Agenda

Title / Purpose:	MiHIN Technical Workgroup Meeting		
Meeting Date:	Jan 20, 2010	**Facilitator:**	Mike Gagnon
Place:	Conf Call and Web-ex	**Time:**	1:00 PM – 3:00 PM
		Conf Call #:	1-888-394-8197 Passcode: 869479
		Web Link	https://premconf.webex.com/premconf/j.php?ED=102412422&UID=0 Password: mihin-tech5

Topic 1:	**Attendance, Review and Approve Minutes**	**10 Min**
Materials:	Meeting Minutes	
Presenter:	Ken Theis and Rick Warren	
Topic 2:	**Review and Approve Final Draft of Technical Architecture**	**70 Min**
Materials:	Technical Architecture Final Draft	
Presenter:	Group Discussion	
Topic 3:	**Developing Questions for other Workgroups**	**20 Min**
Materials:	Preliminary list of questions	
Presenter:	Mike Gagnon	
Topic 4:	**Review status of Vendor Collaboration Team and Vendor Presentations**	**10 Min**
Materials:	List of Nominees for VTCT	
Presenter:	Mike Gagnon	
Topic 5	**Public Comment Period**	**10 Min**

Agenda and Meeting Minutes

Title / Purpose:	MiHIN Technical Workgroup Meeting		
Meeting Date:	Jan 5, 2010	**Facilitator:**	Mike Gagnon
Place:	Conf Call and Web-ex	**Time:**	9:00 AM – 11:00 noon
		Conf Call #:	1-888-394-8197 Passcode: 869479
		Web Link	https://premconf.webex.com/premconf/j.php?ED=102397092&UID=0 Password: mihin-tech3

Topic 1:	**Attendance, Review and Approve Minutes**	**10 Min**
Materials:	Meeting Minutes	
Presenter:	Ken Theis and Rick Warren	
Topic 2:	**Review Specific HITSP Standards**	**20 Min**
Materials:	HIT Standards Presentation	
Presenter:	Mike Gagnon	
Topic 3:	**Review and Comment on Technical Architecture**	**60Min**
Materials:	Technical Architectrure Draft	
Presenter:	Group Discussion	
Topic 4:	**Review coordination with Vendor Collaboration Team and Vendor Presentations**	**15 Min**
Materials:	None	
Presenter:	Mike Gagnon	
Topic 5	**Public Comment Period**	**15 Min**

DISCUSSION	**Topic 1: Attendance, Review and Approve Minutes**	
Voting member Bill Riley was not present.		
Meeting minutes for the first and second Technical WG meetings were approved.		
ACTION ITEMS	**PERSON RESPONSIBLE**	**DEADLINE**
None.		
DISCUSSION	**Topic 2: Review Specific HITSP Standards**	
Mike Gagnon presented 'Proposed HIT Standards for the MiHIN'.		
The first slide presented a list of HITSP Interoperability Specifications and the current version of each of those specifications. Some specifications are more mature than others. Some specifications are not part of priorities or use cases being considered for the MiHIN. For example, IS07 Medication Management could be part of the MiHIN but IS08 Personalized Healthcare probably will not. The specifications likely to be part of the MiHIN were highlighted.		

The next slide presented a matrix of HITSP components and the IS specifications in each of those components. Again, the HITSP components that likely to be implemented as part of the MiHIN were highlighted down the left side of the page.

Rick Brady, co-facilitator of the Business Operations Workgroup gave a brief summary of the HIE Service Priorities and the work being done by the Business Operations Workgroup. The HIE Service Priorities are:

1. Electronic clinical laboratory ordering and results delivery
2. Electronic public health reporting
3. Quality Reporting
4. Clinical summary exchange for care coordination and patient engagement
5. Electronic eligibility and claims transactions
6. Electronic Prescribing and refill requests
7. Prescription fill status and/or medication fill history

The Business Operations Workgroup will develop use cases developed for HIE Service Priorities 1 and 2. Value propositions will then be defined for each use case.

The next slide presented HITSP Transactions (and IS specifications) with those likely to be implemented highlighted.

The Technical Workgroup will need to identify and address technical priorities as well. For example, Transactions T16 and T17 are related to security.

The following slide noted the HITSP transaction packages.

Ernie Yoder noted that while TP46 Medication Formulary and Benefits Information was not highlighted, there are exceptions in reconciliation that require formulary access so this transaction package might have to be considered.

Mike noted that we should build the MiHIN design around the ideal (i.e., standards) and can always then veer from standards where necessary. He also noted that many of these standards are currently implemented in other architectures around the country or around the world.

Mike noted a transaction that was not highlighted (T40 – Patient Health Plan Eligibility Verification) since MiHIN has a clinical focus and this transaction has an administrative focus.

Doug Fenbert noted that there is limited value anyways there because payers have different processes for eligibility.

Mike noted that for some components, clinical documents could be implemented as summary documents and still meet the requirements.

C78 Immunization Document could become a high priority.

Dan Stross noted that in the end, the MiHIN could support all the transactions listed but any initial implementation plan would force the workgroup to choose what to implement first.

Mark Tuthill noted that not all lab results are created equal. In other words, the workgroup would need to know what the most important uses cases are.

Rick Brady noted that there could be trade-offs as to what use cases are most important and what is technically or financially feasible.

Mike concluded with the concept that the architecture needs to be designed to be able to implement ALL the transactions and components, over time and in the long run.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

DISCUSSION	**Topic 3: Review and Comment on Technical Architecture**

HIE policies can make technical implementation easier or administrative activities easier. For example, instead of passing user-ids, the MiHIN could trust organizations to validate user ids and pass trusted ones using SAML.

Dan Stross asked if major vendors like Medicity, or Axlotyl are configured today to interface in this way. Mike noted that most vendors are not currently at this point in their implementations but it is the current direction. We are looking to the Vendor Technical Collaboration to assist us so that we design in this same direction. We anticipate an interoperable architecture and a backbone that will be sustainable in the future as standards and vendor abilities progress forward.

Private HIEs plug into the backbone directly or through a community HIE. Large organizations will set up a MiHIN connectivity layer but it is more straightforward for an organization to plug into an edge server and let Community HIEs set up that MiHIN connectivity layer.

Additionally, once an organization plugs into one community HIE, the information will be shared through the MiHIN connectivity layer. There will be no need to connect to any other HIE for sharing.			
ACTION ITEMS		PERSON RESPONSIBLE	DEADLINE
None,			
DISCUSSION	**Topic 4: Review coordination with Vendor Collaboration Team and Vendor Presentations**		
Mike would like a list of 30-40 EHR vendors. See action item below.			
Vendor presentations will start in mid-January and go through mid-February. The presentations will be scheduled over the lunch hour.			
ACTION ITEMS		PERSON RESPONSIBLE	DEADLINE
None.			
DISCUSSION	**Topic 5: Public Comment**		
Deb Mosher informed the Technical Workgroup that CAHA will go live in 3-4 months**.**			

Attendance list

- Nathan Bunker — General Public
- Don Carne — member
- Lee Castigilioni — Member
- Marcus Cheatman — Member
- Doug Dietzman — Voting Member
- Darrell Dontje — Member
- Chuck Dougherty — Member
- Scot Ellsworth — MiHIN PCO
- Doug Fenbert — Voting Member
- Paul Groll — Member
- Larry Hamilton — Member
- Pat Klima — Member
- Troy Lane — Member
- Thomas Lauzon — Voting Member
- Pat Maltby — MiHIN PCO
- Mark Miller — Member
- Paul G. Miller — Voting Member
- Deb Mosher — Member
- Amber Murphy — MiHIN PCO - Dewpoint
- Samer Naser — MiHIN PCO – Dewpoint
- Mark Notham — Member
- Laura Rappeleye — MiHIN PCO
- Kevin Sackett — Member
- Dan Stross — Voting Member
- Steve Summers — Member
- Ralph Tenney — Member
- Ken Theis — Co-Chair
- Mark Tuthil — Voting Member
- Rick Warren — Co-Chair
- Bruce Wiegand — Voting Member
- David West — Member
- Ernie Yoder — Voting Member

Agenda and Meeting Minutes

Title / Purpose:	MiHIN Technical Workgroup Meeting		
Meeting Date:	Jan 11, 2010	**Facilitator:**	Mike Gagnon
Place:	Conf Call and Web-ex	**Time:**	9:00 AM – 11:00 noon
		Conf Call #:	1-888-394-8197 Passcode: 869479
		Web Link	https://premconf.webex.com/premconf/j.php?ED=102412692&UID=-1 Password: mihin-tech4

Topic 1:	**Attendance, Review and Approve Minutes**	**10 Min**
Materials:	Meeting Minutes	
Presenter:	Ken Theis and Rick Warren	
Topic 2:	**Review and Comment on Technical Architecture**	**90Min**
Materials:	Technical Architecture Draft	
Presenter:	Group Discussion	
Topic 4:	**Review status of Vendor Collaboration Team and Vendor Presentations**	**10 Min**
Materials:	None	
Presenter:	Mike Gagnon	
Topic 5	**Public Comment Period**	**10 Min**

DISCUSSION	**Topic 1: Attendance, Review and Approve Minutes**	
Voting members Tom Lauzon and Dan Stross were not present.		
Meeting minutes for the Third Technical WG meetings will published this week for approval at the next meeting.		
ACTION ITEMS	**PERSON RESPONSIBLE**	**DEADLINE**
None.		
DISCUSSION	**Topic 2: Review and Comment on Technical Architecture**	
Mike Gagnon presented Technical Architecture draft.		
Marcus Cheatham commented that currently we do have end points and connections to HIEs so these organizations will have to dwell in two worlds or MiHIN will have a migration plan to get off one network and onto the MiHIN. The answer is that has not been thought about yet. Will there be a migration over time or will we keep both connections around? (This refers to the layer between the source and the backbone and talks PIX and PDQ to the backbone.)		
Laura Rappleye commented that MDCH is beginning a plan for migrating State systems (MCRS, MDSS and the surveillance system) to the MiHIN.		
Mike pointed out that there are differing concepts here – one is getting communities connected to the backbone through HIEs; another is the state sponsoring an HIE to fill in the gaps when there is no HIE in a particular area (This layer of		

connectivity is time consuming and resource – intensive to build). The idea is the MiHIN project could include an HIE capability that would allow any source organization to connect in. But the question is should the project take that on right now? And is the WG comfortable with that concept? Governance team is starting to ask those questions.

Mike commented that small states can get away with a single HIE, but MI will have nine, or more than that.

Rick Warren on the Vendor Collaboration Team and HIE vendors, asking if they would come up with a better understanding of how to connect in i.e., a clear route for main players. Mike answered that we will go into it the Vendor Collaboration Team with a design concept in mind and let the vendors work from there.

Bruce Wiegand asked about sustainability, suggesting perhaps a fee to participate in the MiHIN. There could be some that have to connect to multiple times so a fee to connect to MiHIN plus a fee to connect to each HIE affect sustainability in the long run? Mike answered that the Finance WG is charged with working that out.

With this conceptual design, we are not designing for a single HIE. But there is still a Governance decision to be made with this design. Will it be a backbone with option to add on an HIE? We are not going to start with that, and it's a viable option.

Marcus Cheatham commented that this design has implications to HIEs and the WG should think about incentives to get HIEs to connect. Mike commented that one recommended plan would be to work with 2 or more HIEs to become pilots and we implement 2 use cases in those pilots, with matching funds for HIE to stand up those 2 use cases.

Any HIE would have to stand up the HIE connectivity layer (i.e, security, SAML, patient identify feed, lookups, NAV functions, etc.). And a backbone-type edge server could be used to query across the backbone. This is an NHIN-compatible model.

Is the team OK with this design concept? **The team stated that it is OK to go ahead with this design concept.**

Could start to centralized the data in the HIE at some point in time. The next step in migration calls for that as MiHIN matures, we will run into reasons to centralize data and the populations should people will be more comfortable, in the future, with allowing that to happen.

There are several technical use cases which will be documented as descriptions and diagrams to help the audience understand. Rick Warren asked if this information will this go along with the prioritized use cases. Mike answered that no, it would not and instead there would be separate design documents for each use case, each with its own technical specifications. This is just an example.

For Lab Orders and Results the backbone will process transactions and might create document transactions that are the 'push' transactions. 'Push' transactions can start out being less stringent on standards because they are one-to-one interfaces between two organizations.

Reporting immunizations to MCRS is a 'push' transaction. Once a document is posted from MCRS, inquiries would be allowed. We have to be sure standards are met.

Scot Ellsworth asked what type of review/approval/certification process will be established to ensure standards are being met. Mike answered that this process is a policy decision and separate from the technical design. We will have security rules based on policy decisions and HIEs will have to comply but this is not directly technology related.

Harvey O. commented on the new standards that come out December 30, 2009 and asked if individual offices can transmit immunization data, shouldn't this information go to the State system first? Mike answered that MiHIN is not looking to replace existing functionality that is already technically-appropriate for the task.

Backbone will be designed as ESB. ESB includes a registry with secure nodes: registry tells systems what services are available and how to communicate with that node/service. For sake of simplification, we could think of the State as one of these nodes.

Record Locator Service (RLS) is a relatively simplistic service – it looks for "these documents on these dates" and that is all it knows. (There are reasons we don't what it to have any protected health information.) Inquiries must go all the way to the end point to get the data. This is just an index.

Mike presented a question on provider/user identities: Will these be fed up to state level, or will we trust organizations and do SAML assertions, trusting that they have been authenticated at the HIE level?

We will expect data to be pre-normalized (ie, patient and LOINC codes) at the HIE level.

MiHIN will not implement a data warehouse in the early phases of implementation– but someday it will be an important part. The reason for this is that we will not have the breadth and depth of data initially to support a warehouse. Bruce Wiegand noted that with the work his organization is doing there could be a parallel network to connect to a centralized storage of normalized data.

Immunizations – VCT could help us decide on the feasibility of using the new standard, c78, (c32 is widely used today.) Do we want to be first?

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

DISCUSSION	**Topic 3: Review status of Vendor Collaboration Team and Vendor Presentations**

Current vendor presentations are:

- Thursday January 21st at 12:00: Axolotl
- Monday January 25th at 12:00: Covisint
- Tuesday January 26th at 12:00: SUN

These are for voting members only.

Three additional presentations are being scheduled.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None,		

DISCUSSION	**Topic 5: Public Comment**

Kathy Smith asked how pharmacy transactions would be handled. Mike answered that those are prioritized use cases and MiHIN would not want to replace the SureScripts/RxHub network that is already in place today.

Deb Mosher corrected a definition in the Conceptual Architecture Design Description glossary of terms – we will update. She also asked about the status of a decision on a Statewide HIE. Mike answered that is an HIE for connectivity to State systems, not a 'state-wide HIE'.

Jeff Hawley asked if the use case for lab order registry was ambulatory or also included inpatient? Mike answered that it is both.

Attendance list

- Don Artman — Member
- George Boersma — MiHIN PCO
- Gerry Branch — Member
- Nathan Bunker — General Public
- Richard Burgis — Member
- Don Carne — Member
- Lee Castigilioni — Member
- Marcus Cheatman — Member
- Kelly Coyle — Privacy and Security WG Facilitator
- Doug Dietzman — Voting Member
- Darrell Dontje — Member
- Chuck Dougherty — Member
- Scot Ellsworth — MiHIN PCO
- Doug Fenbert — Voting Member
- Paul Groll — Member
- Jeff Hawley — Member
- Troy Lane — Member
- Pat Maltby — MiHIN PCO
- Linda McCardel — Privacy and Security WG Facilitator
- Paul G. Miller — Voting Member
- Robert Moerland — Member
- Deb Mosher — Member
- Amber Murphy — MiHIN PCO - Dewpoint
- Samer Naser — MiHIN PCO – Dewpoint
- Mark Notham — Member
- Tim Orient — General Public
- Laura Rappeleye — MiHIN PCO
- Bill Riley — Voting Member

- Kathy Smith Member
- Steve Summers Member
- Ralph Tenney Member
- Ken Theis Co-Chair
- Mark Tuthil Voting Member
- Nancy Walker Member
- Rick Warren Co-Chair
- Bruce Wiegand Voting Member
- Ernie Yoder Voting Member

Questions for the MiHIN Governance Work Group

(from the Technical Work Group)

1. We are moving forward with the concept that the ARRA grant (with some matching funds) will fund the MiHIN Backbone and two pilot projects that includes connecting two HIEs and implementing two use cases. Here are our assumptions about this:
    a. The backbone will include a messaging gateway, EMPI, RLS, Provider Directory, and Security Services.
    b. The backbone is not an HIE and thus individual provider organizations will not plug into the backbone. Only HIEs will plug into the backbone.
    c. The state has decided not to implement a state-sponsored HIE for the reasons of cost, support and issues of potential competition with existing HIE efforts
    d. We will integrate two HIEs as pilot sites and assist them with some matching funds from the ARRA grant. We proposed 50% match.
    e. We will implement two use cases in these pilot sites. These Use Cases are single functions. For example Public Health Reporting is not a use case, rather immunizations reporting and inquiry is a use case. If we want to add syndromic reporting from EDs that is another use case.
    f. HIEs (whether Community or Private) will be implemented by stakeholder organizations and there will not be any state or ARRA support except for the pilots.
    g. If we stick to this plan and assumptions we believe that the ARRA funding with some match will cover this.

Questions for MiHIN Privacy and Security Workgroup

1. What data can or should be stored in the Record Locator Service on the MiHIN? The RLS contains meta-data about documents that are stored in the federated data bases (edge servers or XDS repositories).
2. Will we be implementing opt-in or opt-out consent for collecting data into the HIEs and MiHIN?
3. What technical construct will be required to identify that a provider has obtained consent from a patient to look at their data? A "Y" in a field, a scanned document, a digital signature, etc?
4. Should we implement two-factor authentication for each user of the MiHIN? Two factor authentication requires the user to know something and to have something (username/password and a physical token). Two-factor authentication has advantages and disadvantages. It is much more secure, much less prone to credential sharing, almost eliminates brute force hacking and allows passwords to be much simpler and thus easier to remember. Its major disadvantages are cost, management and user complications.
5. What roles should we establish for MiHIN system users?

MiHIN Vendor Technical Collaboration Team

Stakeholders	Name:	Email Address:
Allegiance Health System	Stephen Pittman	stephen.pittman@allegiancehealth.org
Ascension Health Information Services	Linda Coss	linda.coss@stjohn.org
Ascension Health Information Services	Mary Dery	mary.dery@stjohn.org
Michigan State University	Gerard Aubert	jerry.aubert@hc.msu.edu
Michigan Technical University	Guy Hembroff	hembroff@mtu.edu
my1HIE	John Vismara	john.vismara@my1HIE.com
State of Michigan - DTMB	Chris Weiss	weissc@michigan.gov
State of Michigan - DTMB	Larry Ruble	RubleL@michigan.gov
State of Michigan - DTMB	Paul Groll	grollp@michigan.gov
State of Michigan - DTMB	Scot Ellsworth	ellsworths@michigan.gov
State of Michigan - MDCH	Brad Carlson	carlsonbr@michigan.gov
State of Michigan - MDCH, Bureau of Labs	William Schneider	schneiderw@michigan.gov
Trinity Health	Lee Castiglioni	castigll@trinity-health.org
University of Michigan Health System	James Law	jlaw@umich.edu

Vendors	Name:	Email Address:
Accenture	Steve Wuerthele	steven.e.wuerthele@accenture.com
Allscripts	Jim Bresee	jim.bresee@allscripts. Com

Axolotl Corp	Lin Wan, PhD	lwan@axolotl.com
Capgemini	Gerry Yantis	gerald.yantis@capgemini.com
Covisint	Peter Greaves	peter.greaves@gmail.com
Crystal Lightning	Nathan Bunker	nathan@theizpartnership.org
dbMotion, Inc.	Joel Diamond, MD	joel.diamond@dbmotion.com
GE Healthcare	John F. Moehrke	John.Moehrke@med.ge.com
HP Enterprise Services	Brian Reed	brian.reed2@hp.com
IBM	Richard Franck	Richard_Franck@us.ibm.com

Initiate Systems, Inc.	Ryan Piper	cpiper@initiate.com
Intel Corporation	Joshua Painter	joshua.painter@intel.com
Intelichart	Randall Osborne	rosborne@ihsolutions.org
MedPlus	Derek Plansky	dplansky@medplus.com
Mirth Corporation	Jeff Peters	jeffp@mirthcorp.com
NextGate	Les Marcum	les@nextgate.com
Novell	Larry Chinski	lchinski@novell.com
Red Hat	Keith Babo	kbabo@redhat.com
SETECS Medical Technologies	Sead Muftic	sead.muftic@setecs.com
Symantec	Stewart Tan	stewart_tan@symantec.com
Verizon Business	Gerard A. Grundler	gerard.grundler@verizonbusiness.com
Wellogic	Sumit Nagpal	Sumit@wellogic.com

Phone Number:

517-788-4800 ext 4332

586-753-1500

586-753-1500
517-353-5568
906.370.9913
248-593-0148

517-241-9124

517-242-3680

517-241-8184

517-335-8165

517-335-9343

248-489-5296

734-936-1441

Phone Number:

609-897-5981

802-373-9060

408-920-0800 x117

703-795-3787

615-354-3536

480-213-6630

412-605-1952

920-912-8451

613-751-2265
919-254-9771

810-772-1740

312-320-6521

704-347-0661 x 5315

202-747-4502

949 255 5086

909-227-2236

630-561-1271

919-593-9101
240-535-2095

248-203-2608

703-402-9792

617-818-0000

Qualifications

Steve has been instrumental in establishing the bidirectional health information flow between Allegiance Health System and The Jackson Area Physicians represented by JCMR (Jackson Communitee Medical Record). Steve is the senior techical person on the project leading a team of interface analysts and the hospital health system programmers. He is responsible for the design of the implemented interfaces. He has first-hand experience with the challenges involved when trying to share Health Information betw organizations. Steve has thirty years of programming experience, ten in health care, and is a hands on leader.
Interface Expert from Ascension Health Information Services (IS organization for St. John, Genesys, Borgess, St. Mary's of Saginav St. Joesph of Tawas).

Interface Expert from Ascension Health Information Services (IS organization for St. John, Genesys, Borgess, St. Mary's, and St. Jo

Chief Information Officer for Health Affairs Michigan State University

Assistant professor at MTU, consultant in various medical research an ddeployment projects

President of my1HIE. HIE serving southeash Michigan with over 5,000 users - including 1,000 physicians.
Enterprise Architect - State of Michigan Department of Human Services (DHS) Technical Architect - BRIDGES System DHS Speciali Enteprrise Solution/System Design and Implementations, Security, Messaging, Middleware, Application development, Database Architecture, and OpenSource.
Larry works in MDIT and is responsible for applications in DCH. As you know some of these applications will be a part of the pul health use cases. I think it would be helpful for Larry to hear what the vendor community will present in your collaboration mee and how that will effect the interoperability of many of the state systems.

Enterprise Architect - State of Michigan Specilizes in Security, Middleware, Messaging, OpenSource
Chief Enterprise Architect of State of Michigan Director, Office of Enterprise Architecture fo State of Michigan MiHIN Project Co Office MDIT Project Manager MiHIN Conduit to Care Technical Work Group
Brad Carlson is the MDCH project manager for the Michigan Disease surveillance System (MDSS) and has been involved with coordinating messaging projects beween the MDSS and laboratory systems.
over 31 years in the State of Michigan public health laboratory. Involved with the laboratory information system since 1993. laboratory manager in the microbiology section since 1995.

* Senior Enterprise Architect at Trinity Health. * For the past 3 years, has lead a team that performs Technical assessments on a solutions being implemented in the Trinity Health IT environment. * Has performed technical evaluation and design work for th in the area of document and image sharing using the IHE profiles and protocols. * Has a deep understanding of interoperability standards and organizations. Is a member of the IHE PCD domain workgroups, and a member of the CE-IT Collaboration task forc formed by HIMSS, ACCE, and AAMI. * Is currently involved with HIE and portal architecture development at Trinity Health
James is one of our primary application and integration architects and and can represent the UMHS technical view across In-Patient/CPOE and Ambulatory. He can broadly represent many technologies and existing capabilities UMHS could bring to the ta from a solutions perspective.

Qualifications

Steve is a Senior Technical Architect in the healthcare practice with 15+ years of provider integration experience. In addition, he an extensive background in technical architectures related to interoperability, standards and approaches for HIE. He was one o Accenture architects on the NHIN Trial Implementation project. He has been actively involved in reviewing technical standards a designing solutions for various state-wide initiatives.

Mr. Bresee has filled a wide variety of roles in his 23 year healthcare informatics career. At IDX Systems Corporation, he concei and developed the companies first Web based applications, a solution that won the Microsoft Healthcare Users Group Award fo innovation. Mr. Bresee also served as General Manager of IDX's ChannelHealth.com subsidiary, and brokered the successful sa this business to Allscripts Healthcare Solutions. At Allscripts, Mr. Bresee conceived and developed the Allscripts Analytics Prod and has also served in operational roles as the VP of Support and Implementations, and VP of Development. Mr. Bresee's curren is VP, Connectivity Initiatives, where he is responsible for strategy and execution of Allscripts connectivity programs.

Lin Wan - Director of Application Development Appointed Director of Application Development in 2007, Lin has led the team in creating and deploying the second generation of award winning Elysium products. Currently she is consulting with the State of N York in the SHIN-NY project. Lin joined Axolotl 10 years ago as a Software Engineer and was instrumental in developing its lab ordering and results delivery products, and Axolotl's deployment of the US Nationwide Health Information Network (NHIN) proto Lin has held positions as Technical Operations Manager and Application Development Manager. Lin has a PhD from Princeton University in physics, a BS from University Of Texas at Dallas and a BA from PeKing University.

As the Global Healthcare and US Health Practice Lead for Capgemini Government Solutions, Gerry has over 26 years experience i account advisory management and support. Mr. Yantis' healthcare industry experience spans over 15 years and includes large transformation programs with payers; assessment and implementation of HIPAA transactions, code sets, security, and privacy; a international work on EHR/HIE programs. From February 2003 to December 2006, Gerry work with National Health Services (N England and Wales, on NHS England's National Program for IT (NPfIT); and the NHS Wales Informing Healthcare program, where served as Interim CIO and IT strategy advisor for EHR/PHR and hospital system strategy. In Dubai, United Arab Emirates, Mr. Yar was involved in a local healthcare organization's EHR/HIE strategy definition and project assessment which was attempting to implement HIE across competing hospital organizations for a single EHR service.

Mr. Greaves has over 20 years of IT experience, 12 of them running an IT consulting firm. He has been active in work surrounding National Healthcare Information Network (NHIN) for a number of years, and has worked with various organizations, including th Federation of American Hospitals, the Center for Healthcare Transformation, the eHealth Initiative and the National Alliance for Information Technology. He has been involved in work around RHIOs and HIEs in over 20 states, including Tennessee where he li Mr. Greaves is a former member of the Governor's Health Information Infrastructure Advisory Board for Florida and the eHealth Advisory Board for Tennessee. Greaves has chaired or participated in a variety of workgroups responding to healthcare issues a RFIs, and has authored or participated in a number of whitepapers. He is the current chair of the HIP TN Technical Architecture workgroup. Greaves has worked in a number of technical domains, and in addition to his healthcare experience has consulted i other areas including secondary and tertiary education, mining, manufacturing, legal, forestry and publishing. He has a BA degr from the University of Natal and two post-graduate qualifications in education.

Certified HL7 V2.4 Control Specialist, Certified HL7 CDA Specialist, currently participates on American Immunization Registry Association (AIRA) workgroup sessions, created immunization registry interfaces with EHR systems in 10 states with many more different software vendors

Dr. Joel Diamond, dbMotion's Chief Medical Officer, has extensive clinical and technology experience. He formerly served as CM and chairman of the Physician Advisory Board at the University of Pittsburgh Medical Center, St. Margaret Memorial Hospital, w he helped achieve 100 percent adoption of CPOE in a community hospital. This is one of the first such successes in the United St In addition, Dr. Diamond is president of Associates In Technology, a professional services firm that assists healthcare organizat with clinical information technology. A wide range of clients included physician organizations, state medical societies and IT ve including Misys Healthcare. He is a diplomat of the American Board of Family Practice and a fellow in the American Academy of Family Physicians. Dr. Diamond graduated from medical school at the State University of New York, Health Science Center at Syra in 1988, and completed his residency in Family Medicine at the University of Pittsburgh Medical Center (UPMC), St. Margaret Memorial Hospital in 1991. In addition to his position with dbMotion, Dr. Diamond is an active partner at Handelsman Family Practice in Pittsburgh, PA.

John Moehrke is a Principal Engineer specializing in Standards Architecture in Interoperability, Security, and Privacy for GE Healthcare. He is primarily involved in the international standards efforts related to GE's healthcare businesses. He is co-chair Security, Privacy and Infrastructure Technical Committee of HITSP. He is a GE representative to ASTM, CCHIT, DICOM, HL7, NEMA, OASIS, ISO, and IHE. He represents GE on issues of healthcare data security and privacy, IT Infrastructure, and clinical workflow has been active in the Healthcare standardization since 1999, during which time he has authored various standards, profiles an white papers.

Brian Reed is a Senior Programme Manager in HP's Canadian health care practice. He has deep experience in e-Health architectu (EHR and HIE) and program management in the healthcare industry. At Canada Health Infoway, the federal agency established to design and fund a pan-Canadian EHR, he was responsible for assessing and overseeing the implementation plans and architectu most of the provincial client (patient) registry projects across the country to ensure alignment with the national blueprint and standards. This work also involved exposure to the integration and deployment issues with respect to other core e-Health applic such as diagnostic imaging repositories, lab and drug systems. At the Smart Systems for Health Agency (now eHealth Ontario) he provided technical leadership with respect to the design and deployment of the systems for managing access to the province's e-Health applications and assets (HIE) which include registration of users, establishment of unique identity, provisioning of crede application of security and privacy controls and contextual access control to personal health information and EHR applications worked extensively with Ontario hospitals to map current registration and scheduling processes to develop a design for real tim

Richard is a leading Healthcare IT architect and has lead IBM's HIE architecture direction.

Ryan Piper is a technical consultant at Initiate. Over the past 6 years at both Initiate and Covisint, Ryan has developed deep experience and expertise in interoperability and health information exchange and is especially knowledgeable about Master Pa Index solutions and the role they play in interoperability and HIE. He has worked closely with multiple communities in order to establish health IT strategies for the deployment of electronic health solutions for HIEs, providers, health plans and independen physicians associations. Ryan's primary responsibilities include design, implementation and support of Health Information Exchanges. This includes the identification of use cases, sustainability models, driving of technical design teams and the organization partners based on required solutions sets. Ryan lives in Brighton, MI and already has a deep understanding of th Michigan market as he has been working with many of the stakeholders for years. He is readily available to assist MiHIN on the Vendor Technical Collaboration Team. INDUSTRY EXPERTISE OVERVIEW - IHE - HITSP - AHIC - Health Information Exchange - Federal Health Architecture - Healthcare Provider Information Technology TECHNICAL SPECIALIZATION - Health Information Ex

Joshua Painter is a Chief Architect within Intel's Software and Services Group in the SOA Products team, where he has a leadersh defining healthcare solutions strategy and architecture for Intel's SOA infrastructure products. Joshua has extensive experience areas of distributed computing, integration, enterprise application architecture and security. He spent the past decade working i international markets focused on solutions architecture for the public sector in the US, Europe and the Middle East. During his te years with Intel, Joshua has held various roles within product development, sales and marketing and IT. He spent the last severa years with Intel's healthcare division, where he helped bring Intel's first FDA-cleared in-home medical device to market. He repre Intel's Healthcare IT interoperability agenda through his active contribution for both domestic and international standards bodi including IHE, HITSP and HL7UK. Josh graduated with a B.S. in International Business and M.I.S. from Marquette University.

12 years experience developing HL7 engines/interfaces (v2.x, 3.x), 8 years experience developing voice recognition medical softw developer of 2001 MSHUG emerging technology product of the year. 10 years C#.NET experience 15 years C++ experience 14 ye SQL Server experience 2 years Oracle experience

Member of NY's NYeC workgroups including Protocols and Services, Technical Liaison, and Transport workgroups. Also regular participant in NHIN, NCHICA and Californian HIE standards discussions.

Information technology professional with over 17 years experience specializing in system design, operations, support and management in software development, manufacturing, managed B2B services and healthcare industries.

Lead HIE/EHR projects, Long term clinical integration in healthcare. EMPI, NHIN Architect with multiple implementation project experience

Larry has worked with the State of Mi for several years. He has worked on many of the projects in place and currently under way the North American Director of Identity Management at Novell and has been in the identity space for several years. He has been a active participant in several advisory boards both at the state and private level.

I am currently a Senior Solutions Architect at Red Hat, where I help customers with adoption of open source middleware solutior our JBoss division. Prior to Red Hat, I worked at Sun Microsystems for ten years, where I was a Senior Staff Engineer developing integration and SOA middleware platform software.

Ph.D., security expert (30 years of experience), adviser to VISA, EU, World Bank, etc.

Stewart Tan has been architecting Security and Compliance solutions for Symantec Corporation since 2006. Leveraging his earli experiences within a medical practice, he has been developing end-to-end security and compliance solutions for Symantec dedi Healthcare Team since its establishment in 2008. Prior to joining Symantec, Stewart spent 18 years with EDS performing global strategic and operational Information Security roles. In his current position Stewart concentrates his efforts on architecting healthcare related Security and Compliance solutions that assist organizations in automating and integrating Security and Compliance Programs into existing operational process frameworks. He is a Certified Information Systems Security Professiona (CISSP) and also holds an ITIL Foundations certificate.

Managing Principal for Verizon Healthcare 27 years of IT Professional Services and Consulting experience, 8 years as a Health CIO for a multi-national Healthcare services organization. Specializes in interoperability, data security, and Business Intelligence/Informatics in Healthcare. Owns trhe Interoperability, HIE, EMR, PACS, HIT/HIM vision & strategy for Verizon.

CEO and founder of Wellogic -- participation in numerous standards organizations -- participated in NHIN standards definition NHIN I and II efforts

Michigan Health Information Network (MiHIN)

Architecture Design

Draft v1.0

January 20, 2010

Table of Contents

1 Background 1
1.1 Introduction 1
1.2 Glossary of Terms 2
1.3 Describe the environment 3
1.4 Guiding Principles and Requirements 4
2 Business/Clinical Architecture Design 5
2.1 Meaningful Use Services 6
2.1.1 Lab Orders and Results 6
2.1.2 Public Health Reporting 6
2.1.3 Quality Reporting 7
2.1.4 Clinical Summary Exchange for Care Coordination 7
2.1.5 Eligibility Checking and Claims Transactions 8
2.1.6 ePrescribing and Refill Requests 8
2.1.7 Prescription Fill Status and/or Medication Fill History 8
2.2 Federal Functional Requirements 8
2.2.1 Functional Use Cases 11
2.3 Technical Use Cases 11
3 Technical Architecture Design 13
3.1 Core Design Concepts 14
3.2 Data Exchange Components 15
3.2.1 NHIN Connectivity 15
3.2.2 MiHIN Backbone 15
3.2.3 Community HIE 15
3.2.4 Private HIE 15
3.3 Technical Infrastructure Components 15
3.3.1 MiHIN Backbone 15
3.3.2 EMPI/RLS 16
3.3.3 Provider Index 16
3.3.4 Messaging Gateway 16
3.3.5 Data Warehouse/Repository 16
3.3.6 Identity and Access Management (IAM) Platform 16

3.4 MiHIN Backbone Services 16
3.4.1 Core Services 16
3.4.2 Business/Clinical Phase I Services 19
3.4.3 Business/Clinical Later Phase Services 20
3.5 Leveraging Existing Stakeholder Resources 20
3.5.1 Existing Value Added Networks 21
3.5.2 Existing Components 22
3.5.3 State of Michigan Systems 24
3.6 MiHIN Protocol Stack (MiPS) 25
3.6.1 Connectivity, Transport & Security 25
3.6.2 Messaging Standards 26
3.6.3 Terminology Standards 26
3.6.4 Health Care Service Orchestration 26
3.7 Standards 26
3.7.1 NHIN Standards 27
3.7.2 Transaction Standards 28
3.7.3 Message Payloads 30
3.7.4 Terminology Standards 31
3.7.5 Web Services Standards 32
3.8 Security Architecture & Standards 33
3.8.1 System (Node) Level Security 33
3.8.2 Authorization 34
3.8.3 Authentication 34
3.8.4 Access 35
3.8.5 Auditing 38
4 Interoperability with Stakeholders 40
4.1 HIE Interoperability 40
4.1.1 Infrastructure 40
4.1.2 Security 41
4.1.3 Transactions Workflow 41
4.1.4 Patient Update and Inquiry 42
4.1.5 Query for Documents 42
4.2 State of Michigan Systems Interoperability 43

4.2.1 Objectives 43
4.2.2 High Level Proposed Architecture 44
4.2.3 Description of Proposed Architecture 45
5 Risks and Benefits 48
5.1 Risks 48
5.1.1 Risk of Underestimating the Scope of the MiHIN 48
5.1.2 Technology Risk 48
5.1.3 Implementation Risk 49
5.2 Benefits 49
5.2.1 Architectural Model 49
5.2.2 Building Incrementally 50
Appendix A: Functional Use Cases
Appendix B: Technical Use Cases
Appendix C: Contractual Requirements

VERSION HISTORY

Version	Developed By	Date	Description
0.1	Michael Gagnon	11/27/2009	Initial draft of the document
0.2	Michael Gagnon	1/10/2010	Added to security and core sections
0.3	Michael Gagnon	1/12/2009	Completed a draft of most technical sections
0.4	Samer Nasser	1/14/2010	Added SOM Systems Architecture
0.5	Michael Gagnon	1/14/2010	Completed section on Leveraging Existing Stakeholder Resources
0.6	Michael Gagnon	1/17/2010	Completed HIE Interoperability section and made changes to Core Design Concepts and Standards.
0.7	Rick Brady	1/18/2010	Updated Business Architecture final copy for the report body
0.8	Michael Gagnon	1/18/2010	Added Risks and Benefits section.
0.8.1	Rick Brady	1/19/2010	Minor editing to business architecture section
0.9	Sharon McLear	1/19/10	Updates to format, grammar and sentence structure.
1.0	Michael Gagnon	1/20/2010	Final edits to draft

1 Background

1.1 Introduction

This document describes the technical architecture design for the Michigan Health Information Network (MiHIN). The MiHIN is an infrastructure design that enables widespread interoperability among disparate healthcare systems. This design is both vendor agnostic and technology agnostic, and focuses on technical standards, protocols, and architectural patterns. A key goal of this document is to provide an architectural design framework which can be used to guide detailed requirements definition, vendor selection and the implementation of the MiHIN backbone.

The architectural details specified in this document are intended to accommodate implementation of a State of Michigan backbone and local Health Information Exchange (HIE) projects while providing a framework that sets boundaries on the dimensions of technical implementation to ensure interoperability and consistent operation. The document is intended to describe the relevant interactions between the MiHIN Backbone and Community or Private HIEs. We expect to test these interactions with two or more pilot sites implementing a small number of use cases as recommended by the Business Operations workgroup. It is fully our intention to design the MiHIN to support healthcare transactions and interactions among a variety of entities that are healthcare data sources (e.g. – hospitals, physician practices, insurance plans, etc.) and healthcare data consumers.

The MiHIN Backbone is based on a service-oriented architectural paradigm (SOA), implemented through web services operating through an enterprise service bus (ESB), with a four-tier protocol stack. The protocol stack divides the protocols into categories, with the lower two corresponding to system architecture patterns, and the upper two dealing with healthcare architecture patterns. The MiHIN will be designed to be open, scalable and extensible in order to accommodate variations and improvements in technical, legal, and business standards and practices.

The MiHIN architecture has an overarching goal to be compliant with the national standards for healthcare interoperability recognized by the Secretary of the Department of Health & Human Services (HHS). Specifically, HHS recognizes interoperability specifications containing harmonized standards published by the Healthcare Information Technology Standards Panel (HITSP), and as such, the MiHIN is being designed as a HITSP-compliant and HITSP-consistent (where no direct conformance criteria exist) architecture. Similarly, HHS has sponsored a large scale development effort to build a national health information exchange capability called the Nationwide Health Information Network (NHIN) that instantiates the HITSP standards into real networks and systems. The MiHIN will leverage the work of the NHIN effort in its architectural framework, as is cited later in this document.

It should be noted that this technical architectural design represents our *ideal* for the MiHIN. For various reasons many of the design constructs described within this document may not be practical in the near term. For example while nearly all the constructs in this technical architecture design follow accepted national standards many of them are still emerging and have not yet been implemented in vendor systems. Most vendors are migrating from older HL7 v2.x standards to the newer HITSP and IHE standards but this often depends on customers requesting them. Since it is almost certain that to get the MiHIN working we will need to back away from some of the standards recommended within this document, it is important that we do so in a consistent manner and have a plan for migrating to the standard at the appropriate time. This is consistent with our guiding principles of:

1. Comply with the latest interoperability standards but be practical enough to get something working
2. Undertake an incremental approach to implementing a statewide architecture

Our long term plan for the MiHIN state-wide network includes four core capabilities:

1. Aggregating data and interconnecting providers via Community HIEs
2. A MiHIN state-wide backbone for connecting Community HIEs and providing a vehicle for the delivery of shared services
3. Shared clinical and administrative services and applications
4. NHIN connectivity for sharing data with other states and the federal government

This is a long term venture that will take substantial time and resources. Significant progress has already been made on establishing various models of Community and Private HIE's in Michigan, some sponsored by the state and some through private investment. This phase of the project will focus on designing and implementing the MiHIN Backbone and a limited number of shared services pilots. While the final decision on which shared services should be implemented may change, the current ones proposed are Lab Orders and Results and Public Health Reporting for labs and immunizations. These pilots were chosen for several important reasons:

- Both of these pilot shared services are in the list of the seven ONC (Office of National Coordinator) HIE Meaningful Use (MU) priorities
- They provide significant clinical value to providers
- The data required for these pilots is already being captured electronically
- They will require and test much of the core technical infrastructure needed for the Backbone

1.2 Glossary of Terms

Community HIE – A local HIE that is open to all providers and data sources in a region or across an affinity group

Documents – For the purposes of this design and HIE systems a Document is a patient-identifiable collection of structured, unstructured or image-based clinical or administrative

data that describes acts, observations and services for the purpose of exchange. Documents may be individual data points such as lab results but are more often summary collections of data for a particular episode of care.

HIE – A Health Information Exchange system often run by a RHIO or private organization

Michigan Health Information Network (MiHIN) – The name of the state-wide HIE organization and a term for describing the entire state-wide health network

MiHIN Backbone – The state-wide backbone for HIE interoperability

National Health Information Network (NHIN) – The federal government sponsored set of architectural constructs and standards which allow for basic interoperability among state and federal backbones and other HIEs.

Private HIE – A vendor sponsored, hospital-based or other privately run HIE

Regional Health Information Organization (RHIO) – An organization formed to operate an HIE, usually a not-for-profit.

Service Oriented Architecture (SOA) – An architectural concept that packages functionality as interoperable services within the context of various business domains. Several organizations may integrate or use such services — software modules provided as a service — even if their respective client systems are substantially different. It is an attempt to develop yet another means for software module integration. Rather than defining a specific interface, SOA defines the interface in terms of protocols and functionality.

1.3 Describe the environment

- Nine medical trading areas MTAs; 1 has a security framework implemented and is working to exchange data (UP); 1 has a contract and is in implementation (Capital area); 7 in various stages of planning.
- Seven state systems to be integrated; MICR, Vital records birth, death, disease surveillance MDSS, syndromic surveillance MSSS, data warehouse, StarLIMS (labs), Champs Medicaid. Also potential for Corrections System and Bridges.
- State architecture that could be used for HIE: Data warehouse (Teradata), ETL (IBM Datastage, Information Integrator), SSO (Tivoli but also contract with Novell), Data exchange gateway (FTP server, Messageway), Rhapsody, PHIN MS, Business Objects reporting environment, SAP Business Objects Data Quality platform
- No current SOA standards but there are some platforms i.e. IBM Websphere
- Regions have been sensitive about the original state proposed centralized design
- State workgroups have been formed
- Some large stakeholders may not participating in a region and some have the beginnings of Private HIEs

- Payer mix: Blue Cross Blue Shield (BCBS) (60%), Medicaid (state Medicaid plus some managed care companies) (20%), Medicare, other private payers, Priority Health, Physicians Health Plan (PHP). Delta Dental is also a player.
- BCBS and Medicaid using X.12 HIPAA transaction code sets. BCBS acts as a clearinghouse for many transactions.
- Large healthcare systems: Trinity, Spectrum, Detroit Mercy, Henry Ford

1.4 Guiding Principles and Requirements

The MiHIN will:

1. Be an infrastructure or network and not a system
2. Be built from numerous vendor products which must interoperate
3. Be vendor agnostic
4. Support multiple communication protocols within reason (FTP, SOAP, Sockets, etc).
5. Be a hybrid architecture that will not be entirely federated or centralized
6. Comply with the latest interoperability standards but be practical enough to get something working
7. Undertake an incremental approach to implementing a statewide architecture
8. Be consistent with Industry Standards (web services, etc) when not in conflict with our design
9. Focus on designing Information Exchange, not end-user applications
10. Interoperate with existing state and regional healthcare delivery systems
11. Interoperate with Community HIEs
12. Interoperate with existing state systems
13. Use web services for real-time communications where feasible
14. Interoperate with the NHIN
15. Be highly secure and HIPAA compliant for all external communication paths
16. Maintain the privacy of patient data
17. Be extensible (capable of adding new functions or services easily)
18. Be scalable (capable of adding more users, transactions or other volumes of work easily)
19. Support delegated user authorization, authentication & administration
20. Support auditing
21. Be able to support data and analytical capabilities
22. Be cost-effective to maintain

2 Business/Clinical Architecture Design

The function of the Business Architecture is to define the structure in terms of its processes and information. In the context of a Health Information Exchange backbone, such as the MiHIN, the Business Architecture is the sum of the processes and use cases inherent in the state-wide exchange of health information.

A Use Case is the utilization of a service by a consumer. It describes the transaction of information until the desired end state is achieved. Due to explicit requirements set by the ONC, the business architecture for the MiHIN will include explicit data formats when known.

In the context of health information exchange through a standards based backbone such as the MiHIN, the consumers and producers of data are abstracted; each will produce or consume the same standards based information. Consumers and producers are responsible for pre and post processing of information as required for use in their internal data systems and internal actors.

A base level documentation of current healthcare transaction levels and number of participants is provided to inform capacity planning exercises.

Event	Quantity/Year
Laboratory Transactions	31,715,000[1]
Immunization Events	
ED/Urgent Care admissions (MSSS)	3,650,000[2]
Reportable Lab Results (MDSS)	

Stakeholder representatives from across Michigan have ranked both the implementation order of HIE Services and the use cases in those services. The business architecture initially focuses on the highest ranked use cases in the highest ranked services. As these use cases are implemented, the business architecture will expand to cover all HIE services and their use cases.

Each use case documents the process of the actors and the information exchanged. When requirements for nomenclature or security standards have been mandated by the ONC, we have included the relevant requirement in the use case. The As Is state and To Be state is documented to facilitate the assessment of the expected change in actor processes. These changes are likely to affect and inform outreach, education and support functions: the larger the change in process, the greater the need for support and education services during the transition.

[1] Estimate based on Regenstrief data.

[2] Estimate based on State of Michigan, MDCH data

Several artifacts of relationships are cataloged for analysis. Artifacts:

- Actor Catalog
- Use Case Catalog (interaction of actors and services to obtain defined outcome)
- Data Catalog: data types by HIE Service Priority and their associated actors

The business architecture focuses on the use cases inherent in the ONC HIE Service Priorities and its goal of supporting Meaningful Use. To enable wide-spread adoption and in anticipation of an extended move by providers to meaningful use, the use cases have been written to support data creation and consumption by any standards compliant system. Such a system may be an EHR, an EHR light, an HIE (or its functional equivalent) acting on behalf of an EHR or other clinical system, a web portal capable of presenting standards based data in a human readable format or any other system commonly used which is capable of consuming or creating standards compliant data. The use cases use the term "EHR" to imply any of these systems.

The business architecture focuses on the Meaningful Use objectives for stage one. The architecture can be expanded as stage one objectives are documented in use cases and requirements for stage two grow nearer in time. The same strategy for stage three will apply when stage two is fully documented.

2.1 Meaningful Use Services

2.1.1 Lab Orders and Results

a. Lab Results Delivery
   i. Structured: incorporate clinical lab-test results into EHR as structured data (MU)[3], Harmonized Electronic Health Record (Laboratory Result Reporting) (AHIC)[4]
   ii. Unstructured
   iii. Diagnostic Images
b. Lab Orders: General Laboratory Orders (AHIC)

2.1.2 Public Health Reporting

a. Immunization Events and History: Capability to submit electronic data to immunization registries and actual submission where required and accepted (MU), Immunizations & Response Management (AHIC)
   i. Immunization event sent to MCIR
   ii. Immunization history received from MCIR
   iii. Vaccination forecasting data sent from MCIR
b. Syndromic Surveillance: Capability to provide electronic syndromic surveillance data to public health agencies and actual transmission according to applicable law and practice (MU)

[3] Supports Meaningful Use Objective

[4] Documented in an AHIC use case

c. Disease Surveillance: Capability to provide electronic submission of reportable lab results (as required by state of local law) to public health agencies and actual submission where it can be received (MU)
d. Public Health Case Reporting (AHIC)
e. Chronic Disease Registries
    i. Medical Home: Problem Lists & Practice-Based Registries (AHIC)
f. Newborn Screening (AHIC)
g. Harmonized Biosurveillance (Visit, Utilization, and Lab Result Data) Use Case (AHIC)

2.1.3 Quality Reporting

a. Incentive Metric Reporting
b. Report quality measures to CMS or the States (MU)
c. Research and Analytics
d. Quality (AHIC)

2.1.4 Clinical Summary Exchange for Care Coordination

a. Record, Store, Retrieve, Manage Order Types (MU)
    ii. Medications
    iii. Laboratory
    iv. Radiology/imaging
    v. Provider Referrals
    vi. Blood Bank
    vii. Physical therapy
    viii. Occupational therapy
    ix. Respiration therapy
    x. Rehabilitation therapy
    xi. Dialysis
    xii. Provider consults
    xiii. Discharge and transfer
b. Record demographics (MU)
c. Record and chart changes in vital signs (MU)
d. Record Smoking status (MU)
e. Provide patients with an electronic copy of their health information upon request (MU)
f. Provide patients with an electronic copy of their discharge instructions and procedures at time of discharge, upon request (MU)
g. Provide patients with timely electronic access to their health information (including lab results, problem list, medication lists, allergies) within 96 hours of information being available to the eligible professional (MU)
h. Provide clinical summaries for patients for each office visit (MU)
i. Capability to exchange clinical information among providers of care and patient authorized entities electronically (MU)
j. Provide summary care record for each transition of care and referral (MU)
k. Consultations and Transfers of Care (AHIC)

l. Emergency Responder — Electronic Health Record (AHIC)
m. Clinical Note Details (AHIC)
n. Patient - Provider Secure Messaging (AHIC)

2.1.5 Eligibility Checking and Claims Transactions

a. Check insurance eligibility electronically from public and private payers (MU)
b. Submit claims electronically to public and private payers (MU)
c. Prior-Authorization in Support of Treatment, Payment, & Operations (AHIC)

2.1.6 ePrescribing and Refill Requests

a. Drug-drug, drug-allergy, drug-formulary checks (MU)
b. Generate and transmit permissible prescriptions electronically (eRx) (MU)
c. Maintain active medication allergy list (MU)

2.1.7 Prescription Fill Status and/or Medication Fill History

a. Maintain active medication list (MU), Medication Management (AHIC)
b. Perform medication reconciliation at relevant encounters and each transition of care (MU)
c. Medication Gaps (AHIC)

2.2 Federal Functional Requirements

Some Meaningful Use objectives cannot be fulfilled through HIE. Current objectives not addressed are:

1. Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, and outreach
2. Send reminders to patients per patient preference for preventive/follow up care
3. Implement 5 clinical decision support rules

Some AHIC use cases are currently not categorized by HIE service priority. Currently uncategorized AHIC use cases:

- 2009 Requirements Documents
  - Consumer Preferences
- 2009 Use Case and Extensions/Gaps
  - Common Data Transport
  - Order Sets
  - Common Device Connectivity
  - Maternal and Child Health
  - Long Term Care – Assessments
  - Consumer Adverse Event Reporting
  - Scheduling
  - Preliminary Consumer Preferences Extension/Gap
- 2008 Use Cases
  - Remote Monitoring
  - Personalized Healthcare

- 2007 Use Cases
    - Consumer Empowerment: Consumer Access to Clinical Information
- 2006 Use Cases
    - Harmonized Consumer Empowerment (Registration & Medication History) Use Case (PDF)

It is uncertain if these use cases will be required for future Meaningful Use requirements. If they are, the earliest they will be included is in 2013.

HHS has required certain standards for content and nomenclature. Each use case documents its requirements. The population of requirements is shown below:

Required Content Exchange and Vocabulary Standards

Purpose	Category	Adopted Standard(s) to Support Meaningful Use Stage 1
Patient Summary Record	Cx	HL7 CDA R2 CCD Level 2 or ASTM CCR
• Problem List	V	Applicable HIPAA code set required by law (i.e.,ICD-9-CM); or SNOMED CT®
•Medication List	V	Any code set by an RxNorm drug data source provider that is identified by the United States National Library of Medicine as being a complete data set integrated within RxNorm+
•Medication Allergy List	V	No standard adopted at this time.
•Procedures	V	Applicable HIPAA code sets required by law (i.e., ICD-9-CM or CPT-4®)
•Vital Signs	V	No standard adopted at this time.
•Units of Measure	V	No standard adopted at this time.
•Lab Orders and Results	V	LOINC® when LOINC® codes have been received from a laboratory
Drug Formulary Check	Cx	Applicable Part D standard required by law (i.e., NCPDP Formulary & Benefits Standard 1.0)
	Cx	Applicable Part D standard required by law (e.g., NCPDP SCRIPT 8.1) or NCPDP SCRIPT 8.1 and NCPDP SCRIPT 10.6

Electronic Prescribing	V	Any code set by an RxNorm drug data source provider that is identified by the United States National Library of Medicine as being a complete data set integrated within RxNorm+
Administrative Transactions	Cx	Applicable HIPAA transaction standards required by law
Quality Reporting	Cx	CMS PQRI 2008 Registry XML Specification#,+
Submission of Lab Results to Public Health Agencies	Cx	HL7 2.5.1
	V	LOINC® when LOINC® codes have been received from a laboratory
Submission to Public Health Agencies for Surveillance or Reporting (excluding adverse event reporting)	Cx	HL7 2.3.1 or HL7 2.5.1
	V	According to Applicable Public Health Agency Requirements
Submission to Immunization Registries	Cx	HL7 2.3.1 or HL7 2.5.1
	V	CVX*,+

Meaningful use has a requirement for security, both in abstract and through specifications for security standards to be used. Security use cases ensure the protection of electronic health information created or maintained by a certified EHR technology through the implementation of appropriate technical capabilities (MU). The three types of security use cases are: transport, audit, and authenticate.

This architecture documents one security use case to be used for any transaction via the MiHIN. Details can be found in 3.8 Security Architecture and Standards.

Required Privacy and Security Standards

Row #	Purpose	Adopted Standard
1	***General Encryption and Decryption of Electronic Health Information***	A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (e.g., FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).+

2	***Encryption and Decryption of Electronic Health Information for Exchange***	An encrypted and integrity protected link must be implemented (e.g., TLS, IPv6, IPv4 with IPsec).+
3	***Record Actions Related to Electronic Health Information (i.e., audit log)***	The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (e.g., modification).+
4	***Verification that Electronic Health Information has not been Altered in Transit***	A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA1 or higher (e.g., Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180-3).+
5	***Cross-Enterprise Authentication***	Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g., IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).+
6	***Record Treatment, Payment, and Health Care Operations Disclosures***	The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.+

Required Quality Measures

As the ONC communicates the required quality measures for the HIE Services, the use cases will be updated to reflect these requirements.

2.2.1 Functional Use Cases

See Appendix A.

2.3 Technical Use Cases

Our technical use cases will describe in detail how the users, data and systems (actors) will work together to accomplish the functional use cases. Each technical use case will be depicted using a UML Sequence Diagrams which will describe the interactions between the actors at all levels of the MiHIN. Each sequence diagram will describe a single functional transaction. Some will be required for others to work, for example HIE must populate the MiHIN EMPI using a Patient Identity Feed use case before they can perform Subject Discovery. These constraints will be clearly defined in each diagram.

These diagrams are the precursor to building detailed technical specifications for each use case. Additional specifications will be built from the Vendor Technical Collaboration

Team work but final work will be accomplished just before implementation. Detailed technical specifications will be built incrementally as the use cases are prioritized. For this first phase our technical use cases are focused on the top two ONC priorities from the Business Operations Workgroup which are:

- Lab Orders and Results
- Public Health Reporting for Immunizations

For the two functional priorities identified above we will need the following technical use cases:

1. Patient Identity Feed to MiHIN EMPI
2. Patient Inquiry using ID
3. Patient Inquiry using Demographic Data
4. Lab Order and Result Transaction
5. Populate XDS Registry with Lab Result Document
6. Lab Results Inquiry
7. Report Immunizations to MICR
8. Populate XDS Registry with Immunization Document
9. Immunizations Inquiry

Each of these technical use cases will be described in a diagram in Appendix B.

3 Technical Architecture Design

The MiHIN Architecture Design has three main parts:

- Connectivity to the NHIN
- The MiHIN state-wide backbone
- Interoperability with data sources and consumers

As stated in the Introduction the MiHIN will be implemented using a service-oriented architectural paradigm (SOA), implemented through web services operating through an enterprise service bus (ESB), with a four-tier protocol stack. The Conceptual Architecture of the MiHIN is depicted in Figure 1.

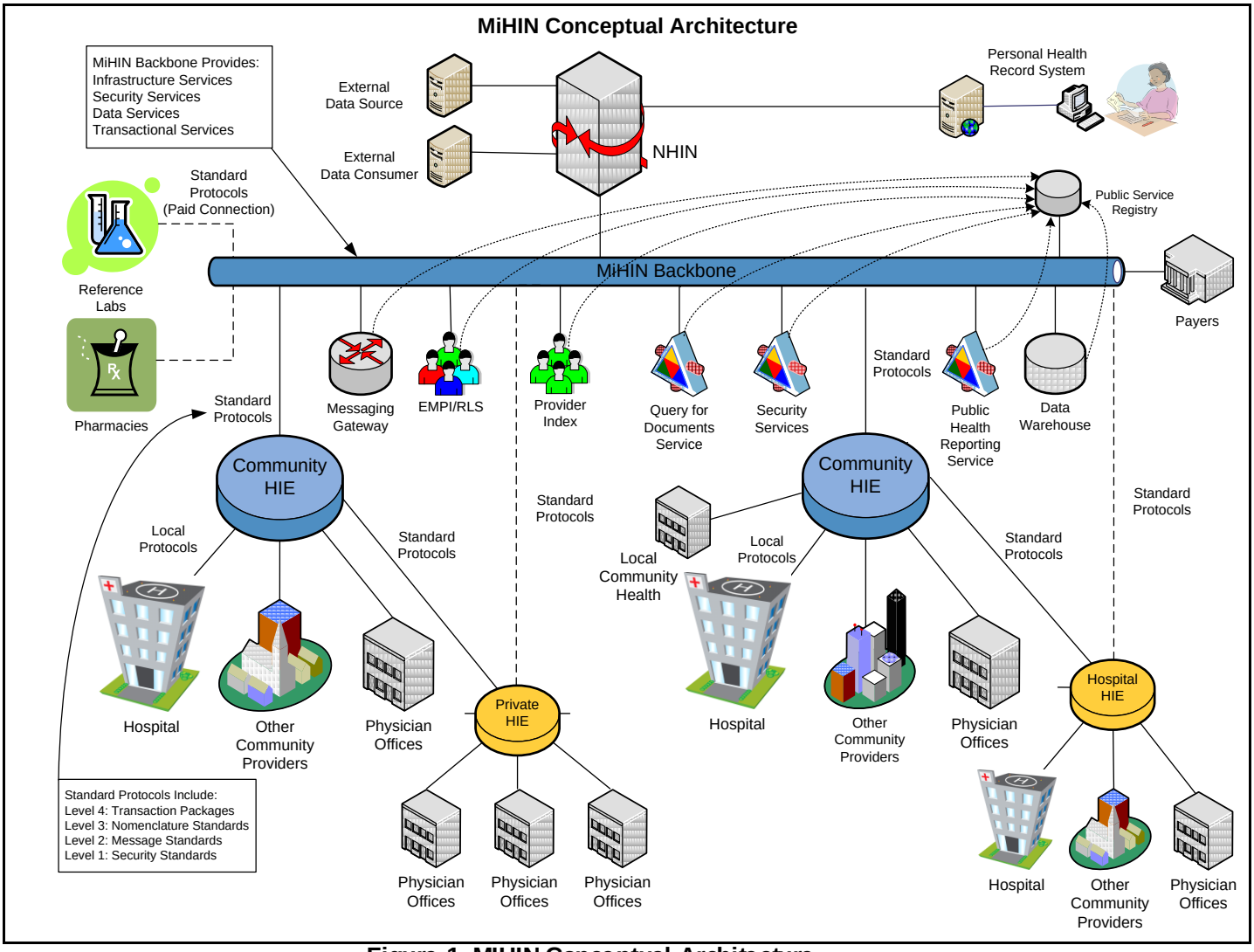


Figure 1: MIHIN Conceptual Architecture

3.1 Core Design Concepts

The design of the MiHIN Backbone is predicated on there being relatively few direct connections (<50). The idea is based on the common network design principle of segmentation for performance, security and reliability. We expect that a significant amount of the patient data that needs to be exchanged will be within Community or Private HIEs where the patient receives care. Just as networks use bridges, switches or routers to segment traffic we will expect that HIEs will segment traffic that can stay within the HIE and only route transactions to the MiHIN backbone that must cross HIEs.

The MiHIN Backbone architecture is designed to accommodate a vast majority of the administrative and clinical use cases that support broad Health Information Exchange by implementing four core services. Those services are:

1. Developing a Security Framework

   Allows for the authentication of systems (nodes) and users and manages patient consent. Also implements appropriate security policies for role-based access and auditing.

2. Messaging

   The ability to “push” messages from one node to another and accommodate data translations required for each site.

3. Subject Discovery

   Subject Discovery is the ability to perform deterministic and probabilistic searches for patients across HIEs.

4. Query for Documents

   Query for Documents is the ability to look up structured and unstructured data in the form of documents stored somewhere in the MiHIN network of data repositories.

Any use case which is predicated on connecting to a secure network and either pushing data or performing inquiries can be met with these core services. Of all the ONC priorities mentioned above the only one that could not be accomplished with these base services alone is ePrescribing which requires a fairly complex prescription ordering system.

Once the MiHIN is ready to move beyond these core services the backbone is designed to support more complex service interactions which we call Health Care Service Orchestration. An example might be performing clinical decision support services for a diabetic patient who had a high A1C lab test. The clinical decision support might be to look up other lab results or the patient current medications and recommend a course of action for the provider.

3.2 Data Exchange Components

3.2.1 NHIN Connectivity

This component provides communication to the Federal Government and other state backbones. This connectivity is effectively for communicating with anything outside the MiHIN. The first functions being supported on the NHIN are Security Services, Subject Discovery, Query for Documents and Retrieve Documents. The standards required for each of these services are identified in section 3.7.1 NHIN Standards below.

3.2.2 MiHIN Backbone

This component provides the backbone connectivity and state-wide services for Community HIEs, Private HIEs, ancillary data sources (labs, RxHub) and connection to the NHIN.

3.2.3 Community HIE

- Locally supported HIE
- Community HIE can select their own vendor and run the HIE
- Open to all providers
- State would require compliance with standards for MiHIN Backbone interoperability

3.2.4 Private HIE

- HIE supported by a private organization such as a vendor or hospital system often for profit or to promote the needs of a particular organization (hospital system) or affinity group (physician offices)
- Would not be an option for a Community HIE unless the Private HIE opened the HIE to all providers including competitors and is accepted by a majority of provider organizations
- Allows private organizations to connect their affinity groups or affiliates
- Private HIEs will be encouraged to connect to the Community HIE for data interchange with other MTA providers
- Private HIEs can connect directly to the MiHIN Backbone. In this case state would require compliance with standards for MiHIN Backbone interoperability.

3.3 Technical Infrastructure Components

3.3.1 MiHIN Backbone

The MiHIN Backbone will be designed as an Enterprise Service Bus architecture. The ESB will be capable of supporting ESB nodes which can provide transaction services. The exact topology of the MiHIN ESB has not yet been designed (single instance or federated for example). The ESB will support one or more service registries for web services provided by secure nodes. Community HIEs

will be required to be secure nodes and utilize a four level protocol stack for communication to the ESB.

3.3.2 EMPI/RLS

Enterprise Master Patient Index/Record Locator Service will be used for subject discovery (patient lookup) and content indexing services. This component can either be a single component or two separate components.

3.3.3 Provider Index

This is an index of all care providers in the state. This could be part of the EMPI listed above or could be implemented as a User Directory.

3.3.4 Messaging Gateway

Used for all transaction-based services such as Lab Ordering, Results Reporting and Eligibility Checking. Primary function with be interface transactions and message translation. Nomenclature normalization will be expected to happen at the HIE level.

3.3.5 Data Warehouse/Repository

Data repository would be used for centralized storage of data for Public Health Reporting, Quality Reporting, Medical Research and Chronic Disease Registries.

3.3.6 Identity and Access Management (IAM) Platform

Security services will provide user authentication, access, authorization and auditing services. The User Directory will be a federated design and the MiHIN User Directory will be built by aggregating users from all connected HIEs or State entities.

3.4 MiHIN Backbone Services

3.4.1 Core Services

3.4.1.1 Patient Identity Feed

One of the primary functions of the EMPI will be the collection of patient demographics for Michigan residents. This will be accomplished by

having each participating HIE or State of Michigan HIE send new patients and patient updates to the MiHIN EMPI in near real-time. In addition we will need to be able to process patient merge and un-merge messages. Patient merge is when two patients are found in either the provider organizations or HIEs EMPI that are really the same person. A this point the HIE should send a merge transaction to the MiHIN EMPI. The MiHIN EMPI will then link the two master ids for the patient but keep the records intact. This is done just in case we need to process an un-merge transaction. This transaction would be sent if a previously merged patient is found to be in error. The standards for Patient Identity Feed are described in section 3.7.2 Transaction Standards below.

3.4.1.2 Subject Discovery

Other primary services provided by the EMPI will be patient matching using deterministic and probabilistic algorithms and cross community (HIE) patient inquiries. Patient inquiry does not stand alone as a separate use case but rather is always part of some other use case such as HITSP IS11 Public Health Case Reporting. The standards for Subject Discovery are described in section 3.7.2 Transaction Standards below.

3.4.1.3 Master Provider (User) Index

The primary uses of the Master Provider Index will be as both a provider database and a user directory.

3.4.1.4 Query for Documents (XDS)

The Query for Documents service will be the primary way that users perform inquiry for clinical and administrative documents over the MiHIN. The QFD service will utilize a patient id obtained from a Subject Discovery transaction to identify documents that are available for viewing on the MiHIN. When a user (or a system function) identifies a particular document to be retrieved the MiHIN QFD issues an XDS query to the HIE XDS repository which responds with a particular document. The standards for these transactions are discussed in more detail in section 3.7.2.3 Query for Documents (XDS.b and XCA).

Figure 3 is a Unified Modeling Language sequence diagram of a typical XDS transaction with document integrity. The diagram outlines several interactions that are integral to the establishment of Document Integrity. The storage and querying of documents, as occurs in the Provide Document to Repository transaction is the trigger by which the Document Integrity activity is invoked. Once a document is provided to the Document Repository by the Document Source, the document is also registered in a Registry, so that it can be located.

Once a document is stored into a Document Repository, it can be located through a registry query and then retrieved by the Document Consumer.

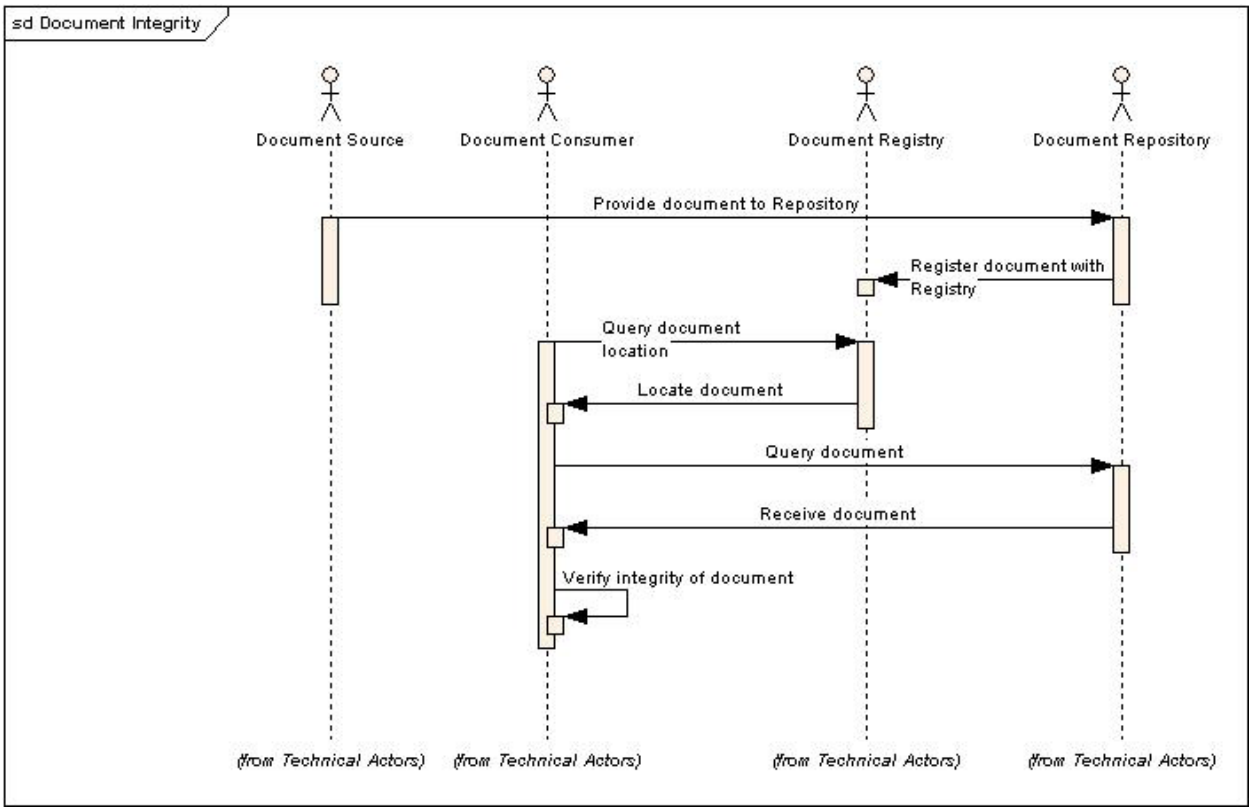


Figure 2 - XDS Inquiry with Document Integrity

3.4.1.5 Security

Security services will include state-wide trusted certificate authority for issuing digital certificates for Public Key Infrastructure (PKI). The security services must also host security polices most likely based on user roles. This is known as Role Based Access Control or RBAC.

It is not yet clear whether we need the MiHIN to have the identity of every provider and their authenticating credentials stored in the Master Provider Index described earlier. User authorization could just as easily be accomplished by using SAML (security access markup language) assertions in each message or inquiry request to the MiHIN and trusting each domain to have already authenticated the user.

Security services must also implement audit controls. See section 3.8 Security Architecture & Standards below for more details.

3.4.1.6 Service Registry

The MiHIN ESB will maintain a service registry using UDDI v2.0.4 as documented in the NHIN Messaging Platform Specification. The services allowed to be registered there will only be the approved list of MiHIN Core Service. The service registry will keep both endpoint servers addresses and Web Services Description Language (WSDL) service definitions.

ESB Nodes shall be found by clients through the use of an ordered or random "hunt group" list. Because the UDDI Registry Nodes for the MiHIN do not all reside in the same organization or in the same network domain, use of network-level multicast technologies will not work. Instead, clients shall each be configured with a list of UDDI Registry Nodes (each containing at least one server). They shall then search for one that is available by trying one after the other, in sequential or random order.

The primary use of the UDDI Registry within the MiHIN ESB will be to find services described by some well-defined criteria. This is accomplished using the find_service UDDI call, which returns a list of services. The specific WSDL for a service can then be acquired via a get_bindingDetail UDDI call. The output from this can then be processed by an automated function to generate the SOAP call to the service itself. Typically, a client will thus need to make two calls to find a service and its definition.

The MiHIN intends to adopt, if viable, the NHIN Connection Management & Service Discovery interface specification when it is finalized which is consistent with the paradigm listed above.

Typical Message Exchange Pattern

The MiHIN ESB, will be an intermediary for service invocation and return of responses and results. The basic sequence is:

1. Service Consumer discovers the availability of a service through interrogation of the ESB's service registry;
2. ESB does not expose true service endpoint, but rather exposes a local proxy;
3. Service Consumer invokes service through ESB;
4. ESB invokes appropriate service on Service Consumer's behalf;
5. Service Provider sends results to ESB;
6. ESB relays results to Service Consumer.

3.4.2 Business/Clinical Phase I Services

The following are the ONC HIE Priorities and will be considered for Phase I administrative or clinical use cases.

- Lab orders and results
- Public health reporting
- Eligibility checking and claims processing
- Quality reporting
- ePrescribing
- Prescription Fill Status and Medication Management
- Coordination of Care

3.4.3 Business/Clinical Later Phase Services

These are some examples of later phase use cases.

- Medical research database
- Chronic disease registries
- Patient transfer to post acute care

3.5 Leveraging Existing Stakeholder Resources

It is an important task when designing a new infrastructure such as the MiHIN to consider how to leverage existing resources. Considering the complexity and overall costs of building a state-wide Health Information Exchange infrastructure is it compelling to want to make sure we are not "reinventing the wheel."

On the other hand in most states the infrastructure that has been put in place is done for business reasons that do not match the business and functional goals, nor adopt the standards necessary, to support state-wide HIE. Just because a component exists does not mean it can or should be reused for the MiHIN. The "devil is in the details" so to speak. It could be too costly, too limiting from an interoperability point of view, or politically unpalatable to reuse existing assets.

The Project Control Office team has reviewed many stakeholder organization's and state systems to determine whether they can be leveraged as parts of the MiHIN. This section of the plan will review the different types of systems that might be leveraged and make some recommendations about how to determine if they can truly be incorporated into the MiHIN. The final determination about which systems can be leveraged will come as part of the Vendor Technical Collaboration Team efforts and during the system implementation phase.

We have identified four types of stakeholder or state assets that might be leveraged as part of the MiHIN. They include Existing Value Added Networks such as the claims processing network, Existing Components such as EMPIs at the state and other organizations, State of Michigan systems such as the Michigan Care Improvement Registry and Existing HIES whether Community or Private.

3.5.1 Existing Value Added Networks

Value Added Networks are existing HIE networks that are focused on a very narrow section of healthcare transactions. These networks are created to perform a particular healthcare service such as processing medical claims or quality reporting. The networks have multiple stakeholder organizations within the state and solve a particular problem for them. Because of their focus they often have clear financial benefit and thus are funded by the participating stakeholders because each derives a benefit from the network.

These networks represent one of the clearest opportunities for leveraging existing resources in the state. While the MiHIN Backbone will be designed to process these transactions, we are not recommending that these networks be subsumed by the MiHIN. Rather we believe that the MiHIN Governance and the State of Michigan should encourage or require these networks to be opened to all stakeholder organizations and follow the MiHIN standards for security and interoperability.

3.5.1.1 Claims Network

There are two claims processing networks in the state, the largest of which is run by Blue Cross Blue Shield who processes approximately 70% of all claims transactions. This network also provides other functions such as eligibility checking. The ideal model for this type of network is the New England Healthcare Exchange Network (www.nehen.org) which has been in place in Massachusetts since 1998. This network operates independently from any clinical HIE efforts. With the current scope of the Michigan claims networks we believe that they could be organized into a network similar to the NEHEN, perhaps governed by the MiHIN, but not a function of the MiHIN Backbone.

3.5.1.2 ePrescribing Network

Through pharmacies and pharmacy benefits managers (PBMs) a network has formed based on technology from SureScripts and Rx Hub. These technologies take electronic prescriptions from independent ePrescribing and Electronic Health Record systems and process them to local or national pharmacies and then to PBMs and eventually to the payers. This network is forming organically because it solves this particular problem and is more cost effective than paper prescriptions and manual claims processing. With the Meaningful Use requirements for EHR systems and due to the business value we believe this network will continue to grow. As with the claims network we do not think this should be performed by the MiHIN Backbone. Rather we believe that a web service connection to the MiHIN from RxHub and/or SureScripts can provide medication data for medication management.

3.5.1.3 Lab Results Network

There are several instances of lab ordering and results reporting networks in the state most often hosted by one or more large health systems whose clinical laboratory acts as a reference lab for physician offices or other smaller hospitals. Michigan Health Connect is one of these entities. Once again these networks reduce costs to the provider organizations by eliminating more manual methods of delivering lab results such as faxes or couriers. As hospital-based laboratories develop interfaces to physician office EHR systems it quickly becomes apparent that there are significant costs in developing these point to point interfaces. There are technologies and working laboratory network systems such the one in Vermont which allows any connected lab to order a test from any other connected lab. The current systems in Michigan are not quite up to this level but are moving in that direction and the MiHIN Governance should encourage this model.

3.5.1.4 Lab Results Repository

Another stakeholder in the business of laboratory is the Joint Venture Hospital Lab (JVHL). This organization was established to allow hospital-based reference labs to compete with large commercial labs for state-wide or regional contracts by having all the labs act as one entity. What is interesting from the MiHIN point of view is the laboratory results repository that the JVHL has in place with near real-time interfaces from many hospital-based labs in the state. While the JVHL would need to stand up an HIE interconnection infrastructure to connect to the MiHIN, if it did this several hospitals laboratory results could be made available on the MiHIN quickly.

There are few barriers that might make this more difficult, for example if an HIE is formed in a region and all clinical data except labs goes to the HIE vendor system how does that system connect to the lab results to incorporate them into their clinical portal? If XDS repositories were wide-spread and working this would be less of a problem but they are not. Even with this issue the MiHIN should consider subcontracting with the JVHL for quality reporting and perhaps for bringing clinical lab results online if only for the volume of data and the acceptance for providers.

3.5.2 Existing Components

Components are individual technology solutions that stakeholders already have that are required by the MiHIN backbone. For example messaging gateways (or interface engines), EMPIs, security tools and data warehouses are all examples of some of the technologies we uncovered during our analysis.

The core components of the MiHIN are crucial to its function, performance, security and success so reusing existing components must be considered only in

very limited circumstances. As the MiHIN matures there will be the need to have more than one backbone for purposes of reliability (by redundancy) and performance. Each of these backbones must operate in the same manner and follow the same standards. This is the model being developed in New York for the State Health Information Network of New York (SHIN-NY), which is to have RHIO HIEs all conform to backbone standards so that they can all process transactions. While this is beyond the scope of the current MiHIN project this model might make sense in the future. This is only mentioned here because it might be at that time that these component resources could be leveraged.

3.5.2.1 Messaging Gateways

Numerous provider organizations in the state have messaging gateways which are capable of processing and translating healthcare transactions. For the purposes of performance, security and to limit network traffic we believe that the MiHIN should have a messaging gateway on the same local area network as the MPI/RLS and other components. If the State of Michigan ends up hosting the MiHIN Backbone then they already have the Rhapsody integration engine which can be used for this purpose.

3.5.2.2 Enterprise Master Patient Index

Several provider organizations have EMPI systems embedded in their administrative or clinical systems but none of these would be capable of processing the PIX and PDQ transactions standards that we require for the MiHIN Backbone.

3.5.2.3 Data Warehouse & ETL Tools

While not a phase I capability a data warehouse would provide capabilities for quality reporting, data analysis and clinical research. The data ware house only becomes useful once a critical mass of data is being collected. For the MiHIN will likely take some time.

The data warehouse does not need to be located with the other MiHIN core components since interface performance is not crucial. The States Teradata Data Warehouse and IBM Data Stage and Quality Stage ETL Tools as well as their Business Objects reporting tools could be leveraged for use by the MiHIN.

3.5.2.4 Security Tools

The security tools for identity management and auditing for the MiHIN must be implanted at the location where the core components are installed. If the state hosts the MiHIN they have two security suites that could meet the needs of the MiHIN, the Tivoli Identity Management tools and the Novell Security tools.

3.5.3 State of Michigan Systems

There are several State of Michigan Systems that should be connected to the MiHIN. Details of the functions of each of these systems and their operations are detailed in another document, the SOM System Analysis. The mechanisms for how these systems should be integrated into the MiHIN are covered in section 4.2 State of Michigan Systems Interoperability.

This section will focus on the systems that play the largest role in meeting the Meaningful Use criteria and the benefits of connecting these systems to the MiHIN. Based on our analysis, we believe that the SOM Systems can be classified into two categories that represent the degree to which they would benefit from, contribute to, and impact the MIHIN:

1. SOM Systems that should be early services on the MIHIN
   These are SOM Systems that require interaction with a number of providers across the state and benefit from two-way communication with those providers. These systems often provide information back to providers or act as a gateway to federal government agencies such as the CDC. These would be MCIR and State Lab Systems. These systems would eventually expose shared services which will be utilized by stakeholders of the MIHIN.

2. SOM Systems that can benefit from the MiHIN infrastructure.
   These are SOM Systems that can benefit from some of the MIHIN Backbone services or communication channels. They would benefit from automatic collection of relevant data or data exchanges with other SOM Systems. These systems, in general, provide little communications back to Michigan providers. The MDSS, MSSS, Birth Registry, and Death Registry would be in this category.

3.5.3.1 Michigan Care Improvement Registry

The Michigan Care Improvement Registry is a powerful registry tool that has grown far beyond its original scope of protecting communities from vaccine-preventable diseases and to assure that the population of Michigan is appropriately immunized and that required child health prevention screenings are completed with the most efficient use of program resources. The MCIR is now a full-fledged population management registry and in conjunction with the state data warehouse provides analysis of at-risk populations.

MCIR will interoperate with the MiHIN in several ways. First it will benefit by utilizing the master data management tools of the MiHIN specifically the EMPI for patient matching. Secondly it will benefit from the connection of EHR and other clinical systems into the MiHIN for reporting the vaccinations given to residents. Finally the MCIR can provide benefit to providers and patients by making vaccination records

available to MiHIN users by populating a State of Michigan XDS repository that will be connected to the MiHIN.

3.5.3.2 Michigan Bureau of Labs Systems

The Bureau of Labs has one main lab system (StarLIMS) and a few other systems which provide lab data management and reporting for the State Lab.

The state labs will benefit from two-way communications over the MiHIN by being able to receive lab orders from providers and being able to report back lab results. In addition the state lab should benefit from being able to report lab results to the CDCP and other organizations using the MiHIN. Finally the state lab will be able to use the same State of Michigan XDS repository as mentioned for MCIR to make lab results available to users of the MiHIN.

3.5.3.3 Michigan Disease Surveillance System

The Michigan Disease Surveillance System (MDSS) will benefit from the MiHIN by allowing labs in the state to report their notifiable-disease test results electronically. Lab results can come from the state lab or private labs and can then use the MiHIN for reporting to the CDCP.

3.5.3.4 Michigan Syndromic Surveillance System

The Michigan Syndromic Surveillance System (MDSS) will benefit from the MiHIN by allowing emergency departments in the state to report their notifiable-disease diagnoses. Diagnoses or chief complaints can come from each hospitals emergency department probably in the form of an HL7 encounter transaction (A01) and can use the MiHIN for reporting to MSSS.

3.6 MiHIN Protocol Stack (MiPS)

Connectivity to the MiHIN Backbone will require each connecting system to comply with the MiHIN Protocol Stack (MiPS). The MiPS consists of a 4-tier stack with the lower two consisting of system architectural patterns and the higher two consisting of healthcare architectural patterns.

3.6.1 Connectivity, Transport & Security

Tier 1 is the base for any MiHIN node to connect to the MiHIN Backbone. This tier consists of the connectivity mechanisms, message transport and node and user security requirements. Standards for this tier are discussed below in the sections on Standards below.

We will implement secure nodes using the IHE Audit Trail and Node Authentication mechanisms. Details on the Secure Node connectivity is described in section 3.8.1 System (Node) Level Security.

All messaging will be using Simple Object Access Protocol (SOAP) over HTTP. For more detail on the Web Services Standards see section 3.7.5 Web Services Standards.

User authorization, authentication, and access are covered in sections 3.8.2 - 3.8.4 below.

3.6.2 Messaging Standards

Tier 2 of the MiPS protocol stack defines the message format standards for each type of clinical and administrative message. These standards are described in section 3.7.3 Message Payloads.

3.6.3 Terminology Standards

Tier 3 of the MiPS protocol stack defines the terminology standards for each type of data included in clinical and administrative messages. Terminology standards will be defined as the use cases are defined and the services implemented on the MiHIN. In phase I we will be implementing Lab Order and Results and Immunizations. The terminology standards for these initial use cases are described in section 3.7.4 Message Payloads.

3.6.4 Health Care Service Orchestration

Tier 4 of the MiPS is Health Care Service Orchestration, The protocols and services definitions for Health Care Services Orchestration will be defined as each MiHIN Backbone Service is designed and developed. These service definitions may fit existing HITSP Interoperability Specifications or we may need to define our own Interoperability Specifications by combining together the appropriate HITSP Transaction Packages, Transactions and Components. If we develop a new service definition it may qualify for submission to HITSP for creation of a new Interoperability Specification.

3.7 Standards

This section will focus on the national standards for web services, security and health information exchange. Our intention is to follow the standards published by the Healthcare Information Technology Standards Panel (HITSP), We are recommending a strict adherence to standards for the MiHIN Backbone due to ONC guidance and also to promote an open and interoperable MiHIN.

There are risks to this approach. Specifically many of these standards are not yet implemented in production vendor systems and this might slow our implementation and thus adoption. This is partly mitigated by our design concept of separating the functions of the backbone from those of the HIE. This allows the HIE proceed with data aggregation and local HIE using whatever method is necessary while keeping the backbone highly standards compliant.

As we describe each of the standards in this section we will categorize them by their maturity level. The reader should note that this is our expert opinion and is not based on

any national rating system. It is also likely that our categorizations will change once we have the Vendor Technical Collaboration Team review these recommendations. In addition these standards are constantly maturing so this is our best estimate of the current state. Despite this we feel that this information is important for the readers of this document to understand. Our categorizations are as follows:

- *Emerging*

  Emerging standards are those that have clear specifications written, have gone through some public comment and have been recommended.

- *Testing*

  Standards that are in Testing have been implemented in some systems and have been tested in NHIN Trials, IHE Connecathons, HIMSS Interoperability Showcases or other test scenarios. There may be working demonstrations of these standards

- *Limited Production*

  Standards that are in Limited Production have been implemented by a small number of vendors, systems or HIE to solve a particular problem and are live.

- *Full Production*

  Standards that are in Full Production are well established and have been implemented by a majority of vendors.

3.7.1 NHIN Standards

We will support the NHIN core functions of Security Services, Subject Discovery, Query for Documents and Retrieve Documents. NHIN Standards are mostly in *Testing* but there is at least one case of Limited *Production* with the MedVirginia connection to the Social Security Administration using Connect Open Source. To meet these functional requirements we will follow the NHIN Trial Implementations specifications as follows:

- Authorization Framework Service Interface Specification v2.2
- Messaging Platform Service Interface Specification v 1.9.8
- Patient Discovery Service Interface Specification v 0.9
- Query for Documents Service Interface Specification v 1.6.10
- Retrieve Documents Service Interface Specification v1.6.8
- Health Information Event Messaging v1.5
- NHIN Services Registry Specification v1.3
- Access Consent Policy Specification v0.3
- HIEM Profile Framework

3.7.2 Transaction Standards

The following messaging standards will be required for interaction with the MiHIN Backbone.

3.7.2.1 Patient Identity Feed (PIX)

Patient Identity Feed is the mechanism used for loading and updating patient identities in a Master Patient Index. Patient Identity Feed is described in the HITSP TP22, Patient ID Cross-Referencing Transaction Package and uses the IHE Patient Id Cross Reference (PIX) message format. PIX is categorized as *Limited Production*.

3.7.2.2 Subject Discovery (IHE PIX & PDQ)

Subject Discovery is the mechanism for looking up patients in a Master Patient Index. There are two HITSP standards for these transactions depending on whether the requesting system already has a deterministic identifier for the patient or whether a non-deterministic query is being performed. PDQ is categorized as *Limited Production*.

For deterministic queries HITSP TP22 will be used. A PIX transaction against the MiHIN MPI would require either performing this query with the master ID of the patient from the MiHIN MPI or using a patient ID from an HIE which maps one-to-one to the MIHIN master ID.

For non-deterministic queries HITSP T23, Patient Demographics Query Transaction will be used. A PDQ transaction would normally provides a set of patient demographics data elements, such as name, date of birth, etc. which can then be used to query the MiHIN MPI. The result of a PDQ transaction is typically a list of candidate patients from which a user (provider) can select the appropriate patient. Once the patient is selected a PIX transaction can be performed.

3.7.2.3 Query for Documents (XDS.b and XCA)

Query for Documents is the mechanism that will be used to provide cross-community (HIE) document sharing. While this construct appears to be the clear standard for cross-HIE document sharing it is not yet in wide use. Most uses of the XDS.b have been in demonstration projects, IHE Connectathons and HIMSS Interoperability showcases. QFD through XDS.b is categorized as *Testing*.

The following text from TP13 helps describe the functions of XDS and XCA:

To support this HITSP Manage Sharing of Documents Transaction Package, HITSP has selected the Integrating the Healthcare Enterprise (IHE) Cross-Enterprise Document Sharing (XDS) and the Cross Community Access (XCA) Integration Profiles, which facilitate the registration, distribution and access of

patient electronic health records across healthcare enterprises and across communities of such enterprises. Cross-Enterprise Document Sharing is focused on providing a standards-based specification for managing the sharing of documents between healthcare enterprises, ranging from a private physician office, to a clinic, to an acute care inpatient facility and other healthcare IT systems. Cross Community Access is focused on creating a "network of networks" or communities by providing the means for a community to access consumer's health records managed by other communities.

It is our goal to implement HITSP TP13 Query for Existing Data Transaction Package to support these transactions. Implementing TP13 would require us to implement XDS.b repositories. However from a practical point this might limit our ability to get rapid adoption of the MiHIN since many Community and Private HIE vendors might not yet have this capability. Thus we may consider a hybrid approach which allows us to support both XDS.b repositories as well as backbone vendor "edge servers" at HIE sites.

3.7.2.4 Document Notification (NAV)

As HIEs or other XDS repository providers make documents available for query over the MiHIN backbone they must notify the backbone of their availability using the HITSP T29 Notification of Document Availability transaction also known as NAV. NAV is categorized as *Testing*.

3.7.2.5 Lab Orders and Result Transactions

Lab orders and result transactions will be implemented on the MiHIN Backbone for routine reference laboratory ordering, results delivery and public health reporting. It is our intention to provide laboratory transaction services but not to replace existing laboratory networks such as Michigan Health Connect or the Joint Venture Hospital Laboratory.

Laboratory Orders and Results transactions will initially be implemented as a basic messaging service on the MiHIN between a lab ordering site and a provider of laboratory services. These transactions will effectively be point-to-point from one ordering site to one lab and back. In this phase of the MiHIN implementation the sending and receiving sites must comply with the MiHIN security requirements but we will not require specific standards regarding the message payloads. We categorize this type of lab transactions use case as being *Full Production* since there are probably thousands of examples of working lab interfaces.

As the MiHIN matures we envision that it will support an open marketplace for laboratory services where any provider of lab services can publish a shared web service which would allow any consumer of lab services to order tests. When this is implemented there will need to

be strict compliance with the HITSP IS01 Electronic Health Records Laboratory Results Reporting Interoperability Specification and the T14 Send Laboratory Result Message Transaction. There are limited HITSP standards for laboratory order messages such as the HITSP CAP99 Communicate Lab Order Message Capability. We categorize the lab results reporting specifications as *Testing* and the lab ordering specifications as *Emerging*.

3.7.2.6 Laboratory Results Inquiry

Laboratory results inquiry will be provided by the Query for Documents capability described above and utilize the message standards described in section 3.7.3 Message Payloads.

3.7.2.7 Immunizations Reporting Transactions

The standard for Immunizations reporting to the Michigan Care Improvement Registry (MCIR) will be to follow the guidelines of the HITSP IS10 Immunizations and Response Management Implementation Specification. IS10 is intended to support current interoperability approaches installed between Electronic Health Records (EHRs) and Immunization Information Systems. However these requirements and alerts are largely untested at this time pending further standardization efforts. The MiHIN could be an early adopter of this standard.

3.7.2.8 Immunizations Inquiry

Immunizations inquiry will be provided by the Query for Documents capability described above and utilize the message standards described in section 3.7.3 Message Payloads.

3.7.3 Message Payloads

3.7.3.1 Lab Order Messages (HL7 2.5.1)

Our standard for lab orders transactions being sent over the backbone will be HL7 2.5.1. HL7 v2.5.1 is categorized as *Full Production*.

3.7.3.2 Lab Result Messages (HL7 2.5.1)

Our standard for lab results transactions being sent over the backbone will be HL7 2.5.1. We will also allow the use of CCD C36 Lab Result Message or C37 Lab Report Document. These two newer standards are preferable for interoperability but there are too few health systems using these standards to make them practical at this point. HL7 v2.5.1 is categorized as *Full Production*.

3.7.3.3 Lab Results Inquiry (CCD C36 or C37)

Our standard for lab results that are posted to an XDS repository for query by other HIEs will be the CCD C36 Lab Result Message or C37 Lab Report Document. These two newer standards are preferable for

interoperability and make sense as standards for HIE connections since HIE vendors are beginning to incorporate these XML-based standards into their products. CCD C36 and C37 are categorized as *Limited Production*.

3.7.3.4 Immunizations Reporting Messages (C72)

Immunizations records will utilize the HITSP C72 Immunization Message which provides the capability to communicate an update to a patient's vaccination record. It is based upon the Centers for Disease Control and Prevention Implementation Guide for Immunizations Data Transaction using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol message type VXU Unsolicited Vaccination Record Update. C72 is categorized as *Emerging*.

3.7.3.5 Immunizations Inquiry (CCD C32 or C78)

There are two possible standards for immunization payloads either the CCD C32 Summary Document which is a well formed XML standard and being used for document exchange. However there is a specific standard for immunizations called the Immunization Document Component (C78) which is based on the IHE Patient Care Coordination (PCC) Immunization Content (C83). It is not clear at this time whether any vendors are actively supporting this standard. As we engage vendors in the process we can determine the feasibility of using this new standard for immunizations that will be stored in XDS repositories. CCD C32 is categorized as *Limited Production and C78 as Emerging*.

3.7.4 Terminology Standards

3.7.4.1 Labs (LOINC)

This is a database of universal identifiers for laboratory and other clinical observations. The laboratory portion of the LOINC® database contains the usual categories of chemistry, hematology, serology, microbiology (including parasitology and virology), and toxicology; as well as categories for drugs and the cell counts typically reported on a complete blood count or a cerebrospinal fluid cell count. Antibiotic susceptibilities are a separate category. The clinical portion of the LOINC® database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments, and other clinical observations. For more information visit the website, www.loinc.org. LOINC is categorized as *Full Production*.

3.7.4.2 *Medications (RxNorm)*

RxNorm provides standard names for (1) clinical drugs and (2) drug dose forms as administered to a patient. Also provides links from clinical drugs, both branded and generic, to their active ingredients, drug components (active ingredient + strength), and related brand names. Food and Drug Administration (FDA) National Drug Codes (NDCs) for specific drug products and many of the drug vocabularies commonly used in pharmacy management and drug interaction software are additionally linked to RxNorm. RxNorm is a part of the Federal Medication Terminologies. For more information visit www.nlm.nih.gov. RxNorm is categorized as *Limited Production*.

3.7.4.3 *Immunizations (CVX & MVX)*

The Centers for Disease Control and Prevention provides a set of vaccine codes called the Codes for Vaccine Administered (CVX) and also a Manufacturer of Vaccine Code (MVX). These codes will be the standard terminology for vaccines. Codes can be founds here: http://www.cdc.gov/vaccines/programs/iis/stds/cvx.htm and manufacturers found here: http://www.cdc.gov/vaccines/programs/iis/stds/mvx.htm. CXV and MXV are categorized as *Full Production* for routine CDC reporting and *Testing* for HIE use..

3.7.5 Web Services Standards

The MiHIN will adopt the NHIN Messaging Platform Service Interface Specification v 1.9 which identifies the following web services standards:

Specification	**Version**
Simple Object Access Protocol	1.2
Hypertext Transfer Protocol (HTTP)	1.1
WS-Addressing	1.0
Message Transmission Optimization Mechanism (MTOM) binding for SOAP 1.1	1.0
Web Services Description Language (WSDL)	1.1
XML Schema	1.0
Universal Discovery and Description Interface (UDDI)	3.0.2

All Web Services are categorized as *Full Production*.

3.8 Security Architecture & Standards

The basis for the implementation of this security architecture is the NHIN Messaging Platform v1.9 and the HITSP Security and Privacy Technical Note TN900 v1.3. Most of the constructs we will use are described in TN900 and we will reference those constructs in each section below.

This specification is primarily concerned with the digital representations and mechanics of the security model. A trusted authority will issue digital certificates to all MiHIN nodes. These nodes use these digital certificates to construct encrypted and digitally signed messages between MiHIN nodes for sending, and to authenticate messages that are received. SAML tokens are used to transmit detailed information assertions about entities requesting information that are used to verify identity and check authorization and consent privileges. Auditable events are captured by each node and stored by that node. Auditable events can be retrieved using the NHIN Audit Log Query Service.

3.8.1 System (Node) Level Security

We will implement the HITSP T17 Secured Communication Channel Transaction for system (node) level security. The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing:

- Mutual node authentication to assure each node of the others' identity
- Transmission integrity to guard against improper information modification or destruction while in transit
- Transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes

This Secured Communication Channel Transaction supports application credentials, machine credentials, and user machines (user nodes). HITSP T17 uses the Authenticate Node Transaction from the IHE Audit Trail and Node Authentication (ATNA) Integration Profile. What follows is a basic description of how to establish a secure node. For more details see the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework, Volume 2, Section 3.19 (IHE ITI-TF-2).

ATNA Secure Nodes utilize Transport Layer Security (TLS) for secure communications over public networks. TLS uses a Public Key Infrastructure (PKI) based on X.509 digital certificates. Each secure node in the MiHIN must have a digital certificate issued by a trusted certificate authority. The MiHIN must either stand up a certificate issuing authority or contract with a third party to perform this service. Full use of ATNA is categorized as *Testing* but all the underlying standards (TLS, PKI, etc) are in *Full Production*.

3.8.2 Authorization

Users with access to patient data on the MiHIN must have been authorized for this access. Authorization will be governed by MiHIN policies and managed in a federated manner. Users will be authorized by local administrators at either the organization or HIE before being granted access credentials.

When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.

The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.

All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.

Authorization is more of an operational function governed by policy than a standard and thus it is not categorized.

3.8.3 Authentication

MiHIN will implement the IHE Cross-Enterprise User Assertion Profile (XUA) for providing a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting principal in a way that the receiver can make access decisions and generate the proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the users, as well as others that may have chosen to use a third party to perform the authentication.

The vast majority of the use-cases that MiHIN will implement rely on claims about an authenticated identity, which a SAML 2.0 Identity Assertion can provide. This is a mature standard produced by OASIS. The early XUA Profile development is focused on the two Web-Services transactions of the XDS.b Document Consumer Actor. XUA specifies that when a Cross-Enterprise User Assertion is

needed, these Web-Services transactions will additionally use the Web-Services Security header with a SAML 2.0 Token containing the identity Assertion. As with any IHE profile, the applications are not forbidden to use other methods of providing the principal (user) identity, providing that interoperability has been assured through some policy.

Authentication using XUA is categorized as *Testing*.

3.8.4 Access

For access control we will implement the HITSP TP20 Access Control Transaction Package. TP20 describes the interaction between the relevant parties in an access control decision as follows:

1. The Access Control Service (ACS) on the Service User side receives the Service User request and responds with a SAML assertion containing user authorizations and attributes.
2. To perform its function, the ACS may acquire additional attribute information related to user location, role, purpose of use, and requested resource requirements and actions.
3. The ACS on the Service Provider side is responsible for the parsing of assertions, evaluating the assertions against the security and privacy policy, and making and enforcing a decision on behalf of the Service Provider.
   - The security policy includes the rules regarding authorizations required to access a protected resource and additional security conditions (location, time of day, cardinality, separation of duty purpose, etc.) that constrain enforcement. Matching the user attributes against the security policy provides the means to determine if access is to be permitted.
   - The privacy policy includes the set of patient preferences, consent directives, and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement. This Transaction Package can retrieve the currently acknowledged consent directives using the Request Consent Directive functionality from HITSP/TP30 Manage Consent Directives.
4. The Service User sends the service request with specified attributes. Attributes include access control information (location, role, purpose of use, data sensitivity, etc.) necessary to make an access control decision.

Figure 3 provides a more detailed overview of the Access Control interactions that are described as part of this Transaction Package. This type of Access is categorized as *Testing* or *Limited Production*.

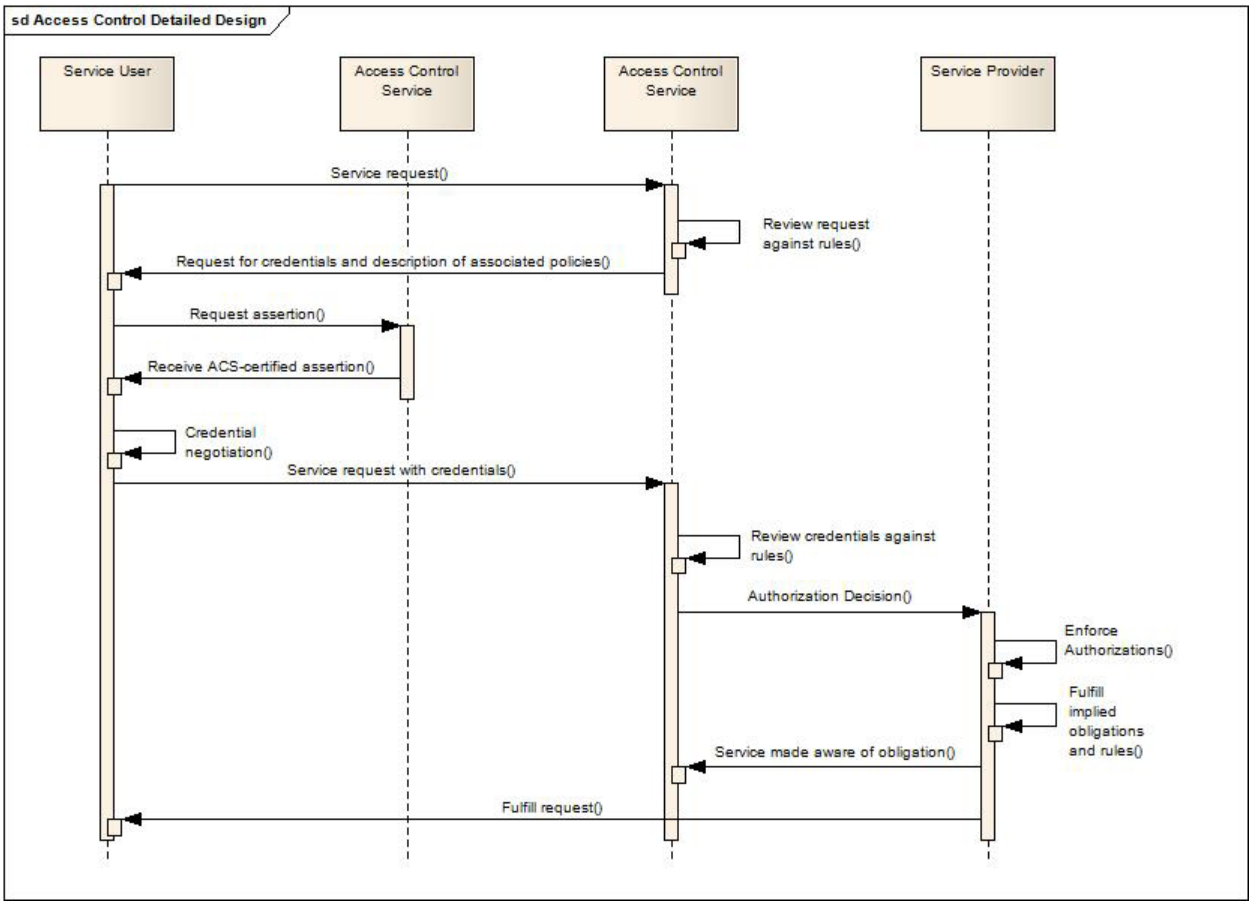


Figure 3: Detailed Access Control Interface Interaction Diagram

3.8.4.1 Cross-Enterprise Security and Privacy Authorization (XSPA)

This profile describes a framework of how SAML and standard candidates encompassed by cross-enterprise security and privacy authorization (XSPA) can be used to satisfy requirements pertaining to information-centric security within the healthcare community. Oasis has provided a specification for this called the Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare. It is the intention of the MiHIN to follow this specification as makes sense.

XSPA is categorized as *Emerging*.

3.8.4.2 Security Access Markup Language

SAML is the baseline authorization attribute exchange protocol that must be supported by use of this Technical Construct. SAML defines XML-based assertions and protocols, bindings, and profiles. SAML

refers to the general syntax and semantics of SAML authorization assertions as well as the protocol (e.g., syntax) used to request and transmit those assertions from one system entity to another. SAML provides authorization statements (e.g., assertions) and a query and response protocol (syntax) for exchanging statements between interfaces. The assertion is a payload in a query and response protocol (e.g., syntax). See HITSP/C19 Entity Identity Assertion for SAML used in the context of authentication 'identity' assertions.

SAML supports the following authorization assertion types:

- Attribute statement: An attribute statement asserts that a subject is associated with certain attributes used to make access control decisions for a particular security policy
- Authorization decision: An authorization decision statement asserts that a subjects request for access to the specified resource has resulted in one

For defining the mandatory and optional value sets required for interoperability, this Transaction Package supports the OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) SAML (U.S. realm) Profile. The XSPA profile of SAML provides access control information needed to make access control decisions for controlling security and functionality within and between healthcare Information Technology (IT) systems. XSPA has become more mature over the last year and should be seriously considered by MiHIN for implemention.

SAML alone is categorized as *Limited Production*.

3.8.4.3 Role Based Access Control

The MIHIN will support the HL7 v3 RBAC specification. At a minimum we expect to implement the following roles within the MiHIN:

1. Practitioner with access to clinical information and Break the Glass authority;
2. Practitioner with access to clinical information but no Break the Glass authority;
3. Non-Practitioner with access to clinical information;
4. Non-Practitioner with access to non-clinical information;
5. System administrators with access to non-clinical information; and
6. System administrators with access to clinical information in order to engage in public health reporting

The use of roles in general is categorized as *Full Production* but the specific implementation of HL7 v3 RBAC is categorized as *Testing*.

3.8.4.4 XACML Overview

XACML together with the WS-Trust Security Token Service define core capabilities of this construct's Access Control Service. XACML is a general purpose language for specifying access control policies. In XML terms, it defines a core schema with a namespace that can be used to express access control and authorization policies for XML objects. XACML provides features that make it possible to support a broad range of policies. It provides the capability to request a specified action within a system using a standardized syntax, and then receive one of four replies:

- Permit – action allowed
- Deny – action disallowed
- Indeterminate – error or incorrect/missing value prevents a decision
- Not Applicable – request cannot be processed

This construct specifies the use of OASIS XACML as a means to express Security and Privacy policy and obligations in a standards based, internally consistent way.

XACML is categorized as *Testing*

3.8.5 Auditing

The MiHIN must implement auditing of all transactions over the MiHIN infrastructure. To accomplish this goal we will follow the HITSP T15 Collect and Communicate Security Audit Trail Transaction. This specification describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.

The following are the requirements of the T15 specification:

1. Data to be collected/audited are identified
2. Data to be reported for audit are formatted
3. Data to be reported for audit are collected
4. Reports are provided for analysis of audit data
5. Audit data are retained for analysis
6. Automated responses are provided for audit data
7. Alerts and alarms are provided for security audit
8. Identity of users is recorded whenever a protected resource is accessed
9. Time of access is recorded whenever a protected resource is accessed
10. Identity of users is recorded whenever registration data are accessed
11. Time of access is recorded whenever registration data are accessed

HITSP T15 supports and references the Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication (IHE ATNA) Integration Profile to accomplish audit trail assurances in support of document-sharing and to support audit trails for message-based communications.

The Audit Trail needs to allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behavior, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). The audit trail must contain information so that questions can be answered such as:

- For some user: which patients' PHI was accessed?
- For some patient PHI: which users accessed it?
- What user authentication failures were reported?
- What node authentication failures were reported?

Auditing is categorized as *Full Production* in nearly all healthcare systems and HIE's. ATNA compliant auditing is categorized as *Limited Production*.

4 Interoperability with Stakeholders

This section of the document will tie together many of the previous sections and describe the interoperability of the MiHIN with various stakeholders who will be data sources and data consumers. For the purposes of this document we are defining only two interoperability models for the MiHIN: HIEs or the State of Michigan (SOM). In keeping with the principles of the MiHIN design these interoperability models do not assume any particular organizational structure, HIE architecture or vendor system. Rather they describe a set of required core services and interoperability standards for connecting to the backbone.

4.1 HIE Interoperability

This section of the MiHIN Architecture Plan will focus on the interoperability requirements for Community HIE organizations which will allow them to connect to the MiHIN Backbone. While this section will provide significant technical detail, this is an architecture plan and not a set of detailed specifications which are ready to implement. Those details must be worked out once the MiHIN vendors and infrastructure are known. This plan will not impose any requirements upon Community HIEs with regards to how they design and implement their internal system. Rather this plan will specify the requirements for Community HIEs to connect to and interoperate with the MiHIN Backbone.

To a large degree most details for how an HIE will interoperate with the MiHIN Backbone are described in the previous sections of this document. The goal here is to put the pieces together and describe the functional workflow and infrastructure that each HIE must implement. Early adopter stakeholders and the pilot HIE sites can integrate with the MiHIN by implementing the infrastructure and services described in this section and shown in Figure 4.

4.1.1 Infrastructure

Much of the core infrastructure necessary for integrating into the MiHIN backbone must be in place to establish an HIE. On top of those core components will be a gateway layer which includes the services for interoperability with the MiHIN Backbone. The core components are:

1. Messaging Gateway

   The messaging gateway or interface engine is the tool that provides network connections to data source and destination systems and can collect, translate and deliver messages. The messaging gateway is used inside the HIE and will be the infrastructure for sending and receiving messages from the MiHIN Backbone.

2. Enterprise Master Patient Index

   The EMPI is the system used for collecting patient identities and resolving identity conflicts across HIE member organizations. Connection to the MiHIN EMPI will be through a Subject Discovery service as described below.

3. Record Locator Service

   The Record Locator Service stores information on any data aggregated into the HIEs federated data repository. There are several models used for this purpose but a typical one is for each member organization to have an edge server for storing this data. The RLS can also look up this data based on a user query. The RLS will interact with the MiHIN through a Query for Documents service.

4. User Directory

   Along with other security services that are internal to the HIE a User Directory must be maintained in order to authenticate users. The User Directory will connect to the MiHIN through a security service described below.

4.1.2 Security

The HIE must develop security practices and services that meet the emerging security and consent policies of the MiHIN. These policies are under development by the Privacy and Security Workgroup and will be published before the Strategic and Operational Plans are submitted to the ONC for review.

While a final design of our security mechanisms are still in process the HIE will be expected to comply with polices and specifications around authorization, authentication, access and audit. Details of the proposed standards are discussed in section 3.8 Security Architecture & Standards.

Further details will come from our Vendor Technical Collaboration Team and during the implementation phase of the MiHIN pilots. Each HIE selected as a pilot site will be expected to actively participate in the development and implementation of the agreed upon standards and operational policies.

4.1.3 Transactions Workflow

The initial design of the MiHIN will implement fairly straightforward organization to organization (point to point) transactions. Due to this we will have varying standards required for these transactions based on the use case. We will require compliance with MiHIN Protocol Stack (MiPS) level 1 for all transactions.

4.1.3.1 Lab Orders and Results

For Lab Order and Results we will only make recommendations for levels two through four at this point. See sections 3.7.2.5 Lab Orders

and Result Transactions, 3.7.3.1 Lab Order Messages (HL7 2.5.1) and 3.7.3.2 Lab Result Messages (HL7 2.5.1) for more details.

4.1.3.2 Immunizations Reporting

For Immunizations Reporting we intend to work with the HIE pilot sites and their vendors to develop standards for levels two and three of the MiPS. While we still categorize the standards around Immunizations as *Emerging,* we want to work towards implementing those standards for reporting immunizations to the Michigan Care Improvement Registry (MCIR). The standards for Immunizations can be found in sections 3.7.2.7 Immunizations Reporting Transactions, 3.7.3.4 Immunizations Reporting Messages (C72), and 3.7.4.3 Immunizations (CVX & MVX).

4.1.4 Patient Update and Inquiry

4.1.4.1 Patient Identity Feed

The HIE must implement a service to push all new patients and patient updates to the MiHIN EMPI using the Patient Identity Feed standard described in section 3.7.2.1 Patient Identity Feed (PIX).

4.1.4.2 Subject Discovery

The HIE must implement a service to perform deterministic and probabilistic patient inquires from the MiHIN EMPI. These queries are described in section 3.7.2.2 Subject Discovery (IHE PIX & PDQ).

4.1.5 Query for Documents

The HIE must implement an XDS.b-compatible data repository to store documents to be shared with clinician users connected with another MiHIN HIE. The HIE must also implement a web service which is capable of notifying the MiHIN about new documents posted into the XDS.b repository and issuing and responding to XDS.b queries. These capabilities are described in section 3.7.2.3 Query for Documents (XDS.b and XCA) and 3.7.2.4 Document Notification (NAV).

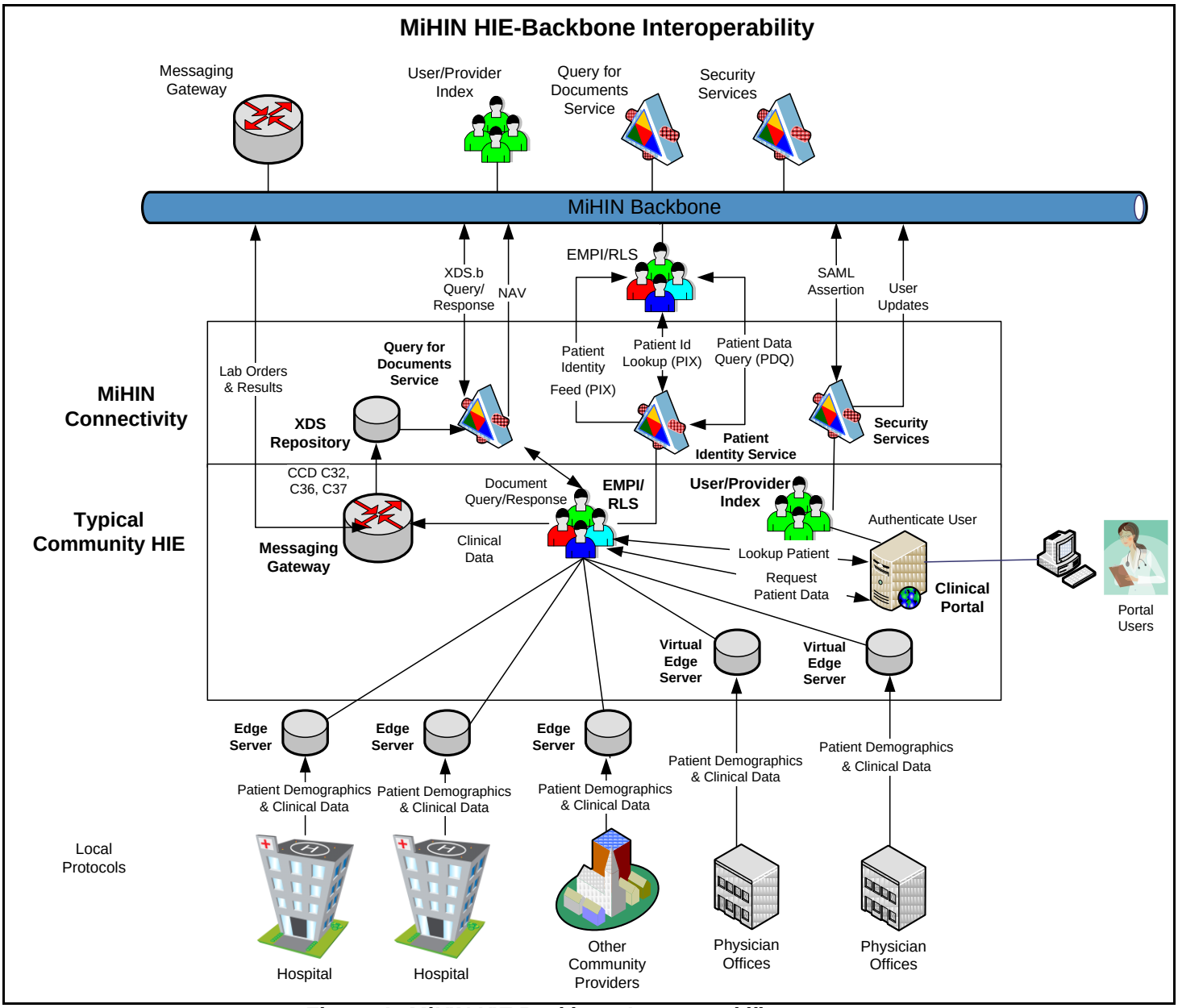


Figure 4 - MiHIN HIE-Backbone Interoperability

4.2 State of Michigan Systems Interoperability

4.2.1 Objectives

The State of Michigan government (SOM) plays multiple roles in relation to HIE/HIT. These roles can be categorized into the following:

4.2.1.1 Public Health

The SOM is the recipient of many required reports from multiple providers and entities. The SOM is also the originator of most Public

Health reports and functions. Systems from the Vital Records Department, Bureau of Epidemiology, and the Bureau of Laboratories are the main systems involved in these functions. The SOM also has interfaces to the CDC.

4.2.1.2 Health Care

The SOM handles care for several populations; The Department of Corrections provides care for Michigan's prison population and has its own EHR system. The SOM also runs several hospitals.

4.2.1.3 Medicare/Medicaid

The SOM, through the CHAMPS system, administers its Medicaid program. The SOM will also eventually be involved in the "meaningful use" quality reporting and determination of whether a provider meets the eligibility criteria.

4.2.1.4 Statistical Analysis and Data Warehousing

The Department of Community Health maintains and runs a large data warehouse that collects and reconciles information from multiple sources. It provides analytical and reporting services to multiple customers.

4.2.1.5 Laboratory Services

The SOM Bureau of Laboratories provides laboratory services to both SOM as well as other providers in Michigan.

Most of the systems used by SOM to carry out the functions summarized in the above list of roles were described in detail in the "State of Michigan Systems Technical Environment Analysis" document and thus will not be repeated here.

The objective of the architecture described here is to attempt to create a roadmap that will not only allow the SOM Systems to continue to fulfill the various roles they currently play, but to also create opportunities for synergy, enhanced functionality, and new functionality.

4.2.2 High Level Proposed Architecture

As can be seen from Figure 5, the best approach to achieving this objective is to create a State of Michigan Government Community HIE that encompasses most of the SOM Systems and that connects to the backbone through the required backbone standards. By following this model, the SOM is able to utilize the infrastructure components it currently owns as well as leverage existing systems interoperability to create a Community HIE that connects to the backbone.

Within this State HIE, certain infrastructure components related to HIE will need to be standardized. One important component is the MPI. Currently, every SOM system utilizes its own algorithm or system to match the identity of persons in the

system. This creates duplication of effort, inconsistency, and maintenance headaches. A single technology to deal with Master Data Management is a central component of this design. With a centralized MPI shown on Figure 5 as Patient Identity Service, the SOM system would utilize a single consistent technology. Similarly, since the State is the licensing body for all providers in Michigan, a service to match and validate providers can certainly be offered by the SOM.

4.2.3 Description of Proposed Architecture

4.2.3.1 Public Health Reporting

Currently, most reporting for public health purposes is done through dedicated Graphical User Interfaces (GUI's) which providers access. Some reporting is also done via flat files and HL7 either through dedicated VPN or through other secure internet connections. In the proposed architecture, all interaction of the Bureau of Epidemiology with external entities would be accomplished through the MiHIN backbone. As can be seen in Figure 5, this would require these external entities to issue, as appropriate, either a PIX/PDQ, or an XDS.b Query for Documents, or both. As an integration engine, Rhapsody would be used both as a Messaging Gateway and as a translation/normalization engine to insure Semantic Interoperability. As an example, Rhapsody can be used to convert Immunization Records from MCIR to the CCD C78 Immunization Document for storage into the XDS Repository.

4.2.3.2 SOM EHR/EMR Integration

Within the SOM, there are populations that receive care through the State. One major group is under the Department of Corrections, which runs the NextGen EMR. The State also runs several hospitals with their own EMR's. These would require integration into the SOM's HIE. Several infrastructure components can be used to do this such as Rhapsody and IBM WebSphere Process Server among others.

4.2.3.3 Medicare Claims Adjudication

The CHAMPS system is the SOM's system used for Medicaid enrollment, eligibility, reporting, provider services, managed care contract management, and claims payment. Since CHAMPS deals with many providers in Michigan, it should ideally connect directly to the backbone to provide the services required. CHAMPS is based on the eCAMS system from CNSI. Version 3.0 of eCAMS is reported to have XDS support among other HIE technologies. This would allow it to plug in directly into the backbone with minimal effort as "Payer".

4.2.3.4 Quality Improvement and Reporting

A cornerstone of "meaningful use" is the improvement of the quality of care. In order to achieve this goal, statistical information on treatment and the consequence of that treatment must be captured. The SOM's Data Warehouse already collects a considerable amount of information from multiple sources, mostly SOM related. The SOM Data Warehouse can potentially be used to collect additional information required for "Meaningful Use" reporting purposes. The Data Warehouse would most likely connect directly to the MiHIN backbone if it were to assume such a role. If that role is not envisioned for the SOM Data Warehouse or is envisioned for a later stage, then the Data Warehouse can be with the SOM HIE and would most likely continue to use existing data exchange capabilities and leverage potentially new ones facilitated by any new MiHIN technology acquired.

4.2.3.5 Bureau of Laboratories

The SOM Bureau of Laboratories performs several functions. The bulk of its functionality is administered (or will be soon) through STARLIMS, a state of the art laboratory system. For that functionality, the Bureau of Laboratories could be treated just like any other commercial reference laboratory and could either directly connect to the MiHIN backbone or through the SOM HIE. For the other functionality such as New Born Screening and Lead Screening a workflow similar to that of MCIR could be implemented within the SOM HIE.

4.2.3.6 Vital Records

Birth and Death registries can provide valuable information that the MiHIN can use to populate its EMPI. Reporting of these events is also useful in other contexts as is described in the "SOM Systems technical Environment Analysis" document. After legal issues are resolved in terms of disclosure of Vital Records information, the reporting of these events can easily be implemented through the use of Business Process orchestration software (the SOM has the IBM WebSphere Process Server and IBM WebSphere Message Broker as part of the Enterprise Architecture suite).

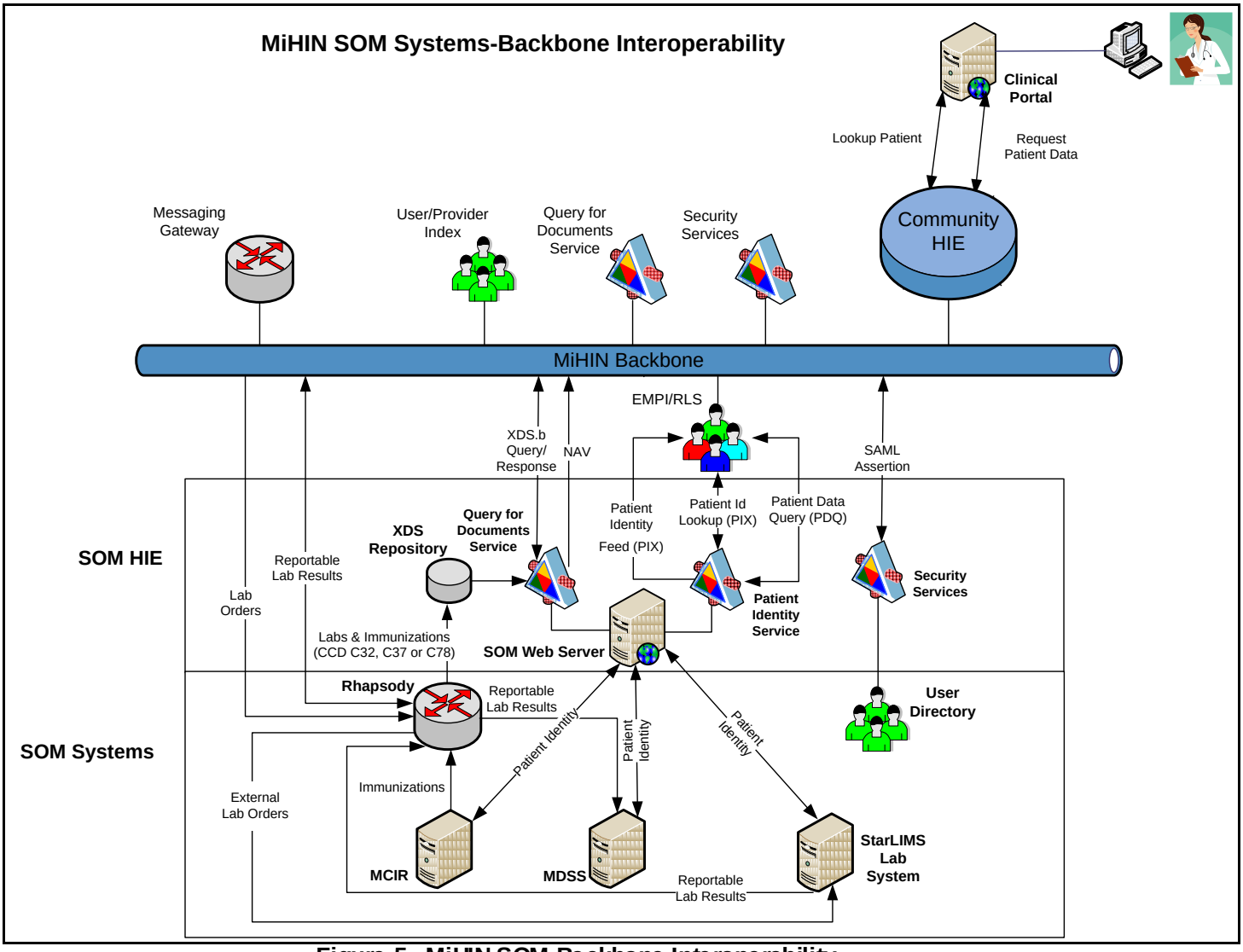


Figure 5 - MiHIN SOM-Backbone Interoperability

5 Risks and Benefits

This section will discuss the risks and benefits of the proposed technical architecture. Health Information Exchange (HIE) and interoperable gateway (or state backbone) systems are still immature technology markets. There are only a few working HIEs in the country and there are no live state-wide backbones that interconnect HIEs using a NHIN type model. The standards that we need to develop for the MiHIN are often just emerging. In addition there is significant risk that we will underestimate the scope of this project. To connect the vast majority of healthcare providers in Michigan could easily take ten or more years and cost hundreds of millions of dollars.

The risks that are encountered in this type of project are quite different than most projects that organizations take on. Recognizing the nature of the type of project this is can improve our chances for success and help mitigate risks. Our design choices were aided by referring to our guiding principles while completing this document.

5.1 Risks

5.1.1 Risk of Underestimating the Scope of the MiHIN

The MiHIN as designed is a network of networks. It is compelling to try and simplify the design in order to reduce costs and implement more quickly. But this will reduce the overall interoperability, services and value of the MiHIN in the long run. The MIHIN must be designed as an open network where any vendor can "plug in" and compete not on the basis of connectivity but on functionality, services and pricing.

5.1.2 Technology Risk

5.1.2.1 Architectural Model

Our choice of architectural model has risks as well as benefits. There are some risks in designing the MiHIN Backbone as a gateway between HIEs and modeling the Backbone as a NHIN compatible architecture. The primary risks are the immaturity of the backbone technology and the potential costs and time to build it.

5.1.2.2 Leveraging Existing Technology

Leveraging existing technology is both an opportunity and a risk. The goal in leveraging existing technology is to save money. But the key risk in trying to leverage technology is the complexity of integration. Please see section 3.5 Leveraging Existing Stakeholder Resources for more details.

5.1.2.3 Use of Standards

The use of standards is another area where there is both opportunity and risk. The opportunity is to create an interoperable network that allows any provider system to connect and share data. However since

most standards are still emerging and many vendor systems do not yet comply with the latest standards, the risk is the time it will take vendors to catch up and keep pace with the latest standards.

5.1.3 Implementation Risk

5.1.3.1 Focusing on the Backbone

For several reasons the MiHIN leadership has decided to focus on the MiHIN Backbone as its first phase of implementation. The primary risk in this approach is that the Backbone really cannot meet any of the ONC use cases without HIEs forming and contributing data. Thus the risk is that until HIEs connect ONC uses cases are not met.

5.1.3.2 Depending on HIEs to Form Independently

As noted above by focusing on the development of the Backbone the MiHIN cannot really demonstrate any capabilities without HIE's (Community or Private) forming and complying with the interoperability specifications described in section 4.1 HIE Interoperability.

But there is also a second risk of having HIEs form independently and that is one of value of the exchange. A typical model for HIE development is to focus on a particular geographic region. This is done because patients tend to obtain their care within a certain distance from their home or work. Thus most relevant healthcare transactions for that patient take place within that geographic region. Without a regional HIE focus it is quite likely that there will be many gaps in the data for patients which may impact clinician adoption.

5.1.3.3 Clinician Adoption

Clinician adoption of health care systems is based on a variety of factors from ease of use to functionality. But for HIE systems a key factor is the critical mass of both patients and completeness of data. Clinician adoption of HIE portals has been found to be very low when they either search for a patient and get few hits or find that much of the clinical data on a patient is missing.

5.2 Benefits

5.2.1 Architectural Model

Our choice of architectural model has significant benefits along with the risks discussed above. Its primary benefits are the open nature of the design which should improve interoperability and allow for significant growth and expansion in the future.

5.2.1.1 Interoperability

The architectural model of the MiHIN has a primary focus on interoperability, scalability and extensibility. Our focus on standards may slow us down a bit in the short run but will allow for much greater interoperability in the long term. By designing the Backbone as an ESB we allow for new services to be deployed as long as they comply with standards.

The design also balances the highly standards-based Backbone with the organic formation of HIEs that can "bend the rules" for aggregating data as necessary. This model keeps the Backbone purely standards-based while still allowing data to be aggregated at the HIE level. We envision that standards will evolve and migrate to HIEs and then to EHRs and other clinical systems over time. This model allows that to happen in a logical manner.

5.2.1.2 Scalability and Extensibility

Two key guiding principles of the MiHIN architecture are scalability and extensibility. Scalability is the capability of the architecture to add more users, transactions or other volumes of work easily. Extensibility is the capability of the architecture to add new functions or services easily.

We address scalability in our two-tier design of the MiHIN Backbone and HIEs. By aggregating and normalizing data at the HIE level we keep much of the traffic between healthcare providers at that level.

We address extensibility by our ESB design concept which allows for state-wide shared services to be developed and shared among HIEs.

5.2.2 Building Incrementally

Another key benefit to the MiHIN design is the ability to build much of it incrementally. While there are some core components which must all be in place before any successful HIE connection, the implementation of use cases can and should occur incrementally.

The core components necessary are the ESB structure, EMPI and RLS, Messaging Gateway, Security Services, Provider Directory and Query for Documents Service. These need to be implemented together and be in place before other services can be deployed.

But the rest of the HIE connections and administrative and clinical functions (use cases) can and should be implemented incrementally. Our current recommendation is to start with two (or more) pilot HIEs and implement two use cases. The architecture is designed to add more HIEs or more use cases as time and money allow.

Appendix A
Functional Use Cases

Use Case: Deliver lab results

Narrative: The results for a laboratory test are sent to the designated recipients in a structured format suitable for consumption by an electronic system. This includes clinical chemistry, hematology, serology and microbiology, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, and pulmonary ventilator management.

HIE Service Priority Classification: Electronic clinical laboratory ordering and results delivery

Supported Meaningful Use Objective: Incorporate clinical lab-test results into EHR as structured data

Additional Supported Use Cases/Objective: Harmonized Electronic Health Record (Laboratory Result Reporting) (AHIC)

Data: Clinical, results of laboratory tests (test, result, patient)

As Is Strategy: Results delivered via fax machine via automated systems.

As Is Workflow:

1. Clinical service provider performs requested test; creates a proprietary clinical result
2. Laboratory information system (LIS) transmits proprietary results via fax to listed recipients
3. Recipients manually process lab results

To Be Strategy: Results delivered electronically via automated systems.

To Be Workflow:

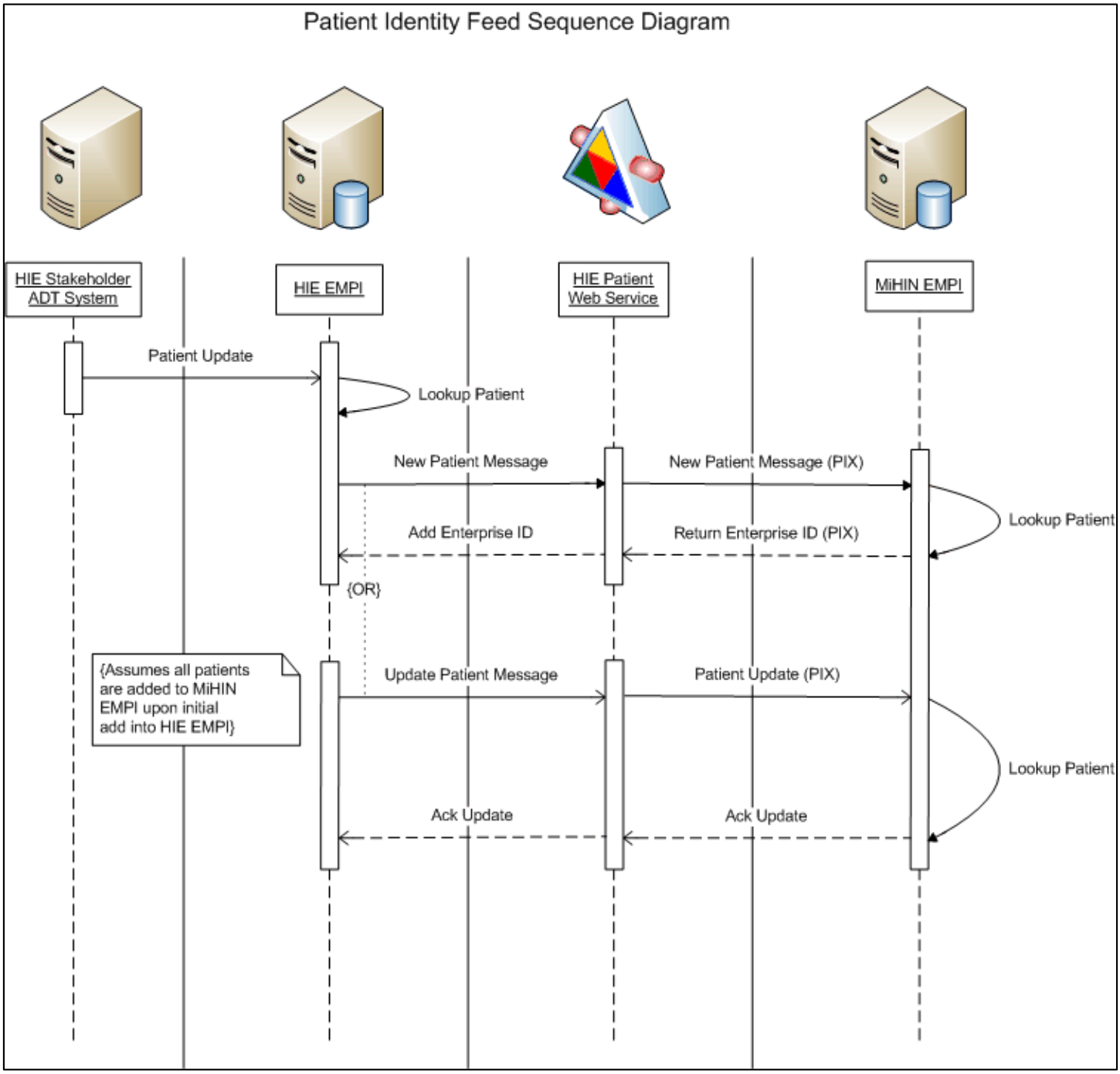
1. Clinical service provider performs requested test; creates a standards-based clinical result
2. Laboratory information system (LIS) transmits structured results to results delivery service
3. Results delivery service verifies ordering physician and maps to appropriate electronic destination
4. Result electronically delivered to ordering physician's EHR
5. Physician authenticates to their EHR and retrieves electronic result

Required Content Exchange and Vocabulary Standards: LOINC

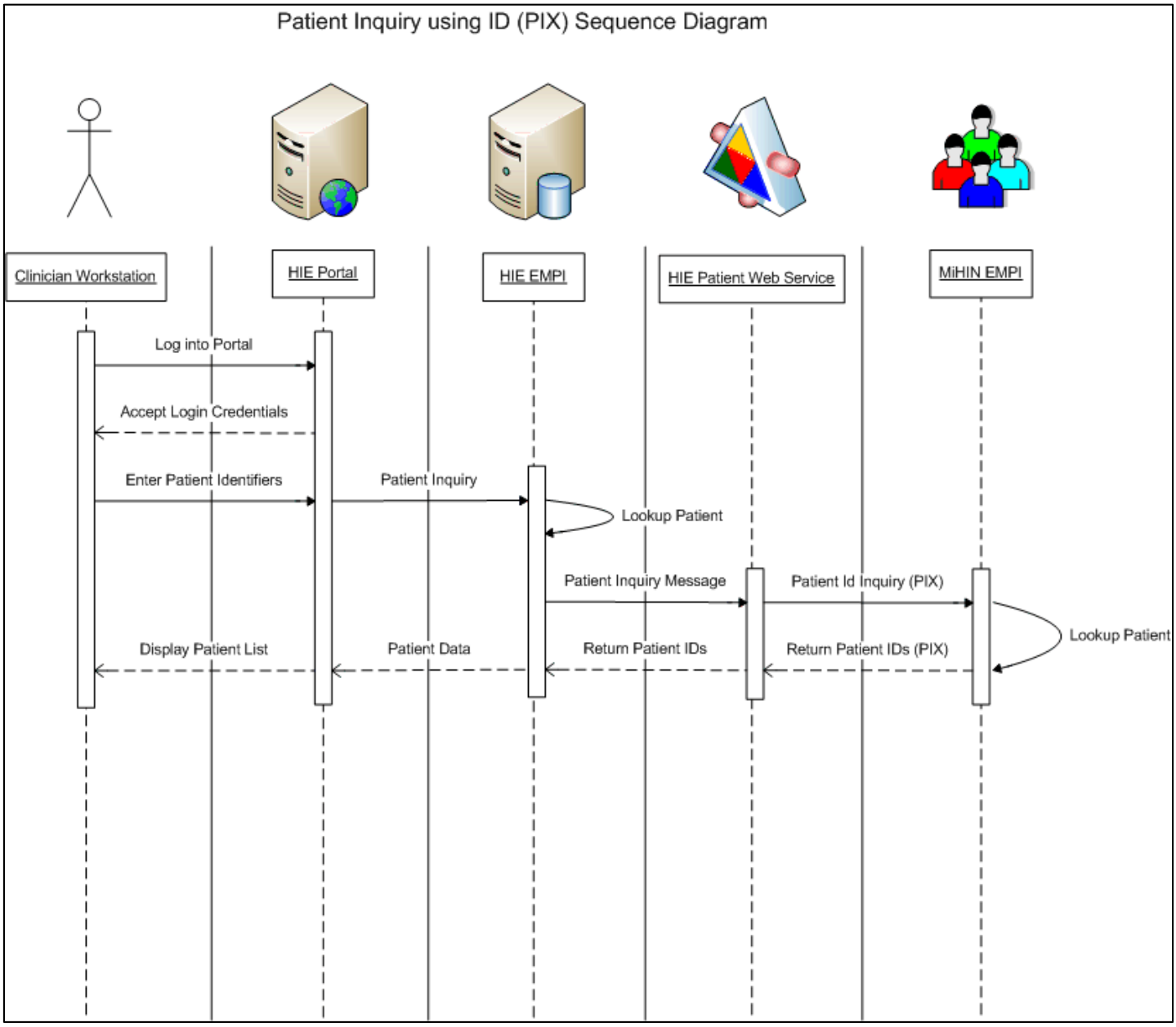
Required Security Use Cases: transport, audit

Actors: Provider, Laboratory (Clinical service provider), LIS, results delivery service

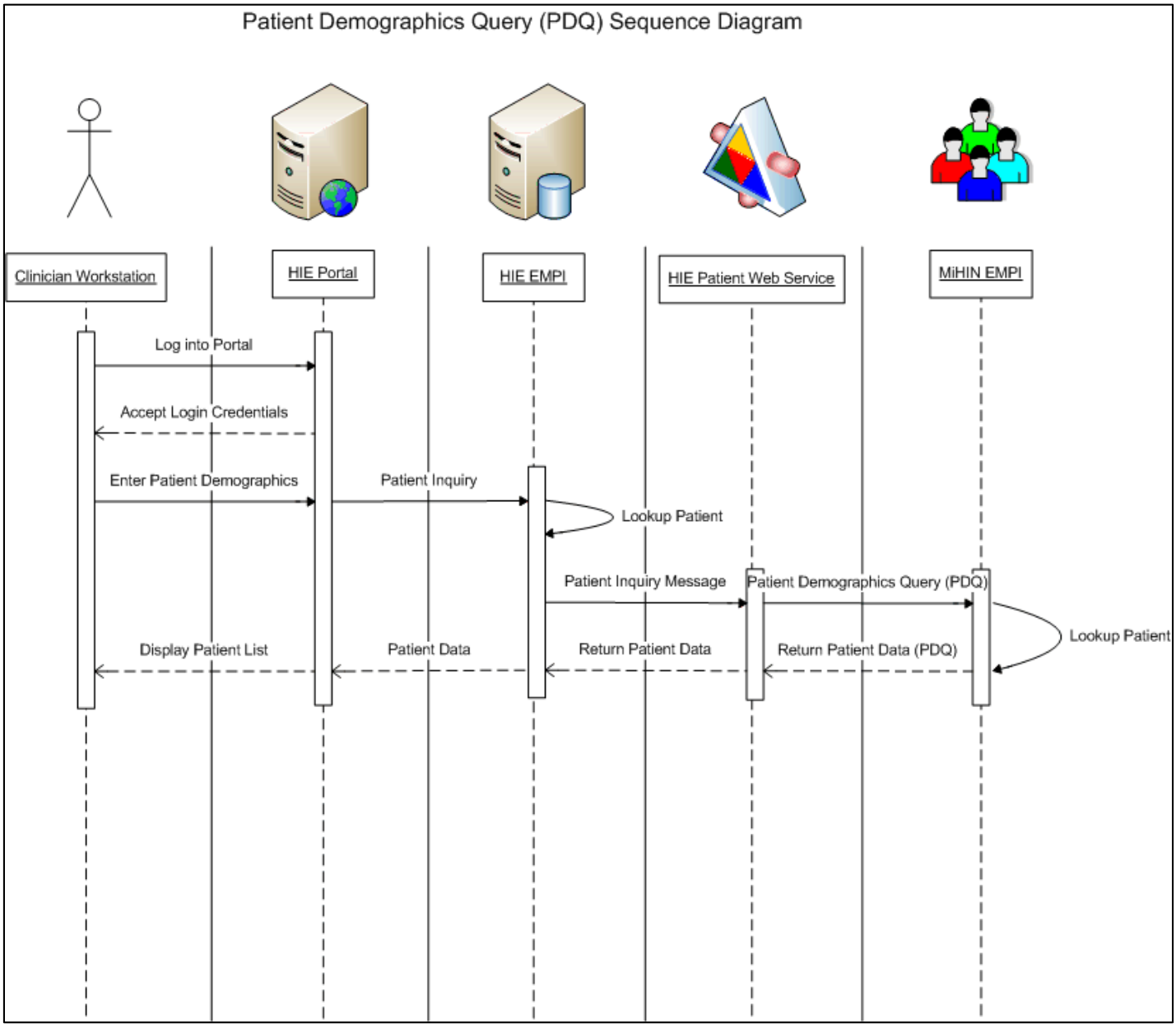
Appendix B
Technical Use Cases



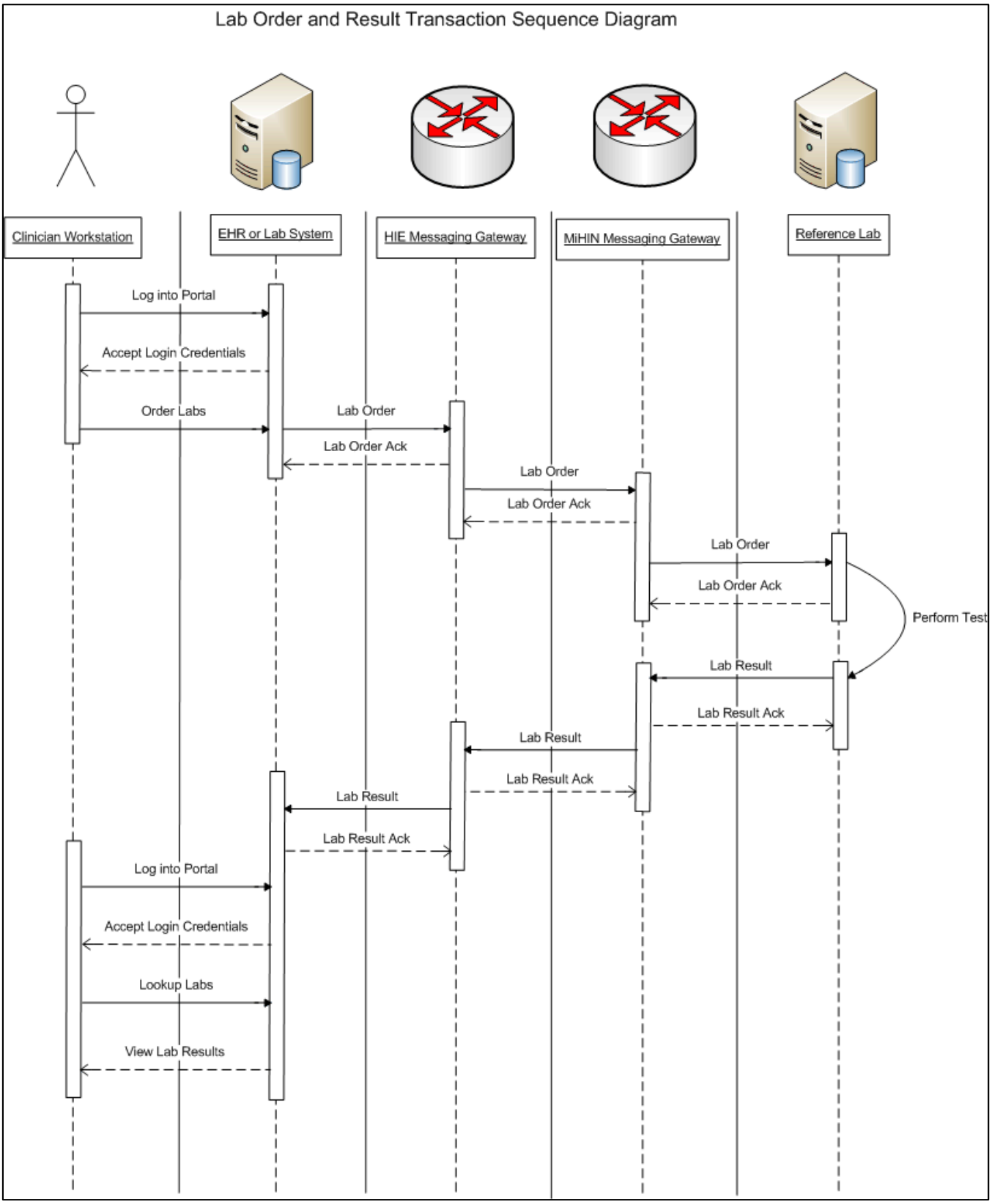
Appendix B
Technical Use Cases

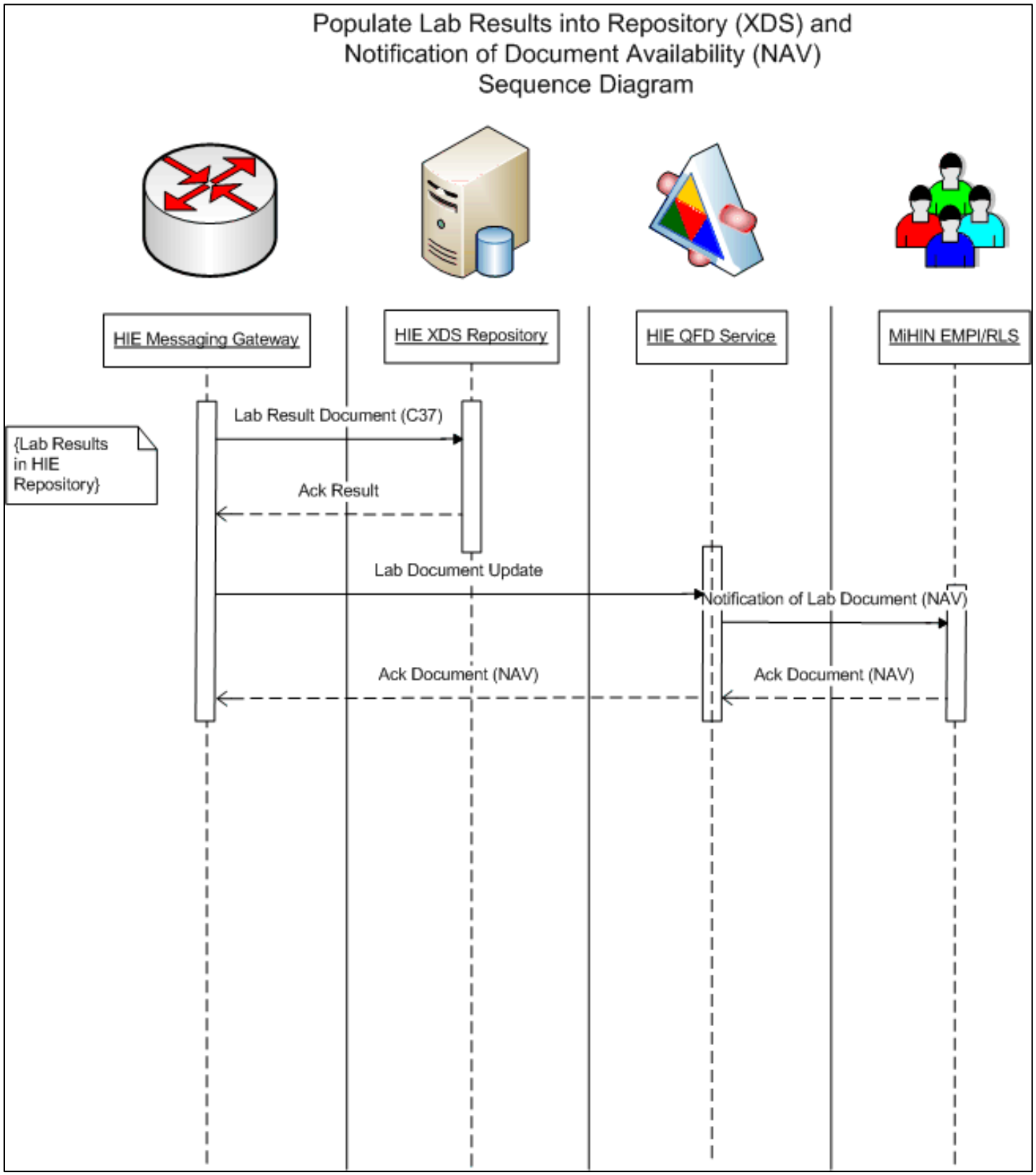


Appendix B
Technical Use Cases

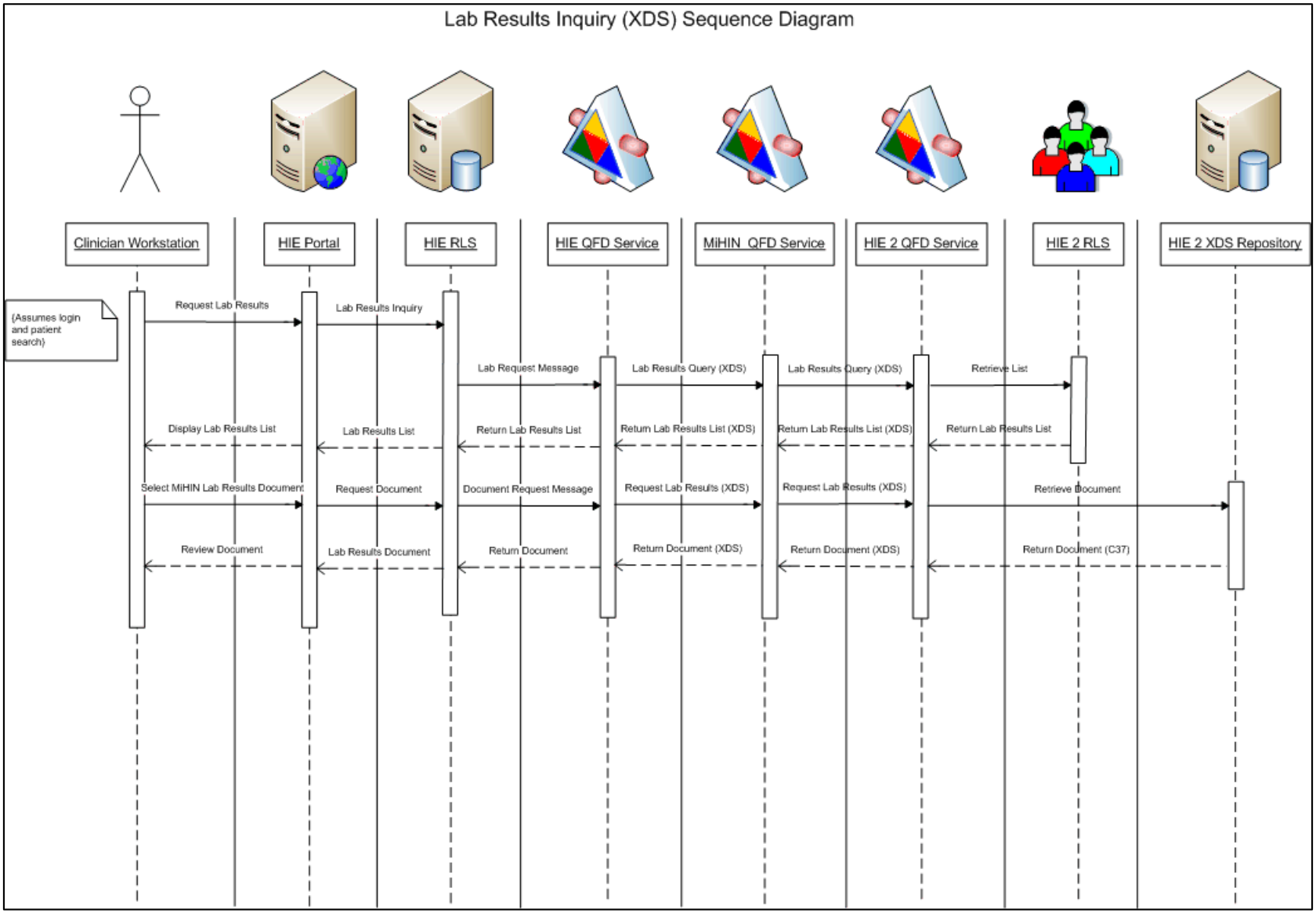


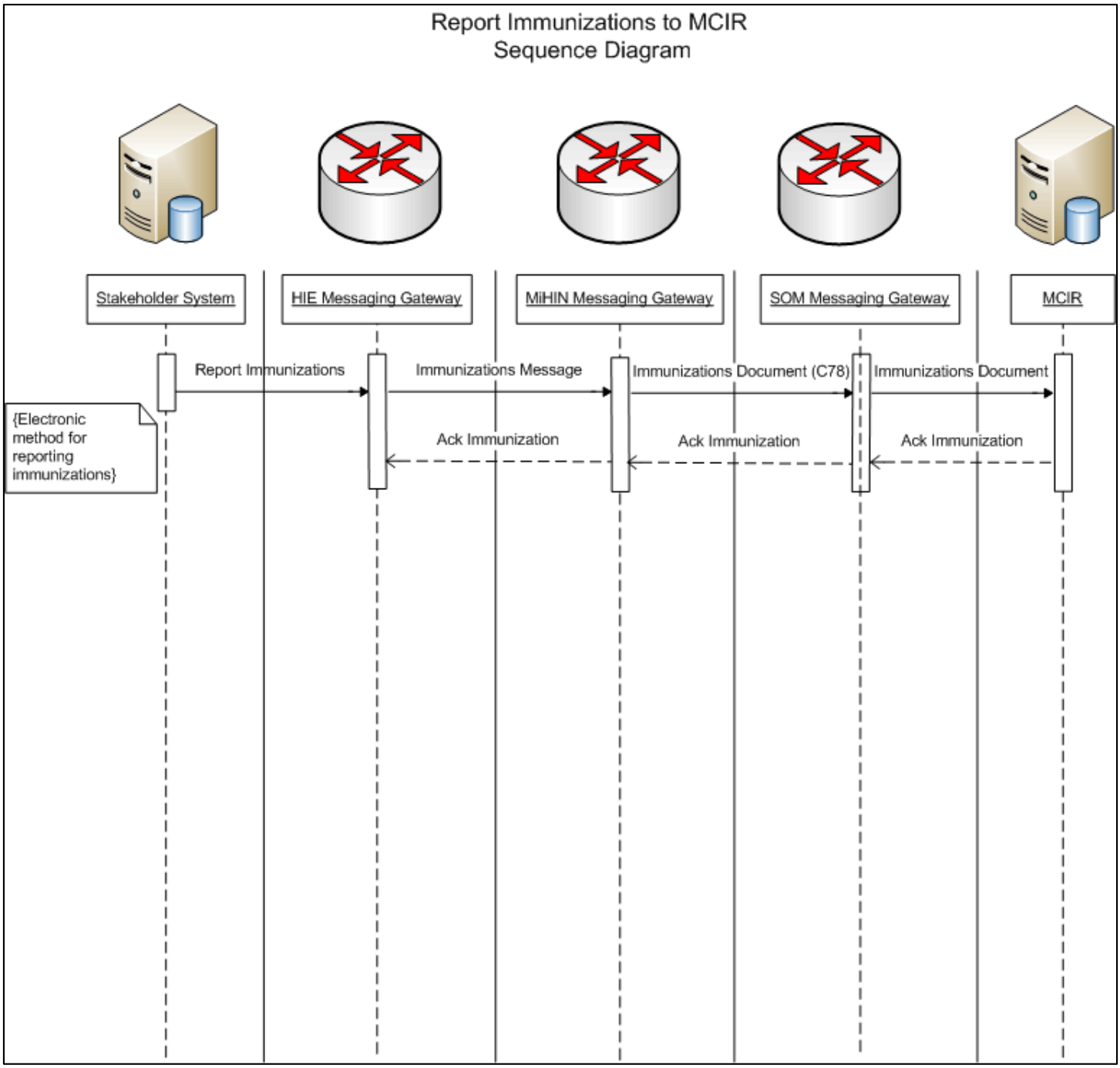
Appendix B
Technical Use Cases

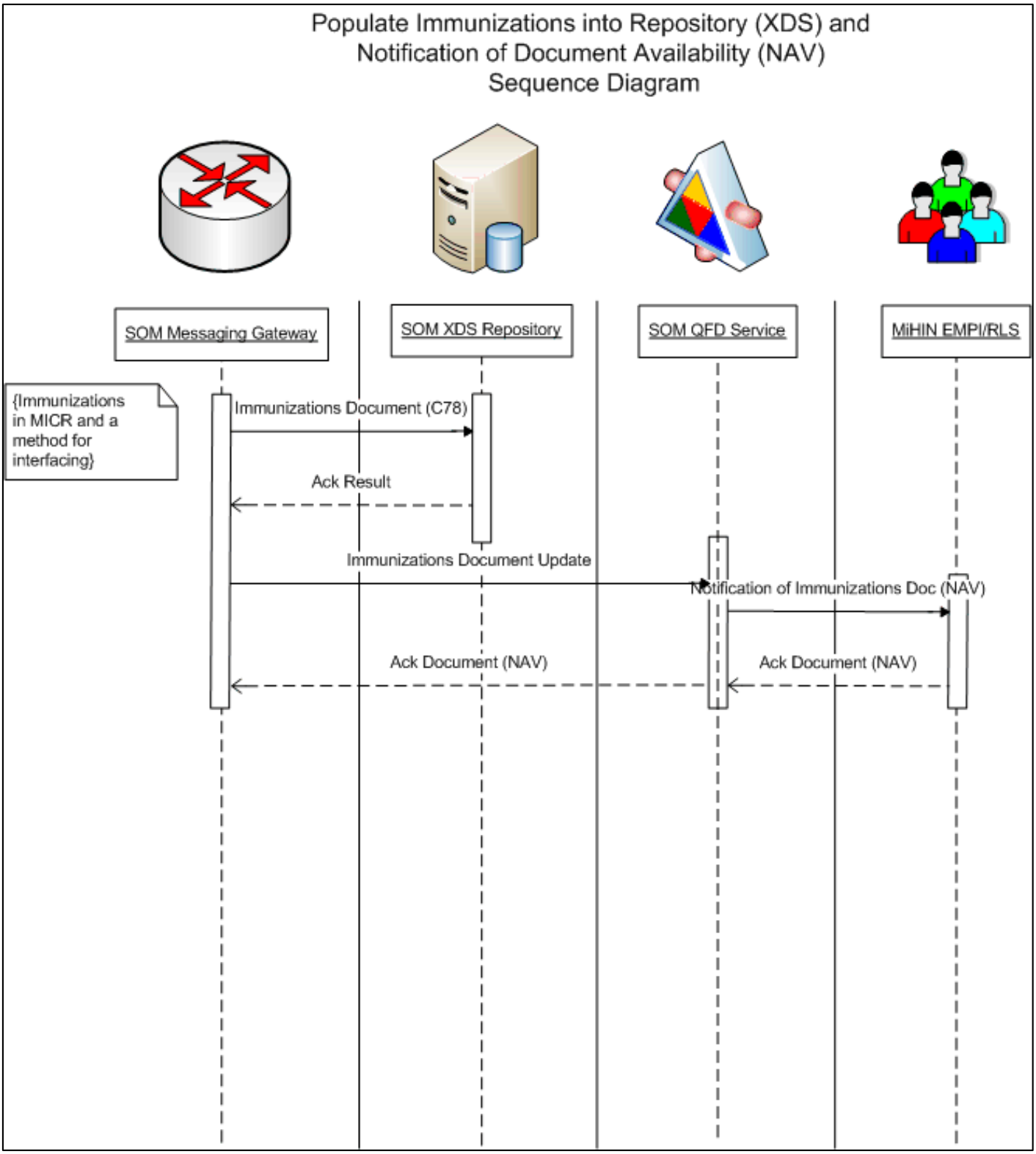



Populate Lab Results into Repository (XDS) and
Notification of Document Availability (NAV)
Sequence Diagram
HIE Messaging Gateway
HIE XDS Repository
HIE QFD Service
MiHIN EMPI/RLS
{Lab Results in HIE Repository}
Lab Result Document (C37)
Ack Result
Lab Document Update
Notification of Lab Document (NAV)
Ack Document (NAV)
Ack Document (NAV)

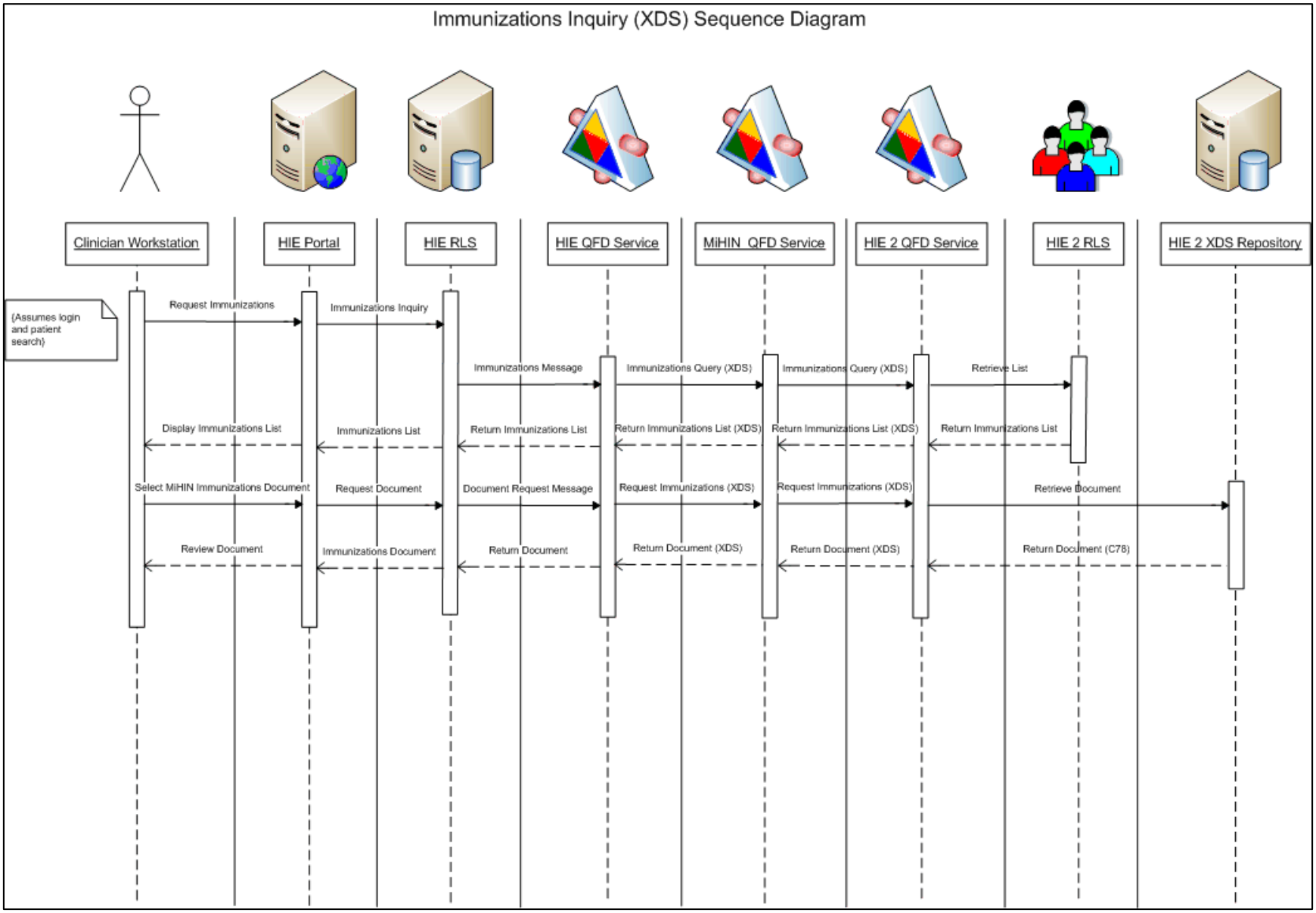
Appendix B
Technical Use Cases




Report Immunizations to MCIR
Sequence Diagram
Stakeholder System
HIE Messaging Gateway
MiHIN Messaging Gateway
SOM Messaging Gateway
MCIR
Report Immunizations
Immunizations Message
Immunizations Document (C78)
Immunizations Document
Ack Immunization
Ack Immunization
Ack Immunization
{Electronic method for reporting immunizations}


Populate Immunizations into Repository (XDS) and
Notification of Document Availability (NAV)
Sequence Diagram
SOM Messaging Gateway
SOM XDS Repository
SOM QFD Service
MiHIN EMPI/RLS
{Immunizations in MICR and a method for interfacing}
Immunizations Document (C78)
Ack Result
Immunizations Document Update
Notification of Immunizations Doc (NAV)
Ack Document (NAV)
Ack Document (NAV)

Appendix B
Technical Use Cases



Appendix C
Contractual Requirements

Contractual Requirements

- A mechanism for providing and managing identity and credentials of all users of the exchange.

  This is addressed in the Security section of the plan.

- A cross-enterprise master data management solution, a record locator service and messaging gateway(s).

  This is addressed in the Core Components section of the plan.

- Develop, manage and review responses to a Request for Information (RFI).

  This is addressed in a separate document which is a review of the vendor RFI responses.

- Technical specifications of each technical component and service, including interfaces within the architecture.

  This is addressed in several sections of the document including Data Exchange Components, Technical Infrastructure Components and MiHIN Backbone Services.

- How the architecture shall comply with existing and evolving security and privacy standards and policies.

  See the section on Security. MiHIN security and consent policies will be developed by the spring of 2010.

- How the architecture incorporates or uses existing statewide technical assets and resources identified in the early adopters' analysis and the SOM systems analysis. Identify and detail the use of specific statewide and technical assets and resources

  This is covered in section 3.5 Leveraging Existing Stakeholder Resources.

- How the architecture shall provide the highest level of security and privacy.

  This is addressed in the Security section of the plan.

- How the architecture conforms to the evolving national HIT/HIE standards, frameworks, specifications, and best practices, including CCHIT, HITSP and the successor's standards and specifications.

  This will be addressed in the Standards section of the plan.

Appendix C
Contractual Requirements

- How the architecture shall bridge and interoperate with developing regional HIE's, SOM systems, interoperable EHRs, health systems, payers, health plans and other health care organizations in Michigan.

  This is addressed in the HIE Interoperability section of the plan.

- How the architecture shall bridge and interoperate with the Nationwide Health Information Network (NHIN).

  This is addressed in the NHIN Connectivity section under Data Exchange Components.

- The architecture's ability to accommodate variations and improvements in technical, legal, and business standards and practices.

  This is addressed throughout the plan.

- How the State of Michigan may expand the use of the HIE infrastructure components and technologies, such as, the Master Data Management solutions to streamline and improve SOM business processes enterprise wide.

  Much of this was already covered in Milestone 3 the State of Michigan Systems Analysis deliverable. This document described the opportunities for most of the healthcare-related systems at the state with the implementation of the MiHIN. However more details will be included in section 4.2 State of Michigan Systems Interoperability where we will describe the functional integration of the early SOM systems, MCIR, MDSS and StarLIMS.

- Risks and benefits, taking into consideration how the architecture accounts for the information acquired in the early adopters and SOM systems analysis.

  This is addressed in section 5 Risks and Benefits