



## Agenda

<b>Title / Purpose:</b>	MiHIN Technical Workgroup Meeting		
<b>Meeting Date:</b>	Feb22, 2010	<b>Facilitator:</b>	Mike Gagnon
<b>Place:</b>	Conf Call and Web-ex	<b>Time:</b>	9:00 AM – 11:00 noon
		<b>Conf Call #:</b>	1-888-394-8197 Passcode: 869479
		<b>Web Link</b>	<a href="https://premconf.webex.com/premconf/j.php?ED=102412862&amp;UID=0">https://premconf.webex.com/premconf/j.php?ED=102412862&amp;UID=0</a> Password: mihin-tech9

<b>Topic 1:</b>	<b>Attendance, Review and Approve Minutes</b>	<b>10 Min</b>
Materials:	Meeting Minutes	
Presenter:	Ken Theis and Rick Warren	
<b>Topic 2:</b>	<b>State HIE Announcement Overview</b>	<b>10 Min</b>
Materials:	State HIE Announcement Overview presentation	
Presenter:	Mike Gagnon	
<b>Topic 3:</b>	<b>Review of Questions for other Workgroups</b>	<b>20 Min</b>
Materials:	Preliminary list of questions for each workgroup	
Presenter:	Mike Gagnon	
<b>Topic 4:</b>	<b>Review Vendor Presentations</b>	<b>30 Min</b>
Materials:	None	
Presenter:	Mike Gagnon	
<b>Topic 5:</b>	<b>Review of MiHIN Security Use Cases</b>	<b>10 Min</b>
Materials:	None	
Presenter:	Mike Gagnon	
<b>Topic 6:</b>	<b>Review of VTCT Work</b>	<b>30 Min</b>
Materials:	None	
Presenter:	Mike Gagnon	
<b>Topic 7:</b>	<b>Public Comment Period</b>	<b>10 Min</b>



## Meeting Minutes

<b>Title / Purpose:</b>	MiHIN Technical Workgroup Meeting		
<b>Meeting Date:</b>	Feb 8, 2010	<b>Facilitator:</b>	Mike Gagnon
<b>Place:</b>	Conf Call and Web-ex	<b>Time:</b>	9:00–11:00 AM
		<b>Conf Call #:</b>	1-888-394-8197 Passcode: 869479
		<b>Web Link</b>	<a href="https://premconf.webex.com/premconf/j.php?ED=102412762&amp;UID=0">https://premconf.webex.com/premconf/j.php?ED=102412762&amp;UID=0</a> Password: mihin-tech8

Topic 1:	Attendance, Review and Approve Minutes	10 Min
Materials:	Meeting Minutes	
Presenter:	Ken Theis and Rick Warren	
Topic 2:	Developing Questions for other Workgroups	50 Min
Materials:	Preliminary list of questions for each workgroup	
Presenter:	Mike Gagnon	
Topic 3:	Review Vendor Presentations	30 Min
Materials:	None	
Presenter:	Mike Gagnon	
Topic 4:	Review of Vendor Technical Collaboration Team work	20 Min
Materials:	None	
Presenter:	Mike Gagnon	
Topic 4:	Public Comment Period	10 Min

<b>DISCUSSION</b>	<b>Topic 1: Attendance, Review and Approve Minutes</b>
Voting members Marcus Cheatham, Bill Riley, Bruce Weigand, Mark Tuthill and Dan Stross are absent.	
Motion to approve meeting minutes is seconded and meeting minutes are approved.	
Sharon asked the workgroup if they preferred an in-person meeting on Feb 22. The group decided they preferred web-ex so the next meeting will not be at the Kellogg Center as stated in the Master Schedule and meeting invite; it will be web-ex.	
Sharon reminded the workgroup there are 4 meetings left. Feb 22, Mar 8, Mar 22, and Apr 5.	



ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Send email reminding the workgroup that the next meeting is not at the Kellogg Center.	Sharon	2-12-10

DISCUSSION	Topic 2: <b>Developing Questions for other Workgroups</b>
------------	---

Mike comments that we are framing these questions on the fact that we have to develop a strategy and operational plan. The questions need to be framed to learn how to start, what will we do first, and what are the questions we need all the workgroups to answer.

**Governance:**

George Boresma comments that the questions for the Governance WG are too open-ended and it will be difficult for that workgroup to make a decision based on the way the questions are worded. There are many other questions could be reworded, made more specific, or we could add our assumptions. For example:

1. Assumption 1.a – The message gateway, RLS, and MPI and potentially the provider directory would be designed in such a way that the HIE could make use of it (even if it is not done immediately).
2. Assumption 1.b - approved. The state is not implementing a state-sponsored HIE.
3. Assumption 1.c – A State-sponsored HIE is not affordable right now and there is no support structure in place. It is a future consideration. Doug Dietzman asks about state-systems collectively mimicing the HIE and the answer is yes, that the state will develop their own internal HIE that allows the state systems to plug in. This is what our terminology refers to as the SOM HIE as opposed to a community, regional, or private HIE. The SOM HIE supports the purpose of creating a structure for data sharing.
4. Assumption 1.d – The two or more pilot sites being discussed are the community, private or regional HIEs. These sites would have to be formed, ready to go, and have some sort of funding in order to make themselves able to connect.
5. Assumption 1.e. Meaningful use outlined by the Business Operations Workgroup will be the order in which the functionality is implemented over the length of time that grant funding is available.
6. Assumption 1.f. Change this assumption to clearly refer to the scope of the grant vs scope of the MiHIN.
7. Assumption 1.g – comes from research on how many connections you would need; early costs and budget figures for vendors; if personnel costs were not too high, etc. MiHIN could make it within the range of where the ARRA funds would be according to the initial budget in the Grant application. Rick W. says what about on-going costs of one option vs another. Ongoing costs – 20 mil, a little high but not too far off.
8. MPI - Shaun Grannis has commented on the strong value of the Provider Directory. Mike asked George if the State has a provider credentialing system that can be leveraged in building a Provider Directory. – Laura – yes they have a license registry administered by the DCH. It could be a user directory and MiHIN could leverage it for access credentials. Action Item maybe it's another application within the SOM that we need to look at. There is also a health alert system (MHAN - Michigan Health Alert Network ) that is role-based so there is a possibility that it could be leveraged for role-based privacy and security.
9. Question # 2- Remove the first sentence and change the rest to ask: Will Governance own the resolution of patient ids? Will they actively try to resolve patient identity? Will there be web-based tools and identities across communities that will match? Can we push that to a queue for a person to resolve? This is a detailed vision but is important to know these answers. Most matching algorithms are 'tune-able'; they are good but not fool-proof and there are on-going activities.
10. These questions could include data normalization as well but another thing we were assuming is that we are not going to do normalization in the backbone. Getting someone else's normalization tool could be difficult. Better to determine what data to normalize first. Suggestions to normalize first is labs and medications. Harvey Organek comments that for meaningful use for 2011, we will be standardized and it is just a matter of adopting it. If sending and receiving systems know then we do not have to use someone else's normalization tool. To illustrate, in Vermont a physician could order a test from any lab and the system would convert the data to a standard form (LOINC). We could push for standards up front but that might not be a requirement. (This needs further explanation.)
11. Question 3 – we said we would not look to leverage existing components, like the SOM message gateway, even though it could be made to work in the MiHIN. In the long run we could look at it that way but we will

not start out that way. The time to consider what we would have to do to 'make it work' could be when we need additional components to factor in redundancy.

12. Someone asks, What does Question #4 mean? If the SOM is not the hosting site or the owner of the backbone, will there still be a vision for a data warehouse? Rick Warren asks about cost and regional governance .
13. Bullet 3 – Value-added networks are not being replaced by MiHIN but we are looking for them to be governed by the MiHIN. Ernie notes that we do not want to exclude or replace any of these networks. For one reason, they are a natural pathway for reporting and gathering metrics. If people are not comfortable with one vendor providing the capability, then maybe the new governance entity could coordinate this. Ernie says we have to figure out how these networks become value-added components first.
14. Question 5 – For stakeholders that are national players, how are we going to approach connections to other states? For example, if Trinity can connect to the NHIN, we could use that functionality but we would lose functionality in other areas. So the question is, how to resolve state backbone to state backbone connections? Does the HIE have to plug into multiple states? What we would want is for the HIE backbone connection to be able to plug into some other state's NHIN-connected backbone without re-writing the middleware.
15. Question 6 – Maybe they will issue an RFP for pilots sites. They must consider readiness, etc. They might choose in pairs because the level of exchange of patient information between the two is critical for demonstrating value.
16. Question 7 – This is a question for P&S.

#### P&S

1. Question 1 – Add the following: The RLS could pull in metadata on the fly (e.g., provider, date and document type) and the question to the P&S workgroup is “What is too much information where it could become a privacy issue? For example, mental health document types could become a privacy issue. Mike explains that the idea is to index returning meta data in a google-like user interface, but how much information is too much information when you are also protecting the privacy of a patient's health information.
2. Question 2 - Add the following: The Technical workgroup is not concerned with the specifics of the policy, just how complicated it is to implement.
3. Question 4 – The WG will need more guidance on this question. Specifically, what we are asking is “How fine do we want the roles to be?” For example, provider with break the glass, provider without break the glass, etc. There are four roles suggested in the Architecture Design document and Mike asks if the workgroup thinks there are others. Someone suggests that this should not be too prescriptive because it will depend on workflow and responsibilities could be team-based. We do not want to hamper those types of process design and improvement.
4. Add the question- Will we be able to store and access the information that tells us a certain individual has received a HIPPA violation in a certain role? Will we be able to prevent that individual from performing the same violation in the future?
5. Question 7 - How will security be implemented down to HIE level? 2-factor authentication has its positives but also alot of cost. The question is more about what the minimum security policy will be. The MiHIN minimum security policy will become requirement for connecting to another organization through the MiHIN. The NHIN policy states that the more stringent organization can obtain information the less stringent organization but not the other way around. How stringent we want to policy to be is also an adoption issue.
6. Question 8 - Add the question: “How much public comment will the MiHIN PCO or governing entity take or ask for?”
7. Question 9 – More specific questions could be, “How do we certify that policies, actions, requirements are being met?” “How does the MiHIN track that audits are being performed?”
8. One suggestion is to make audit logs available on a website and let people know they can find out who accessed their records. Mike mentioned a study where compliance was the affect of having an accessible audit log.



ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Update Questions for Other Workgroups documents	Sharon	2-12-10
Determine if the group can we agree with the assumption on data normalization not being done on the Backbone.	Mike	2-22-10

<b>DISCUSSION</b>	<b>Topic 3: Review Vendor Presentations</b>	
-------------------	---	--

Vendor presentations – We are almost with the vendor presentations. CSC is rescheuling and Harris will be later this week.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None,		

<b>DISCUSSION</b>	<b>Topic 4: Review Vendor Collaboration Team work</b>	
-------------------	---	--

The team will break into subteams to tackle the topics and we are working with PCO Team to assign who will facilitate the sub-teams. Mike listed 3 of the 4 topics the VTCT will specifically help us with right away. The first is an Architecture Overview and Mike will lead that sub-team. Then, there is “How we will implement security?” and Mike and Rick Brady will lead that sub-team. The third topic is HIE interoperability (i.e., middleware, subject discovery, QFD, XDS repositories, etc.) Those are the key topics but there will be others.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

<b>DISCUSSION</b>	<b>Topic 5: Public Comment Period</b>	
-------------------	---------------------------------------	--

Steve Summers asks for update on VTCT, specifically if Initiate, Eclipsys, and Meditech have signed up. Mike answers that Initiate has but not Eclipsys, and Meditech. EHR vendors are important but of the most important right now. And they can still be nominated or nominate themselves.

Deb Mosher asks how do HIEs know MiHIN users are adhering to P&S standards, HIPAA, etc?

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

### Attendance list

- George Boersma                      MiHIN PCO
- Rick Brady                              MiHIN PCO - Consulting Team
- Nathan Bunker                         Member
- Brad Carlson                            Member
- Don Carne                                Member
- Lee Castiglioni                         Member
- Kelly Coyle                               Member
- Doug Dietzman                         Voting Member
- Darrell Dontje                         Member
- Cynthia Edwards                       Member
- Doug Fenbert                            Voting Member
- Christine Fend                         Member
- Chris Foster                             General Public
- John Hazewinkel                       Member
- Pat Klima                                 Member



- Troy Lane Member
- Tom Lauzon Voting Member
- Linda McCardel Member
- Paul G. Miller Voting Member
- Robert Moerland Member
- Deb Mosher Member
- Amber Murphy MiHIN PCO – Consulting Team
- Samer Naser MiHIN PCO – Consulting Team
- Laura Rappleye MiHIN PCO
- Randall Rothfuss Member
- Steve Summers Member
- Rick Warren Co-chair
- Ernie Yoder Voting Member



## News Release

FOR IMMEDIATE RELEASE  
Friday, February 12, 2010

Contact: HHS Press Office  
(202) 690-6343

### **Sebelius, Solis Announce Nearly \$1 Billion Recovery Act Investment in Advancing Use of Health IT, Training Workers for Health Jobs of the Future**

**Grant Awards to Help Make Health IT Available to Over 100,000 Health Providers by 2014, Support Tens of Thousands of Jobs Nationwide**

- 40 States were awarded a State HIE Cooperative Agreement
- 32 Regional HIT Extension Centers were awarded
- In Michigan:
  - State HIE Cooperative Agreement: \$14,993,085
  - Regional Health IT Extension Center: \$19,619,990

# Top 11 State HIE Awards

Awards were given based on a formula that includes a base allocation for every applicant (\$4 million) and then an equity adjustment was added to account for: number of primary care physicians, number of acute care hospitals, number of medically underserved and rural providers.

1	California Health and Human Services Agency	\$38,752,536
2	New York eHealth Collaborative Inc.	\$22,364,782
3	Illinois Department of Health care and Family Services	\$18,837,639
4	Commonwealth of Pennsylvania	\$17,140,446
5	Michigan Department of Health	\$14,993,085
6	Ohio Health Information Partnership LLC	\$14,872,199
7	Missouri Dept of Social Services	\$13,765,040
8	Georgia Department of Community Health	\$13,003,003
9	North Carolina Department of State Treasurer	\$12,950,860
10	State of Tennessee	\$11,664,580
11	Virginia Department of Health	\$11,613,537

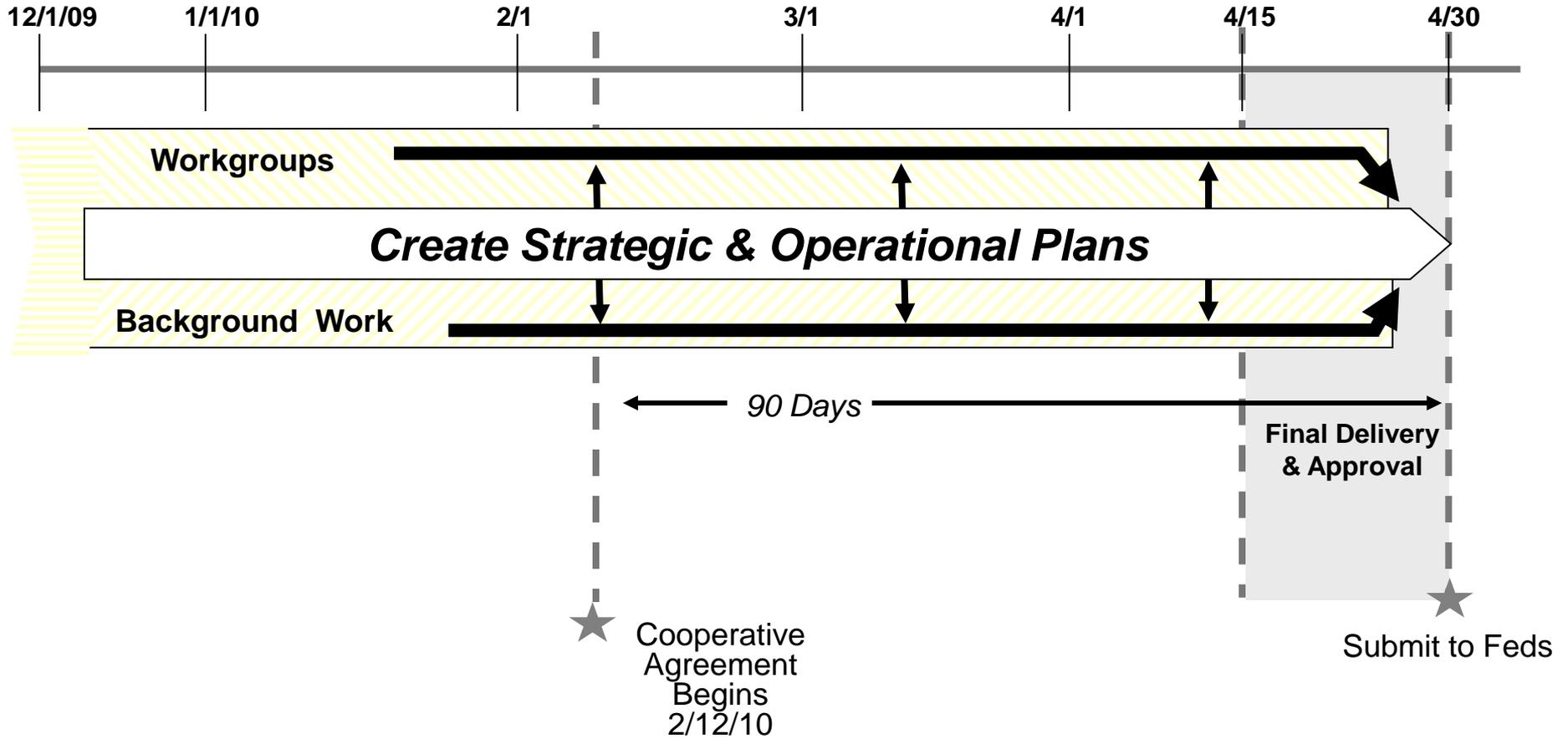
# State HIE Cooperative Agreement

- \$14,993,085
- \$1,690,912 required in matching funds
- 4 year cooperative agreement
- Cap of \$1,000,000 for planning
- Remainder of agreement must go toward statewide HIE and nationwide HIE



# Timeline

**Goal:** Submit Strategic & Operational Plans by **April 30, 2010**



## 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 some number of pilot projects that includes connecting HIEs and implementing use cases. Here are our assumptions about this:
  - a. The backbone will include a messaging gateway, EMPI, RLS, Provider Directory, and Security Services. These services would be designed in such a way that the HIE could make use of it (even if it is not done immediately).
  - 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. A State-sponsored HIE is not affordable right now and there is no support structure in place. It is a future consideration. The state will develop their own internal HIE that allows the state systems to plug in. This is what our terminology refers to as the SOM HIE, as opposed to a 'state-sponsored' community, regional, or private HIE.
  - d. We will integrate two or more HIEs as pilot sites and consider assisting them with some matching funds from the ARRA grant. The two or more pilot sites being discussed would be the community, private or regional HIEs. These sites would have to be formed, ready to go, and have some sort of funding in order to connect themselves to the backbone.
  - e. We will implement use cases in these pilot sites that exercise all components of the backbone (messaging, subject discovery and query for documents). The order in which the functionality is implemented is outlined in the Meaningful Use from the Business Operations Workgroup and that would be over the length of time that grant funding is available.
  - f. Except for the pilots that are within the scope of the ARRA grant, there will not be any state or ARRA support for community or private HIEs. Community or Private HIEs will be implemented by stakeholder organizations. . The MiHIN backbone could be implemented within the range of the ARRA funds with some matching amount, according to the initial budget in the Grant application. This assumption is based on research on how many connections are needed; early costs and budget figures for vendors; if personnel costs were not too high, etc.
  
2. Will Governance own the resolution of patient ids? Will Governance set policy to actively try to resolve patient identity? Will there be web-based tools and identities across communities that will match? Can we push that to a queue for a person to resolve?

- a. We are not going to do normalization in the backbone.
3. We believe that the MiHIN Governance and the State of Michigan should encourage or require the existing value-added networks in the state to be opened to all stakeholder organizations and follow the MiHIN standards for security and interoperability. Value-added networks are not being replaced by MiHIN but we are looking for them to be governed by the MiHIN.

We have to figure out how these networks become value-added components first.

During our analysis we uncovered four such networks; the claims network, the ePrescribing network; the Michigan Health Connect lab results delivery network and the Joint Venture Hospital Lab repository which is used mostly for quality reporting.

- a. With the current scope of the Michigan claims networks we believe that they could be organized into a network similar to the New England Healthcare Exchange Network (NEHEN), perhaps governed by the MiHIN, but not a function of the MiHIN Backbone.
  - b. With the Meaningful Use requirements for EHR systems and due to the business value we believe the existing ePrescribing 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.
  - c. In Vermont there exists a system which allows any connected lab to order a test from any other connected lab. The current systems in Michigan (Michigan Health Connect) are not quite up to this level but are moving in that direction and the MiHIN Governance should encourage this model.
  - d. 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.
  - e. .
  - f. The MiHIN will not look to leverage existing components, like the SOM message gateway, even though it could be made to work in the MiHIN. In the long run we could look at it that way but we will not start out that way. The time to consider what we would have to do to 'make it work' could be when we need additional components to factor in redundancy.
4. The State of Michigan Data Warehouse would most likely connect directly to the MiHIN backbone if the state were to host the MiHIN. However, if the SOM is not the hosting site or the owner of the backbone, will there still be a vision for a data warehouse?
    - a. If that role is not envisioned for the SOM Data Warehouse or is envisioned for a later stage, then the Data Warehouse can be incorporated into 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.

- b. What would be the regional governance? Cost?
5. The concept and technical ability to provide patient information to other states is included in the architecture design. National vendors will try to plug into other states. But is this functionality going to be part of the MiHIN? How are we going to approach connections to other states? For example, if Trinity can connect to the NHIN, we could we use that functionality but we would lose functionality in other areas.

From a technology perspective, how are we going to resolve state backbone to state backbone connections? Does the HIE have to plug into multiple states? Can the HIE backbone connection plug into some other state's NHIN-connected backbone without re-writing the middleware?

6. Will there be a formal request process to determine which regional HIEs should be considered to participate in a pilot? What will the criteria be? Will an RFP be issued for pilots sites? They must consider readiness and might choose in pairs because the level of exchange of patient information between the two is critical for demonstrating value.

## Questions for MiHIN Privacy and Security Workgroup

1. The RLS contains meta-data about documents that are stored in the federated data bases (edge servers or XDS repositories). The RLS could pull in metadata on the fly (e.g., provider, date and document type) and the question to the P&S workgroup is What data can or should be stored in the Record Locator Service on the MiHIN? “What is too much information where it could become a privacy issue? For example, mental health document types could become a privacy issue. If the idea is to index returning meta data in a goggle-like user interface, how much information is too much information when the protection of a patient’s privacy of health information is concerned.
2. Will we be implementing opt-in or opt-out consent for collecting data into the HIEs and MiHIN? The Technical workgroup is not concerned with the specifics of the policy, just how complicated it is to implement.
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. How fine do we want to establish authorization, users and roles for role-based security? For example, provider with break the glass, provider without break the glass, etc. There are four roles suggested in the Architecture Design document. Should there be others? How deeply should the Technical WG go as far as?
5. Is consent granted to a provider for a period of time for a particular episode?
6. Background checks (or flags) for HIPAA violations
7. How will security policies be implemented down to the HIE level? What should the minimum security policy will be? MiHIN will develop a minimum set but also conform to any stronger policies at the local HIE level.

The MiHIN minimum security policy will become requirement for connecting to another organization through the MiHIN. The NHIN policy states that the more stringent organization can obtain information from the less stringent organization but not the other way around. How stringent we want to policy to be is also an adoption issue.

- a. 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. 2-factor authentication could impede rapid adoption/participation. Would this be a requirement of the HIE before they connect to the MiHIN?
8. How will privacy and security policies will it be communicated to the public? How much public comment will the MiHIN PCO or governing entity take or ask for?

9. How do we certify that policies, actions, requirements are being met?" "How does the MiHIN track that audits are being performed? What method will be used to certify that HIEs are adhering to P&S standards, HIPPA, etc.?
- 10.
11. What will be the policy on patients knowing who accessed their records? What information will be needed going from the HIE to the backbone when it comes to a breach in privacy and security policies? How will the rules be followed when there is a security breach (i.e., someone obtains unauthorized access to a patients records)?
12. Will we be able to store and access the information that tells us a certain individual has received a HIPPA violation in a certain role? Will we be able to prevent that individual from performing the same violation in the future?

## Security Use Cases

This is a simplification of IHE/HITSP security theory.

Definitions:

MiHIN: the state-wide backbone

MiHIN node: A single logical system with a valid Internet FQDN that acts on behalf of an organization to provide connectivity for Health Information Exchange.

The MiHIN will provide or specify three categories of security services: authentication and authorization, transport, and audit.

Authentication: two types of authentication are in scope: node and user

Node Authentication: Nodes will be mutually authenticated via PKI certificates. The certificate infrastructure will be managed by the MiHIN Certificate Authority. Participating nodes on the MiHIN will authenticate their respective certificates by inquiring to the MiHIN. As nodes join the MiHIN, they will be issued the appropriate certificate(s). When their participation has ended, their certificate will be revoked. Revocation will have immediate effect since there is only one level of authentication (MiHIN to nodes, no sub-nodes)

User Authentication: Users will be authenticated to a MiHIN node in a fashion acceptable to MiHIN policy and as in daily use at the participating node. The node will assert, on behalf of the user, the request for a service and give the role of the user (security assertion). All MiHIN nodes will represent roles according to the HL7 Permissions Catalog. This may be accomplished at the MiHIN node level by mapping internal roles/users to the MiHIN standardized HL7 Permissions Catalog roles, or may be accomplished natively by implementing the HL7 Permissions Catalog roles in your IAM solution or at the application level. The node will present the security assertion in SAML. The MiHIN will process the security assertion through its policy enforcement point. The policy enforcement point can be instantiated by being placed as a proxy for all MiHIN service requests, either a stand-alone filter in front of the MiHIN hardware/software, or as a logical layer in the application server system. All requests for MiHIN services will first pass through the policy enforcement point. The policy enforcement point will check its database of allowed transactions (called a policy definition point). The policies are stored in a format compliant with the XACML standard. If the role and type of transaction are allowed, the service request is authorized, and the proceeds to the MiHIN service it was intended.

Enforcement of patient consent is enforced at the MiHIN level through inclusion of XACML policies in the policy definition point covering patient. XACML is formatted in XML. If the consent is simply "opt-in or opt-out", the patient id will be checked for policies in the policy definition point that would not allow access to the role presented.

If consent allows for denial for named individuals, the policy definition point will contain many more policies to include requestor consent policies. A policy definition point could be instantiated through a

database that store XML documents natively. A request from the policy enforcement point could be handles as a database transaction. You may want to allow other policy enforcement points (non-MiHIN) to access the policy definition point. In that case, you would want to provide the policy definition point as a service and it would likely contain a policy governing its own use by a non-MiHIN policy enforcement point.

Break the glass functionality is implemented by having a “break-the-glass” role which will allow authentication and authorization for any service request. The use of the break-the-glass role will obviously required a detailed audit after the fact. The MiHIN node has the duty to document the user and reason for invocation of the break-the-glass role.

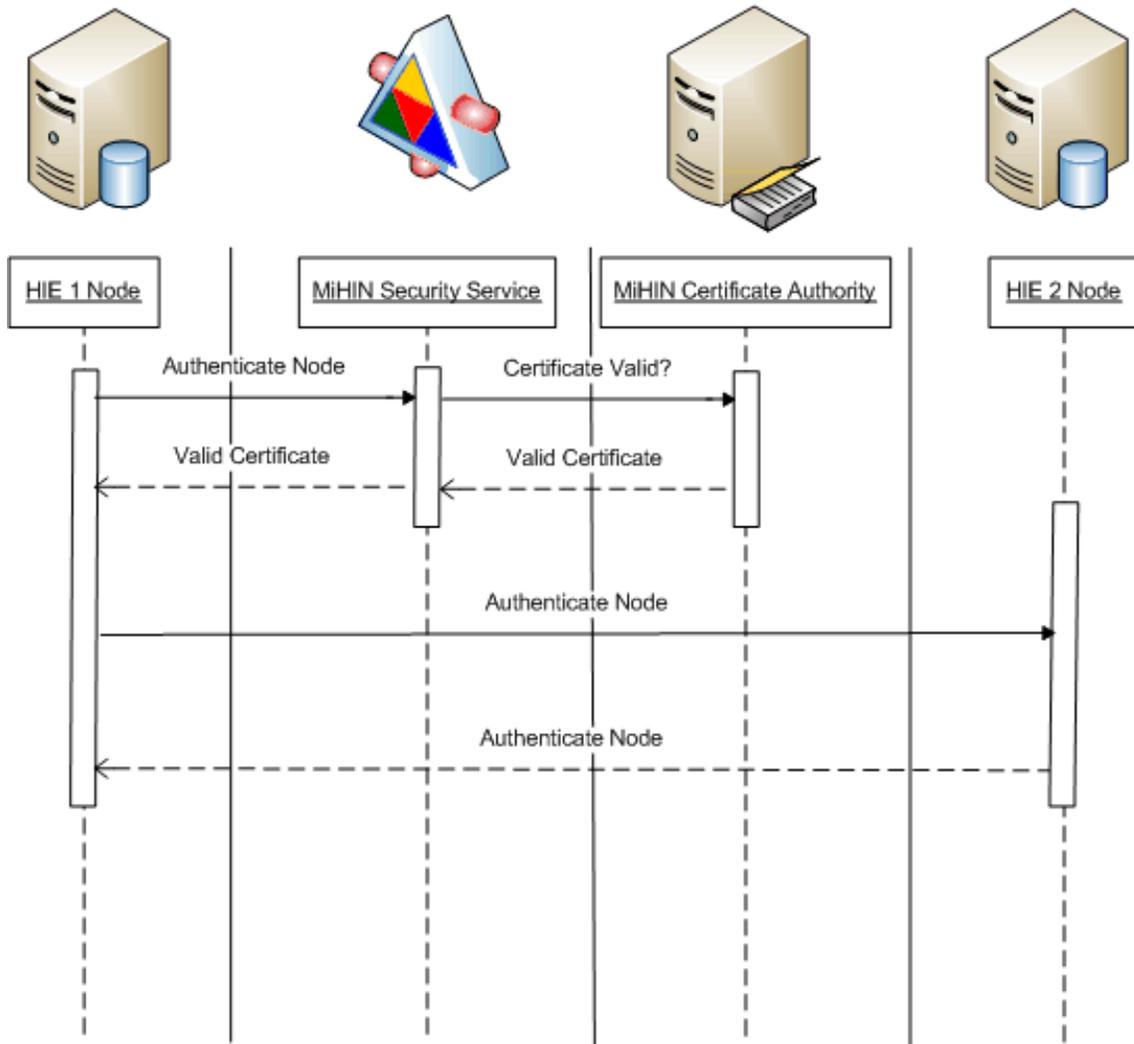
Transport: All transactions occur over TLS. All modern web servers can perform TLS transactions. When configuring your Application Servers web server, set it to only perform TLS transactions. The certificate to use in the TLS connection is the PKI certificate outlined in Node Authentication section.

Logging: All service requests are logged in compliance with the ATNA standard. At the MiHIN level, requesting node, organization, service requested, role asserted, success or failure (denial) are logged with a UTC format (ISO 8601) time stamp. At the requesting MiHIN node, the following are logged, along with UTC format time stamps:

- (1) date and time of the event (in UTC format)
- (2) the identity and component of the internal system (e.g. software component, hardware component) where the request originated
- (3) The internal user ID of request
- (4) The role of requester
- (5) type of event (including: service and patient identifier when relevant)
- (6) subject identity (e.g. user identity)
- (7) the outcome (success or failure) of the event.

If ever a need arises to check an event, the logs from the MiHIN node, the internal systems represented by the MiHIN node, and the MiHIN logs can all be coordinated via the UTC timestamps to allow forensics.

## Secure Node Authentication Sequence Diagram



### User Authentication for Service Sequence Diagram

