Board in the summer of 2008, and submitted to AHRQ for approval in September 2008. The project revision retained the original project goals, but required a 12-month, no-cost extension of the project to reflect: (a) implementation of the newer HIE solution; and (b) revision of the timeframes to reflect completion of the original project by the end of Year 4.

Phase III: HIE Network Implementation—from October 2008 – September 2009

This revised phase of the project focused on the following three objectives:

a) Develop a network security architecture for Upper Peninsula hospitals to support the storing, maintaining, sharing and transferring of electronic data and documents;

b) Develop an accurate patient identification processes, based on fingerprint biometric data;

c) Permit data interoperability between the 14 rural hospital sites.

The expected results of the revised project remained to:

- Increase patient safety
- Reduce duplicate testing
- Accurately and securely share information between hospitals
- Increase efficiency of accessing data across sites
- Develop a network design that can continue to develop as the hospitals' network expands
- Permit hospitals to use their existing EHR systems to access information in the regional HIE system.

Methods

The project focused on the following four Key Areas or Tasks:

Task 1. Develop patient identification system to accurately identify patients and permit authorized physicians/staff access to these records within the federated domains. A prototype system was created to demonstrate patient identification system and its association with the network. The plan is to use smart cards and biometric technologies (fingerprints) for this system, based on accepted national standards.

Task 2. Establish database interoperability of disparate systems by developing a system to map received data to each of the selected site's electronic medical record system. Data mapping interfaces were developed to demonstrate interoperability between individual systems.

Task 3. Design and develop medical documents exchange system between hospitals within the federated domain. This includes creating an infrastructure and documents sharing servers that permit patient's clinical documents to be securely exchanged when transferred from one hospital to another, provided that both hospitals participate within the federated domain.

Task 4. Develop a federated security architecture for accessing, sharing, and transferring various types of medical data. The HIE includes role–based and policy–based authentication and authorization framework. Within this task, the goal was to develop/create a comprehensive solution including hardware/software that enables security services for different network topologies/environments and to demonstrate the product on a single-user workstation, multi-user networks in single/multiple cross-certified domains, and in a fully distributed environment within a federated topology.

The proposed solution was designed to meet national and international Health Information Exchange standards, and included a security system and architecture that would support rich functionality, strong security, and easy interoperability and scaling across the broader number of participants and potential users of the envisioned system.

The planned HIE system would provide accurate registration and handling of patient records, smooth exchange of patients' medical data both in databases and documents, and also controlled and authorized access to and sharing of medical information. The system also would provide better protection of medical data, easier handing of databases and documents, and efficient exchange of information, therefore contributing to the better, more efficient, but at the same time a more economical, platform of healthcare services.

Requirements and Needs for the Healthcare Information Exchange

For this Phase of the project, the participating hospitals and the UPHCN specified the following requirements and needs for the healthcare information exchange system.

Accurately Identify Each Patient throughout the Region. Hospitals within the region identify each patient by using a series of variables such as first name, last name, social security number, gender, etc. to establish a patient's master patient index (MPI) number. The uniquely assigned MPI number is used to identify the patient throughout each site. This methodology is problematic due to user error. Common issues assigned with this process include mistyping of patient information or inaccurate information provided by the patient themselves. As a result, more than one unique MPI identifier could be derived for a single patient. Patient records could show inconsistencies or inaccuracies as a result of multiple MPI numbers for a patient. Medical institutions within this project were searching for a solution to permit accurate identification and registration of patients that would integrate into each site's current EMR infrastructure.

Accurately Track Patients throughout Each Institution and Region. The hospitals had no method of electronically tracking patients within the region. Due to the smaller stature of most of the hospitals located within this region, many offered a limited number of services and must send their patients who are in need of advanced medical care to Marquette General Health System, which is the only tier II regional center within the area, or another hospital within the region. Therefore, developing a solution that would enable physicians and staff from each hospital within the Network to accurately track patients throughout the region was identified as a key feature for the proposed HIE solution.

Exchange Medical Information Electronically throughout the Region's Institutions. Due to the consistency of transferring patients to and from the hospitals within the region, along with the heightened possibility that patients may need medical service with another hospital in the region, permitting the electronic exchange of information between sites of the Network was felt to be critical. The ideal solution would permit real-time access of patients' records from any site in the Network to be displayed via a web graphical user interface (GUI). By instituting this process, medical institutions could better prepare and treat the patient, which would ultimately increasing the patients' safety within the hospitals of the HIE network. This process would also incorporate a significant monetary savings as well. The amount of duplicate testing between the hospital sites would decrease, since patient test values would be displayed in real-time for authenticated physicians and staff to view. Therefore, the same test that was conducted at hospital "A" before the patient was transferred to hospital "B", would not have to be performed again. Also, time taken to send and receive this information from the sending and receiving hospital respectively, would be greatly reduced with this proposed solution, and therefore resulting in an increase of savings.

Exchange Medical Documents between Medical Clinicians throughout the Region's Institutions. The hospitals within this project also had an immediate need to be able to securely share clinical documents throughout the region. Critical documents such as admission, discharge and transfer (ADT) were currently sent to other hospitals within the region by fax or unencrypted email. Both methods posed security threats to confidential patient data and infringed on policies set forth by governing health care agencies and legislation, such as Health Insurance Portability and Accountability Act (HIPAA). In addition, the process of document exchange was a manual process. The hospitals were seeking a sound method of document exchange that would be both secure and allow automation of document transfer when a patient was transferred to another site within the region.

Provide a Secure and Scalable Role-Based Solution to Access Patient's Records. To maintain a heightened state of security, each site within the Network sought to provide physicians and staff the ability to access patient records to better serve the patients' needs and become more efficient in their area of operations. Essentially, they wanted to integrate a solution that allowed physicians and staff to have secure web access to patient records within the region under a privileged role-based system. This solution would allow authenticated personnel to view critical information securely from each hospital's site or from a remote location.

The Concept of the Federated Security Healthcare System

Critical technical issues in health care, such as lack of interoperability due to the inclusion of proprietary systems, coupled with vague security requirements from HIPAA polices has resulted in a lack of information exchange between medical institutions. To combat this structure and enforce the exchange of medical information between sites under a secure platform, this project sought to develop a federated approach that would permit each site to securely exchange information between other hospitals within the Network. In addition, this project sought to develop an architecture that would empower patients within the Network to securely maintain their own patient health record (PHR) with the use of medical smartcards. To accomplish both goals, this project invoked a public key infrastructure (PKI) that used certificates to securely validate hospitals, patients, physicians and staff within the Network. The developed topology, under the PKI approach permits each site within the Network to maintain its established autonomous domain, thereby granting each site the authority to regulate or implement specific policies or rules that may be unique to their institution. This developed solution enforces strict use of noted standards in the field to ensure compliancy is met, scalability is possible, and interoperability of data is encouraged between sites within the Network. In order to implement security services in a federated environment, the system was established in the form of multiple autonomous domains. The following security management and operational services are reflected in various SETECS products (components of the overall system) and were further developed and tested by Michigan Technological University (MTU):

a) Identity management services (IDMS), compliant to the FIPS 201 (PIV) standard;

b) Public Key Infrastructure (PKI) components, protocols and services handling X.509 certificates;

c) Web Security Services (WSS), comprising components and protocols based on W3C, OASIS, IETF, and Liberty Alliance standards (secure XML, SOAP, SAML);

d) Secure transactions services for wired and wireless devices based on SSL, S/MIME, and SAML standards;

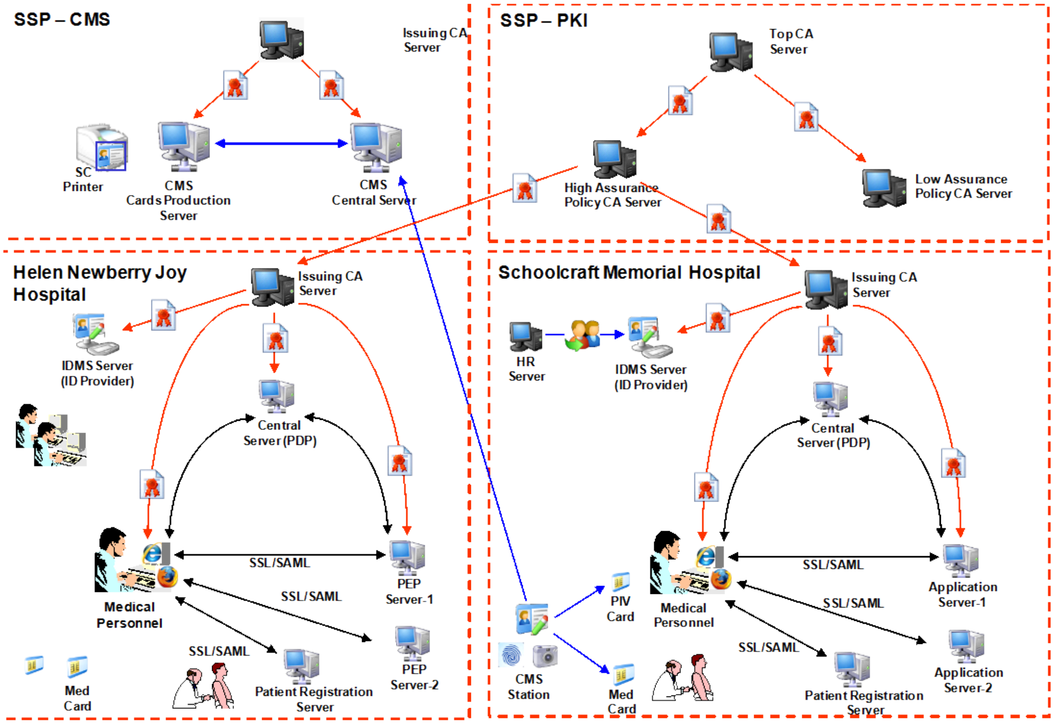
e) Patient Registration Server capable of registering each patient into a unique Master Patient Index (MPI) number, which will be used to accurately cross-reference patients throughout the federated architecture.

f) Smart Cards Management Services (CMS) compliant to the FIPS 201 standard and GSA requirements for architectures suitable for large–scale card deployment services.

The federated architecture deployed specified hardware and software products within each domain, as shown in Figure 2. Sites are be linked into a comprehensive system that enables security services for different topologies and environments including single user workstations and multiple users of local area networks in single or multiple cross-certified domains, and in a fully distributed environment of federated domains. Secure cooperation between those autonomous security domains is achieved by cross–certification between their Top CA Servers and by Network of Identity Providers (IDP) and Service Providers (SP) in the two domains. For the development period and the prototype of this architecture, three PCs were used at each site and the MTU Security Lab. Computer 1 served as IDMS Server. IT supported local security management of identities, remote, open network access for registrations and updates, and was used as the ID Provider in the SoA. This served as the source of personal registration data for other servers and components of the system.

In Figure 2, Computer 1 was used as a Certificate Authority (CA) Server. IT was linked to the IDMS Server and also in the overall PKI hierarchy, managed (in this project) by the MTU Security Lab. Computer 1 was a SoA Authentication and Authorization Server. It provided management of authentication credentials and was also used as a Policy Decision Point (PDP) for on-line authorization decisions. Computer 2 was used as the Secure Application Server. It stored locally some medical data, local Web–based applications and provided control access to those applications and data using XACML / SAML protocols. Thus, each such application server was extended to be Policy Enforcement Point (PEP) in the secure SoA. Computer 3 was used as an Integrated Card Management Station, and used to register patients and medical personnel, to capture their biometric data, and to manage their PIV smart cards. Other computers were user notebook computers with smart card readers. They were used for user access to other components of the architecture

Figure 2: Two of the hospital sites associated with the project – System Architecture and Component



In the HIE architecture, besides fourteen instances of the local security systems, located in each hospital, there are also additional Shared Services. In this project MTU acted as the Shared Services Provider (SSP) until final deployment, where the UPHCN entity will inherit ownership of the SSP technology. MTU supported two groups of such services: PKI and Card Management services. Thus, in addition to computers located in each hospital, MTU ran two additional computers: Computer 1 was used to host regional PKI servers: the Top CA Server and Policy CA Server. Computer 2 was used as an Integrated Card Management Server for smart cards. It was used to issue smart cards and store information about issued cards that would be used by Card Management Stations for post–issuance management and administration of smart cards.

Figure 2 above displays two of the autonomous domains that were federated within the HIE architecture. In this diagram, all components in the system (users and application servers) are certified. Each domain is cross–certified by their Top CA Servers. Smart cards transactions during card issuance procedure (CMS) are shown in red. When requests are approved, they are moved to the Security Infrastructure Provider (SIP) server where they are scheduled for printing and personalization, performed by Card Printing and Personalization (CPP) servers. Finally, they are activated by card issuers. Secure Web service transactions are shown in blue. Two Identity Providers are federated, using WSS Trust transactions. Users initially access their local Policy Decision Providers to obtain login SAML ticket. These tickets are presented on–line to Policy Enforcement Points (PEP) at secure application servers, which verify them by assistance of the PDP. This is SAML single sign–on, authentication and authorization protocol. Because of the Network, these protocols work equivalently in a single as well as in multiple, but federated domains.

System Operations and Utilization

This section describes the HIE's structure and the data flow within the network. The following five processes define the backbone of the developed HIE architecture.

a) Accurate Patient Identification. To enforce accurate patient identification of patients within each hospital, the HIE incorporates the utilization of fingerprint biometrics to identify each patient.

a) Accurate Patient Identification: Scenario #1—Patient Has Not Registered at Any of the Hospitals within the Network. Upon initial registration, patients provide preliminary information that is used to identify each patient. To accomplish this task, a GUI interface is provided for the patients to place their finger on the fingerprint reader to capture their fingerprint. A designated web camera also takes the patient's picture.

The captured print is then mapped to a unique MPI number within the SETECS identity management server. The patient's unique MPI number is separated between digits that reference the hospital that has initially registered the patient, while the other set of digits reference the patient themselves. The database backend of the SETECS identity management server then ties in the patient's identification information (i.e. Network MPI number, picture, first name, last name, date-of-birth, SSN and gender) to the hospitals EMR database. Therefore, when the patient's registration is finalized with the additional fields for the site's EMR system, initial patient registration information has already been transferred to these generic fields. Since each EMR uses its own set of Master Record Number (MRN) as the primary key between each of its databases, the unique MPI number that is created from the patient's fingerprint must be cross-referenced with the MRN number that is supplied with the EMR system at each site.

a) Accurate Patient Identification: Scenario #1—Patient Has Previously Registered at Same Hospital in the Network. If the patient has originally registered in the same hospital within the Network, a patient returning to the hospital would then place fingerprint on biometric reader located within the registration office(s) of the hospital. Pattern matching software then queries the identity management server for match of patient's fingerprint. When match is found, identity management server queries for cross-referenced the EMR's MRN for the patient. This process brings up the patient's registration information within the site's EMR to allow the hospital's registration personnel to confirm field entries of the patient. Once confirmed, the patient may proceed to location of appointment, as registration process is successful and secure.

a) Accurate Patient Identification: Scenario #1—Patient Has Previously Registered at Another Hospital within the Network. If the patient originally registered in a different hospital within the Network, the patient follows standard protocol of identification by placing fingerprint on biometric reader located within the registration office(s) of the hospital. Pattern matching software then queries the identity management server for match of patient's fingerprint. If local identity management server does not locate match, then remote identity management servers located within the Network are queried for the patient's fingerprint match. When a match is located, the remote identity management server sends the patient's registration information stored within its database to the identity management server where the patient is currently attempting to register. Once information is transferred, the identity server's database forwards generic fields to the site's EMR database. The patient's MPI number created by the identification process may then be cross-referenced with the new EMR created MRN upon registration. This process brings up the patient's registration information within the site's EMR to allow the hospital's registration personnel to confirm field entries of the patient. Once confirmed, the patient may proceed to location of appointment, as registration process is successful and secure.

b) Accurately Tracking Patients throughout the Network. The developed HIE permits physicians and staff to accurately track patients within the Network. Using a secure method of role-based access, authorized personnel are able to view a patient's electronic medical history throughout the institutions within the Network. Using the resource locator service, an authorized physician or staff member may track a patient by searching the implemented web front-end GUI available from a secure Internet connection. This web front-end incorporates patient search fields such as first name, last name, middle name, date-of-birth, gender, etc. The search process locates patients that match these defined criteria. To assist in confirming patient's identity, or when more than one patient is listed in the results of the search, a picture of each patient is placed next to their name, along with their Federated MPI number that matches to their unique fingerprint. This process provides accurate identification of the patient being searched. Each patient's picture is taken from the initial registration with the biometric system and serves as an alternative method of confirming patient's identity when fingerprint is not available (i.e. when tracking patient is conducted without the patient being present). Once the correct patient is found, authorized personnel then click on the patients EMR icon to bring up the patient's past medical information.

c) Electronic Exchange of Information. Once the patient has been accurately identified, authorized personnel may proceed to view the patient's medical records. A resource locator service is used to locate the patient's records throughout the Network. Due to the secure open-distributed architecture of the Network, real-time searching of institutions within the Network will commence and search for records associated with the identified patient. In this process, each institutions database is queried using the patient's federated MPI, cross-referenced to each of the local EMR's own MPI or MRN (as that is the primary key in searching for the patient). When a match is found, it is sent to the Network's database, where its fields are populated. Once complete, the Web front-end use to initiate this process will be populated with the medical information on the patient. The authorized physician or staff personnel are then able to view the patient's medical records and the electronic exchange of information is complete.

d) Document Transfer. Medical documents, such as Discharge Summaries, are very useful and widely used by medical personnel to obtain information about their patients. The HIE incorporates a method of transfer for selected documents for sites within the Network. The process of obtaining a document relating to a patient by authorized personnel functions in a similar manner as the electronic information exchange. If a document has been created for a patient at one or more of the hospitals, when the system is queried for a patient record, documents relating to the patient are transferred to the web database, where they are able to be viewed via the web front-end GUI.

e) Role-based Access within the Network. Using the PKI approach described in the above section regarding federated security, role-based access is available to access patients' records within the HIE. The system allows a security/ network administer at each hospital access control to the HIE to permit or deny the hospital personnel access at each site. This process also permits each site to develop its own rules and policies to ensure that individual regulations from each site are being satisfied. In addition, each site is responsible for adding or removing hospital personnel within their facility. In this architecture, a hierarchy stemming from the UPHCN was developed and a trust mechanism was built between each of the hospitals within the Network. As a result, only sites within the Network have access to patient records within this architecture.

Pilot Site Testing of the HIE

Four Pilot Sites were selected in development of the HIE system in order to account for each of the four different EMR systems used by hospitals in the UPHCN Network. The four EHR systems and pilot hospitals included: (1) Healthland EMR Systems at Helen Newberry Joy Hospital: (2) McKesson EMR Systems at Dickinson County Memorial Hospital; (3) Meditech EMR Systems at Portage Health; and (4) CPSI EMR Systems at Baraga County Memorial Hospital.

The development, testing and successful implementation of the HIE solution at these four pilot sites was designed to serve as solid platform for full implementation at all participating sites.

Results

Principal Findings

The project successfully designed and implemented a secure Health Information Exchange between the 10 critical access hospitals in Michigan's Upper Peninsula and the regional medical center, Marquette General Hospital.

The project successfully:

(a) Developed a patient identification system to accurately identify patients and permit authorized physicians/staff access to patient records;

(b) Established database interoperability of disparate systems by developing a system to map received data to each of the selected site's electronic medical record system;

(c) Developed a medical documents exchange system between hospitals within the federated domain; and

(d) Developed the federated security architecture for accessing, sharing, and transferring various types of medical data.

During the course of the 4-year implementation phase of the project, the scope of the project was expanded to include all hospitals involved in the Upper Peninsula Health Care Network (UPHCN), which includes fourteen hospitals and one regional center.

Although the HIE system successfully operates as detailed in this report between the four pilot site servers at MTU, there was insufficient time to deploy the HIE servers at the pilot sites and to test the system using actual patient identifiers and clinical data. This fact also resulted in an inability to compare pre-installation user survey data with post-installation surveys as required to assess the impacts of the HIE solution at the local level.

Technical Outcomes

The technical results of the project include:

Task 1. Develop patient identification system to accurately identify patients and permit authorized physicians/staff access to these records within the federated domains.
The patient identification was created to enable patient identification both locally and in association with the network. Smart cards and biometric technologies (fingerprints) were used for this system, and were based on accepted national standards.

The patient identification system was detailed in the previous section and includes:

1. IDMS servers located in each hospital, where patients are registered.

2. MIX Smart Cards Stations, used for enrollment and administration of smart cards.

3. Enrollment and Central Card Management Servers located in UPHCN which issues (printing and personalization) of smart cards.

4. 1500 smart cards delivered to the UPHCN (average 100 cards/hospital, plus 100 cards for UPHCN) to be used for MIX Security Cards, issued to professionals and for MIX Medical Smart Cards issued to patients.

Task 2. Establish database interoperability of disparate systems by developing a system to map received data to each of the selected site's electronic medical record system.
Data mapping interfaces were developed to demonstrate interoperability between individual systems. These systems include an engine to receive, process and store patient data into DB tables HL7 messages supported by the four EHR vendors in UP hospitals.

Task 3. Design and develop medical documents exchange system between hospitals within the federated domain.
The documents exchange system includes servers that permit each patient's clinical documents to be securely exchanged when transferred from one hospital to another, provided that both hospitals participate within the federated domain. This system includes:

1. An engine that creates A04 and R01 HL7 messages and stores them in a temporary DB table

2. MIX Hospital Server that support transfers of records

3. Extensions of the UPCare server to perform transfers

4. Crypto engine that performs PKCS#7 encryption of messages

Task 4. Develop a federated security architecture for accessing, sharing, and transferring various types of medical data.

Solution will include role–based and policy–based authentication and authorization framework. Within this task the goal was to develop/create a comprehensive solution including hardware/ software that enables security services for different network topologies/environments and to operate on a single-user workstation, multi-user networks, in single/multiple cross-certified domains, and in a fully distributed environment within a federated topology.

The federated security architecture includes:

1. Policy Administration Point Servers located in each hospital and in UPHCN, together with its associated Administrative Station that creates XACML authorization policies.

2. Policy Decision Point and Policy Enforcement Point components that support SAML–based authentication (single sign on) and authorization.

3. SAML and XACML extensions of the UPCare server.

4. Smart Card client that uses MIX Security Cards for user login and authorization.

5. Local Certification Server in each hospital and also in UPHCN, all linked to and certified by Hierarchy (UP CA Server) located in UPHCN and linked to and certified by SETECS Policy CA Server.

6. IDMS Server located in each hospital and in UPHCN.

In addition to the above Tasks, the project also delivered the following additional outcomes:

1. A MIX Hospital Server, that performs registration and administration functions for medical information system in each hospital and links hospitals through a federated MIX security infrastructure

2. A MIX Group Server, that performs MIX infrastructure functions linking hospitals with each other for data transfers and sharing, and linking the MIX infrastructure of UP to other (future) HIE infrastructures in the Country

3. A MIX Administrative Station, in each hospital and in UPHCN, used to administer MIX Hospital and MIX Group Servers

4. A PIV Integrated Station, to register PIV applicants, enroll them for PIV cards, and for management of PIV cards, used by UPHCN to create security cards for hospitals and PIV cards for its employees

5. A MIX Database, comprehensive HL7–compliant database schema with HL7 tables: data tables, coding tables, local tables, external and internal tables

6. An HL7 Engine, comprehensive HL7–compliant processing engine that can create and also receive / process all HL7 messages, not only the subset supported by the four EMR vendors

7. Upgraded UPCare Web Server capable of performing the following functions:

   - Transfer of A04 and R01 messages between hospitals

   - Authentication based on use of MIX Security Smart Cards

   - Authorizations based on XACML policy

Discussion

During the course of this Implementation project, 11 of the 13 rural community hospitals (excludes Marquette General Hospital) acquired and installed EHR systems within their facilities. This fact greatly enhanced the Network's capacity to create the necessary electronic patient records to be shared between providers in the HIE.

However, the inability of KliniTek (the HIE developer during the first 3 years of the project) to expand the Marquette HIE system (UP-Care) to include other EHR systems nearly caused the project to end in failure.

Identification of an alternative HIE solution in the summer of 2008, based upon the collaboration of Michigan Tech University and SETICS, and salvaged the Network's efforts of the previous 3 years. The HIE solution developed during the final year of the project does provide the Network with the solution it was seeking. However, the time necessary to develop the new HIE exceeded the project's ability to fully implement, and evaluate, it at the four pilot sites.

A significant issue faced throughout the project was the creation of interfaces between the central HIE and each of the four separate EHR vendor systems. Each site tested different clinical software, which made compatibility difficult. To achieve connection, several of the hospital EHRs required upgrades to transmit data with the HIE. Recent work at the national level to "certify" the various EHR systems should greatly reduce the types of incompatibility issues faced by this project.

In addition, data were not reported consistently between hospitals. To overcome these "data compatibility" issues, project leaders established a standards committee, with broad representation from the participating organizations. The group set standards for data consistency, using standards such as HL7, LOINC and SNOMED for transmitting information. Again, recent work at the national level should greatly reduce the types of issues.

In addition to technical barriers, project leaders had to contend with physicians' reluctance to change the way they report data to the HIE. To address this issue, project leaders began providing technical training and continuing education for physicians. In addition, project staff created a survey for doctors thought to be the most reluctant to embrace the project. The survey gauged their potential concerns and fears about the project. Staff then worked with those doctors to address their concerns and help them get comfortable with the software.

The collection of meaningful evaluation data could not take place as originally planned given that installation of the HIE servers could not be completed by the end of the project period. During the next six months, the planned electronic transfer of patient records between facilities will become possible as servers are installed at the pilot sites, and a subsequent evaluation of the HIE system will be possible.

The initial project plan called for development of a central data warehouse where each patient would be given a unique Master Patient Index (MPI) number. As part of the revised HIE solution developed during the fourth year of the project, the HIE system design was altered to a "federated" model where the patient identifier assigned within each hospital EHR would remain valid, while the HIE system would create a federated MPI for the identification of patients at each hospital.

Conclusions, Significance, and Implications

Based on the experience of the project team, the primary issues and problems faced by rural providers in their implementation of a rural HIE include:

1. A lack of understanding concerning the community's "readiness" to undertake this type of project. Implementation of an EHR system and/or participation in a regional HIE should not be a new concept. A poorly prepared community/facility will cause the project to lag behind even the most generous timelines.

2. Adequate resources are necessary for local health providers to acquire needed EHRs within their own organization, as well as to acquire interfaces to the regional HIE.

3. Adequate resources to acquire an effective, open-sourced HIE system for the rural network are required, as well as to develop effective interfaces with each local EHR.

4. Adequate pre-implementation planning for CAH participants is required to ensure their readiness to implement an EHR system and to participate in the regional sharing of their EHR data for the benefit of their patients.

5. Adequate state and national resources for the development of HIE and EHR standards, and for the sharing of ideas and experiences related to provider installation, use of EHR systems, and the sharing of patient data on a regional basis.

Although the Network has yet to become fully operational and achieve all its original objectives, the practices used in the planning, preparation, modification, and implementation of this project were effective and should prove to be very applicable, helpful, and relevant to other rural areas seeking to develop a regional health data exchange.

Where some networks have demonstrated a successful collaboration between CAHs owned by a tertiary hospital, this model addresses the issue of independent regional hospitals that have different needs and have selected different EHR systems. To date, the UPHCN are continuing to move the project forward to full implementation. Once the HIE becomes fully operational, we believe that it will be an excellent model to repeat in other areas with scattered, independent, smaller, rural hospitals.

List of Publications and Products

Design and Implementation of a Centralized Electronic Medical Records Consortium in a Rural Area of Michigan; Hembroff, Guy C., Wheeler, Donald, Boyle, Daniel. Published as part of the 9th International Conference on e-Health Networking, Application & Services (Healthcom 2007) June, 2007 in Taipei, Taiwan.

Secure Healthcare Information Exchange for Local Domains; Hembroff, Guy C., published as part of the 3rd International Conference on Pervasive Computing Technologies for Healthcare April, 2009 in London, UK.

Michigan Electronic Medical Records Project Provides Lessons Learned for Data Exchange; Wheeler, Donald. Published on the AHRQ website, Health IT Implementation Stories, in June, 2007. http://healthit.ahrq.gov/portal/server.pt?open=514&objID=5562&mode=2&holderDisplayURL=http://prodportallb.ahrq.gov:7087/publishedcontent/publish/communities/a_e/ahrq_funded_projects/health_it_implementation_stories/healthitimplementationstories/michigan_electronic_medical_records_project_provides_lessons_learned_for_data_exchange.html