



Privacy and Security Sub Work Group Agenda

Meeting Date:	Tuesday March 16, 2010	Facilitator:	Kelly Coyle
Place:	Web-ex	Web-ex Information:	https://premconf.webex.com/premconf/j.php?ED=102879307&UID=0 password: mihin-ps7
Time:	9:00 – 11:00 AM	Teleconference #:	1-888-3948197 passcode 869479

Topic 1:	Housekeeping and Logistics Roll Call of Voting Members <i>For both voting and public work group members- when you sign in on the web ex, please use your first and last name so we know who is participating</i> Approval of meeting minutes Review of Meeting Schedule- timeline Questions
Topic 2	Finish up review of Access, Audit, Authorization, Authentication policies
Topic 3	Review policies for <ul style="list-style-type: none"> • Breach • Audit
: Topic 4:	Recommendations for Direction of MiHIN Privacy and Security Governing Body <ul style="list-style-type: none"> • Structure • Role of Sub-state HIEs
	Next Meeting Reminder Tuesday, March 23, 9-11 am



Privacy and Security Sub Work Group Meeting Minutes



Meeting Date:	Tuesday March 9, 2010	Facilitator:	Kelly Coyle
Place:	Kellog Center, Room 106 East Lansing, MI	Web-ex Information:	https://premconf.webex.com/premconf/j.php?ED=102879277&UID=73752947 password: mihin-ps6
Time:	9:00 – 11:00 AM	Teleconference #:	1-888-3948197 passcode 869479

Topic 1:	Housekeeping and Logisitics Roll Call of Voting Members <i>For both voting and public work group members- when you sign in on the web ex, please use your first and last name so we know who is participating</i> Approval of meeting minutes Review of Meeting Schedule- timeline Questions
Topic 2:	Review of draft policies <ul style="list-style-type: none"> • Access • Authorization • Authentication
Topic 3:	Strategic Plan Please continue to review updated versions and make comments on Work Zone
Topic 4:	Next Meeting Reminder Tuesday, March 16, 9-11 am

DISCUSSION	Topic 1: Housekeeping and Logisitics
------------	---

Roll Call of Voting Members: All voting members are present except for Nancy Walker.

Approval of meeting minutes:

MOTION: Approve meeting minutes
MOTION SECONDED

Comment made that the minutes from last week’s meeting need to clarify that data will not be pushed out unless it’s legally permissible and in regards to substance abuse information under Part 2- this information cannot leave the provider without express permission, either consent or statutorily permitted release.

VOTE: Approved with revision (all present Voting Members)

Kelly reported on the March 4 Outcomes of the Governance WG review of the Informed opt out policy. Time ran out so that policy as well as the ones we review today will be taken up at the next meeting. The strategic and Operational plans will be

used to frame some of the issues that have arisen in our discussions of the policies. The meaning of Opt Out will be clarified

A summary of the Governance meeting discussion on changes for MiHIN is listed below.

- The term “backbone” will no longer be used – it will be Shared Services or Core Services. There will be statewide shared services such as a Master Patient/Provider Index and Record Locator Services, Security Services, Messaging Gateway that can be utilized by all Health Information Exchange initiatives in Michigan
- HIE in Michigan today is not always “local” nor “regional” since HIE initiatives are forming in natural partnerships across the state and not bound by geography. The descriptor is “sub-state” HIE will be used as opposed to regional or local HIE.
- Starting with cross sub-state HIE Lab Results Delivery and integration with public health as initial use cases makes sense.
- Since mostly HIE initiatives in Michigan will connect and use the “shared services” then it is important for the sub-state HIEs to take the lead role in Governing and Financing these shared services. This holds to the guiding principle that “those who benefit should pay” and further holds to the decision that those who will utilize the system are central to governing the system.
- There is a role for state government as part of governance since public health communication is a core functionality and the state is paying significant costs for the matching funds.

Next steps and details can be found in the document posted on Workzone.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Make the report from Governance meeting available to P&S WG members.	Sharon	Mar 11
Change any reference to "backbone" to “shared services” in all documentation that will be referenced moving forward.	Kelly, Linda	Mar 25

DISCUSSION	Topic 2: Review of draft policies
------------	--

These are minimum policies for sub-state HIEs to connect to the core shared services. Sub State HIEs can implement more stringent policies if they wish.

Access Policy

Comment is made that the ‘minimum necessary’ does not apply to clinical information and that qualifier should be stricken from the policy. There is a suggestion to use “need to know” language instead. A comment is made that most health care professionals have a high level of integrity and are not looking for information they are not entitled to. Another point is that health care professionals may need to look at many documents before they find the information they are seeking. Decided laws are already in place to cover this and making a statement that they will access info in accordance with applicable laws is sufficient.

Role-based access is where limitations would be defined. That is in the Authorizations policies the workgroup will review later in the meeting.

Margaret comments that the definition of ‘authorized user’ should be in data exchange agreements as well as requirements that all authorized users must receive specified training.

A voting member comments that it would be an administrative burden if we are expecting to have individual ‘named users’ managed through the MiHIN. In response it is commented that HIPAA requires authentication at the person level, however the manner in which that is implemented varies.

Authentication will come from the HIE level or below. Authentication could be done at the provider level with single sign-on at the portal that provides access to the HIE and then the MiHIN. There must be security at the level where the record is accessed but does that have to be done at the Shared Services Bus level? If so, how would it be administered at that level? Mike Gagnon answers that SAML makes an assertion each time a user accesses information and that assertion says “I’ve already authenticated that person and here are their credentials – this would then be accepted at the higher levels

A voting member points out that this is a technical discussion and has to be deferred. Just two points to remember – for access login must be at the person level and the audit has to be at that level as well,

Regarding being prescriptive with passwords – Kaiser Permanente found that changing them often is actually less secure – people forget, then write them down and it becomes counterproductive.

The point is made that while this workgroup needs to work with the technical group to understand the solution, this workgroup should focus on high level policy. The Access Policy should not be overly prescriptive. It should adhere to a high order' and remember that all entities are governed by HIPAA. It should minimally meet what is prescribed by law with a caveat that the application of that should be technically feasible and not overly costly.

It was decided that this workgroup should make recommendations to the governing body regarding how security should be implemented such as with a Security workgroup once the Governance entity is in place. This WG would then develop guidelines for all HIEs to follow to ensure security protections remain up to date and current.

A voting member makes the point that the workgroup needs to think in terms of three levels _ policies, procedures and guidelines. We will circulate the policy and ask for comments. This group should focus on the policy level, setting a floor for minimum policy. At the same time, the group would like to be able to define best practices. Other voting members agree and remove overly specific bullet points.

Authorization Policy

There was a question regarding whether a single policy would cover identified and de-identified information. That answer is that de-identified information (i.e., research data where all identifiers are stripped off) is not being addressed by this workgroup at this time. So, the answer is no, a single policy does not cover both types of information. The policies coming out of this workgroup refer to identified information.

What is an authorized user? Comment made that it should include certified trading partners. Linda reads the definition from documentation from the State of New York and certified trading partners are included. The definitions developed can be all inclusive.

A voting member asks whether the policy is referring to categories of users or role-based users. The answer is that we should have definitions for role-based categories (there are six of them) and specific role definitions at the HIE level. The role-based categories would be kept very simple and any role definitions from the HIE would have to map into those six at the MiHIN level. Need to add a category for system administration / technical support.

A voting member asks if behavioral health should be a separate category. Behavioral health requires special consent and that is already addressed. The issue of a special category for mental health and maybe specially protected health information will be a parking lot issue in the strategic plan. There are many things in that area to be addressed.

The last bullet will be wordsmithed to indicate that HIEs may have additional roles – they just need to map into the role categories at the MiHIN level.

Also need to address an individual who may have more than one role for example a physician is a clinician but also owns a billing company. Need to ensure they are using the role they are functioning in at the time. Mike suggested there could be two logins. Language added to the policy to cover the multiple roles.

Authentication Policy

A voting member asks, "Can we take a person to court over their claimed identity?" Concerned about the strength of the identity. The fourth level – passport, will stand up in court. Level 1 is not good, Level 2 is password, level 3 is stronger. Should there be Level 2 or 3 NIST required? Might need to parking lot this issue but the question is what level of trust (i.e., authentication) do we need. Ultimately there will be a contractual agreement with HIES and their participating entities.– We need to set the bar at what level that should be. Margaret will post what has been agreed to in the national model data exchange agreements. Many of these go down to the individual user. Have to ensure that each individual is responsible for their actions and that it can be audited – this can be achieved. Concern was expressed about the technical implications. If there is a certified entity (EHR) and the HIE plugs into it, that should be "trusted" as being authenticated. Confirmed that is the way it works – it's a pass-through – the individual user is certified, that's passed to next level, etc.

The policy will set a minimum level of required user authentication. Then each provider will determine how they meet legal and regulatory requirements and that could stipulate more demanding requirements at that level. This is all achieved in the data exchange agreements.

Overly prescriptive requirements were stricken – the policy was left at a high level.



Training on all these policies is required. We can have a separate policy on training in general. We can address training in the policy as well.

Audit policy will be addressed separately along with Breach next week.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Make edits and pass the revised version to members. This version will contain the introductory language for each policy.	Kelly and Linda	March 16
Create a definitions page and align language in all policies.	Kelly and Linda	March 16
Post the national model data exchange agreements.	Margaret	March 16
DISCUSSION	Topic 3: Next Meeting Reminder	

Next meeting is Tuesday, March 16, 9-11 am. Audit Policy and Breach will be the topics.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None		
DISCUSSION	Topic 4: Public Comment	

Question whether the Opt-Out form will need a verification to indicate that the person has been identified as the person they say they are at the provider level. This will be looked into.

Question sent in via Web-ex Chat from Harry McGee: If I visit a health care provider and do not submit an "opt-out." PHI is shared and goes to other community HINs. Does this info then reside in these other HINs? If so, and if I later decide to "opt-out" what will happen to my info that has already gone to other community HINs?

Post meeting response: The data will not be purged. It will remain where it is and from the point the patient decides to opt out, no information will be shared with others. The opt-out effectively puts a stop on pushing any of that patient's data out to other users.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Answer the Chat question.	Kelly. Linda	March 16

Attendees:

- David Allen MiHIN PCO – Consulting Team
- George Boersma MiHIN PCO
- Jeff Bontsas Voting Member
- Donald Carne Member
- Denise Chrylser Voting Member
- Kathleen Cornish MPHI
- Moira Davenport-Ash Voting Member
- Darrell Dontje Voting Member
- Chuck Dougherty Voting Member
- Mike Gagnon MiHIN PCO – Consulting Team
- George Gobel Voting Member
- Tosca Habel Member
- John Hazewinkel Voting Member



- Huzaifa Jamali
 - Gary Lockhart
 - Glen Lutz
 - Linda McCardel
 - Harry Levins
 - Margaret Marchak
 - Melissa Markey
 - Teresa Mulford
 - Paul Muneio
 - Amber Murphy
 - Beth Nagel
 - Harvey Organek
 - Laura Rappleye
 - Kurt Riegel
 - Jim Shaw
 - Mike Tarn
 - Shelli Weisberg
- MiHIN PCO – Consulting Team
General Public
Voting Member
MPHI
MPHI
Chairperson
Voting Member
Member
Member
MiHIN PCO – Consulting Team
MiHIN PCO
Member
MiHIN PCO
Member
General Public
Voting Member
Voting Member

MiHIN Access Policy

Access controls govern when and how a patient's information may be accessed by authorized individuals via the MiHIN. These access policies are designed to reduce unauthorized access and ensure information is used for authorized purposes.

Policy: Access

- Authorized Users will access information via the MiHIN in accordance with all applicable policies, state laws, and federal laws.
- Sub state HIEs will establish policies and procedures to ensure that access meets current security standards
- Only Authorized Users shall access information via the MIHIN.
- Authorized Users shall be authenticated in accordance with the provisions of the Authentication Policy.
- Sub state HIEs and their participating entities will have processes and capabilities in place to ensure accountability and enable identity of each user who has accessed patient information
- All participating entities shall implement and enforce an accountability policy that meets legal and regulatory requirements.
- Authorized Users shall be prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others. The use of another's credentials to access the system is prohibited.
- Users are responsible for all activities related to their unique credentials
- All breaches of credentials must be reported in a timely manner.
- Authorized Users who have access to electronic PHI via the MiHIN will be required to receive training on the access and authentication process and mechanisms required for their job function.
- Sub state HIEs will meet security requirements under state and federal law, and policies and procedures as determined by the MiHIN governing body.
- The MiHIN Governance entity will create and maintain a security workgroup that will recommend best practices and policies/procedures to the MiHIN.

MiHIN Authentication Policy

Authentication is the process of verifying that an authorized individual is who she or he claims to be. Sub-state HIEs using the MiHIN Core Services will implement policies and procedures to verify that an Authorized User seeking access to electronic Protected Health Information is the person or entity he/she/it claims to be.

Policy: Authentication

- All participating entities shall implement and enforce a user authentication mechanism that meets legal and regulatory requirements.
- Community HIEs must authenticate, or must require their participating entities to authenticate, each Authorized User's identity prior to providing any Authorized User with access to Protected Health Information (PHI) via the MiHIN
- Authorized Users shall be prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others. The use of another's credentials to access the system is prohibited.
- Authorized Users who have access to electronic PHI via the MiHIN will be required to receive training on the access and authentication process and mechanisms required for their job function.

MiHIN Authorization Policy

Authorization is the process of determining whether a particular individual within a sub state HIE has the right to access Protected Health Information via the MiHIN. Authorization is subject to role-based access standards that take into account an individual's job function and the information needed to successfully carry out a role within the entities participating in the HIE. These requirements are designed to limit exchange of information to accomplish the intended purpose of the exchange, thereby allowing patients to have confidence in the privacy of their health information.

Policy: Authorization

- Sub state HIEs shall establish and implement policies, standards and procedures that:
 - Establish role definitions for Authorized Users;
 - Define the purposes for which Authorized Users in those roles may access Protected Health Information (PHI) via the MiHIN
 - Define the types of PHI that Authorized Users within such roles may access (e.g., demographic data only, clinical data).
- The purposes for which an Authorized User may access information via the MiHIN and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized User's:
 - Job function
 - Relationship to the patient
- Sub state HIEs shall require their participating entities to assign roles to the individuals within their organizations who will be authorized to access information via the MiHIN. Sub state HIEs and their participating entities may have additional roles, but they must map those roles to one of the seven roles listed below:
 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. Community HIE administrator with access to non-clinical information
 6. Community HIE administrator with access to clinical information for the purpose of public health reporting
 7. System administration support and technical support access
- Users with multiple roles will access data using the role that applies to the job function they are performing at the time.

MiHIN Audit Policy

Audits are oversight tools used for recording and examining access to information within an electronic health information exchange system. They are necessary for verifying compliance with access controls implemented to prevent/limit inappropriate access to information

Policy: Audit

The identity and time frame of each entity that accesses or transmits information through the MiHIN must be recorded and maintained.

Audits must be conducted on a regular basis and once a year at a minimum.

Sub State HIES and Participating entities will implement a system wherein, upon request, patients have a means of seeing who has accessed information about them via the MiHIN and when such information was accessed.

All Sub State HIEs and Participating entities must cooperate with the MiHIN and/or other Sub State HIEs with respect to any audits.

MiHIN Breach Notification and Response Policy

Breach Notification requires Sub State HIEs to notify individuals when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, including when a confirmed breach in the security of the system poses a significant risk of identity theft or other harm. (42 USC §17931)

Policy: Breach Notification

- The Sub state HIE will abide by all applicable federal, state and local laws, rules and regulations pertaining to any security breach related to MiHIN. (42 USC §17931)
- If any HIE or participant experiences a security breach related to MiHIN they must immediately notify the MiHIN governance entity.